VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENI DMS SYSTÉMU V ORGANIZAČNÍ SLOŽCE SPOLEČNOSTI

PROPOSAL FOR THE IMPLEMENTATION OF DMS SYSTEM IN THE ORGANISATIONAL UNIT OF A COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Gabriela Mužilová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Mužilová Gabriela, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh zavedeni DMS systému v organizační složce společnosti

v anglickém jazyce:

Proposal for the Implementation of DMS System in the Organisational Unit of a Company

Pokyny pro vypracování:

Úvod
Cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ADAM, Azad. Implementing Electronic Document and Record Management Systems. New York: Auerbach Publications, 2007. 270 s. ISBN 0-8493-8059-6.
CURRY, Ben. Microsoft SharePoint 2010: kapesní rádce administrátora. Brno: Computer Press, 2011. 647 s. ISBN 978-80-251-3401-6.
KUNT, Miroslav a Olga KUNTOVÁ. Správa dokumentů v praxi. Ostrava, MONTANEX 2002. 172 s. ISBN 80-7225-078-7.
MYŠÍK, Jiří. Hodnocení efektů při zavedení nebo inovaci informačního systému v podniku. Ostrava: Key Publishing, 2010. 55 s. Monografie (Key Publishing). ISBN 978-80-7418-059-0.
STRNÁD, Ondřej. Systémový prístup k riadeniu informačnej bezpečnosti. Tripsoft v Trnave, 2009. ISBN 978-80-89291-20-5.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 29.2.2016

Abstrakt

Diplomová práca sa zameriava na problematiku podnikovej dokumentácie a systémov pre správu dokumentov. Práca rieši návrh projektu implementácie systému SharePoint, vo verzii využívajúcej technológiu Cloud Computing, do vybranej organizačnej zložky spoločnosti. Analyzovaním možných rizík vyplývajúcich z tohto projektu vyplynú v praktickej časti práce návrhy možných zabezpečovacích opatrení. Tie sú v závere práce ekonomicky porovnané s finančnými výdavkami vyplývajúcimi z potenciálnych rizík projektu.

Abstract

Master´s thesis focuses on company´s internal documentation and Document Management Systems. It presents a proposal for the project of SharePoint implementation in the selected organisational unit of a company, using the Cloud Computing technology. An assessment of risks, resulted from the project and especially from the Cloud Computing, leads to the essential part of this paper, to the proposal of security arrangements and solutions. The arrangements will be advised to the organisational unit considering the economic cost comparison with potential risks.

Kľúčové slová

Podniková dokumentácia, DMS, SharePoint, Cloud Computing, Projekt, Dostupnosť, Integrita, Dôvernosť

Key words

Company´s Documentation, DMS, SharePoint, Cloud Computing, Project, Availability, Integrity,Confidentiality

Bibliografická citácia

MUŽILOVÁ, G. *Návrh zavedení DMS systému v organizační složce společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 111s. Vedúci diplomovej práce Ing. Viktor Ondrák, Ph.D.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušila autorské práva (v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa: 24.05.2016 ……

Poďakovanie

Rada by som sa poďakovala pánovi Ing. Viktorovi Ondrákovi, Ph.D. za vedenie mojej diplomovej práce a za cenné a ochotné rady v oblasti riešenej problematiky.

OBSAH

1 ÚVOD

Informácie sú v dnešnej dobe považované za veľmi hodnotné aktívum. Kto ich má a dokáže ich adekvátne využiť, stáva sa flexibilnejším a dokáže sa prispôsobovať aktuálnej situácii či očakávať vývoj novej situácie efektívnejšie než ten, kto informácie nemá. Vďaka extrémne rýchlemu technologickému vývoju produkujeme denne enormné objemy dát. Informácií, v nich obsiahnutých, sa nám dostáva zo všetkých strán a to v neúmernom a až nespracovateľnom množstve. Nositeľom týchto informácií bývajú prevažne určité formy dokumentov. Ich množstvo sa v podnikoch v dnešnej dobe preto zo dňa na deň exponenciálne navyšuje a to samo vytvára priestor pre nové technológie, ktoré dokážu s dokumentami efektívne pracovať, spracovávať ich a upravovať či zdieľať ďalej.

Systémy pre správu dokumentov (Document Management System - DMS) preto v dnešnej dobe pútajú veľa pozornosti, hlavne vo veľkých podnikoch, kde zefektívnená činnosť s dokumentami môže priniesť citeľné ekonomické výsledky. Firmy si takéto systémy implementujú do svojej infraštruktúry väčšinou formou projektu, pričom majú dnes v ponuke hneď niekoľko implementačných platforiem, medzi inými aj cloudové riešenie. To občas zvykne dávať firmám mylný pocit, že všetko podstatné je v rukách poskytovateľa a spoločnosti stačí za zaplatený paušálny poplatok v pohodlí využívať výhody cloudovej aplikácie. V takomto pohľade je však výrazne zanedbané bezpečnostné hľadisko plynúce z úplnej závislosti od poskytovateľa. Žiadny systém totiž nie je neomylný a v prípade výpadku systému, ktorý zhromažďuje všetky potrebné podnikové dáta by mali mať firmy navrhnutý rýchly a efektívny spôsob obnovy, ktorý im umožní fungovať vo svojej podnikateľskej činnosti plynulo ďalej. A ohrozená dostupnosť dát zďaleka nie je tou jedinou hrozbou.

Uvádzaná diplomová práca aplikuje túto problematiku na servisnú pobočku globálne pôsobiacej spoločnosti Zebra, ktorej sa projekt implementácie cloudového systému pre správu dokumentov bude čoskoro týkať. Práca bude stavať na úvodnej analýze aktuálnej situácie pobočky, prevažne v oblasti jej podnikovej dokumentácie. V následnej časti budú spracované teoretické základy, z ktorých práca vychádza a tretia časť bude prezentovať vlastný návrh postupu implementácie systému do firemného prostredia pobočky spôsobom, ktorým maximalizuje jej úžitok.

2 CIELE PRÁCE

Hlavným cieľom diplomovej práce je navrhnúť postup zavedenia DMS systému v organizačnej zložke vybranej spoločnosti s ohľadom na analýzu jej aktuálnej situácie a požiadavky zo strany hlavného podnikového vedenia.

Čiastkové ciele práce zahňujú:

- Zanalyzovať aktuálny stav podnikovej dokumentácie v danej organizačnej zložke a vyhodnotiť potrebu implementácie nového DMS systému
- Návrh projektového riadenia plánovanej zmeny v organizácii a konkrétnej postupnosti projektových činností
- Analýza rizík vyplývajúca z projektu implementácie konkrétneho DMS systému
- Návrh opatrení eliminujúcich negatívne dopady nájdených rizík projektu
- Preskúmanie ekonomickej efektívnosti aplikácie navrhovaných opatrení v rámci projektu v organizačnej zložke

3 ANALÝZA SÚČASNÉHO STAVU

V úvodnej kapitole diplomovej práce bude uskutočnená analýza aktuálnej situácie vybranej organizačnej zložky spoločnosti. Jej analýza bude vychádzať zo základnej analýzy celej firmy, hlavne čo sa týka globálne platných podnikových pravidiel či nariadení. Analýza bude zameraná prevažne na situáciu s podnikovou dokumentáciou a so spôsobom, akým sa s ňou vo vybranej pobočke aktuálne pracuje. V závere analýzy bude súčasný stav stručne zosumarizovaný a ná základe toho budú navrhnuté odporúčané zmeny.

3.1 Základné informácie o firme

3.1.1 Charakteristika podnikateľskej činnosti

Spoločnosť Zebra figuruje na trhu mobilných komunikácií a dátových riešení už od roku 1969, kedy bola v Spojených štátoch amerických založená, so sídlom v Lincolnshire (Illinois). V priebehu času figurovala firma pod rôznymi názvami, no smer svojho zamerania, ktorý bol nastavený na začiatku, sa rozvíjal až do dnešnej podoby jednotným smerom. Spoločnosť z počiatku dodávala tlačiarenské technológie so zameraním sa na čiarové kódy. Presunom výroby do Ázie si začala v 90-tych rokoch otvárať globálny trh. Postupnými zmenami, akvizíciami a fúziami firma rozširovala aj svoje produktové portfólio až do dnešnej podoby. Dnes firma ponúka komplexné produktové riešenie v dvoch hlavných oblastiach:

- Systémy tlače pre automatickú identifikáciu – tlačiarne etikiet s čiarovými kódmi, plastových kariet, lokalizačné riešenia pre lokalizáciu mobility osôb aj majetku v reálnom čase
- Riešenia podnikovej mobility –Scanner na snímanie dát, Mobilné čítačky dát, bezdrôtové technológie, technológie RFID, ako aj riadacie systémy pre manažment zariadení v podnikovej sieti

Spoločnosť sa profilovala ako v štátnom, tak aj v súkromnom sektore, pričom po novom začala pôsobiť aj v oblasti zdravotníctva. Súčasný rozsah pôsobenia spoločnosti je globálny s predajom produktov vo viac než 100 krajinách sveta a s pobočkami vo všetkých hlavných svetových regiónoch. Do týchto pobočiek patrí aj servisné stredisko v Brne, ktoré poskytuje servis zákazníkom z Európy, Blízkeho Východu a z Afriky.

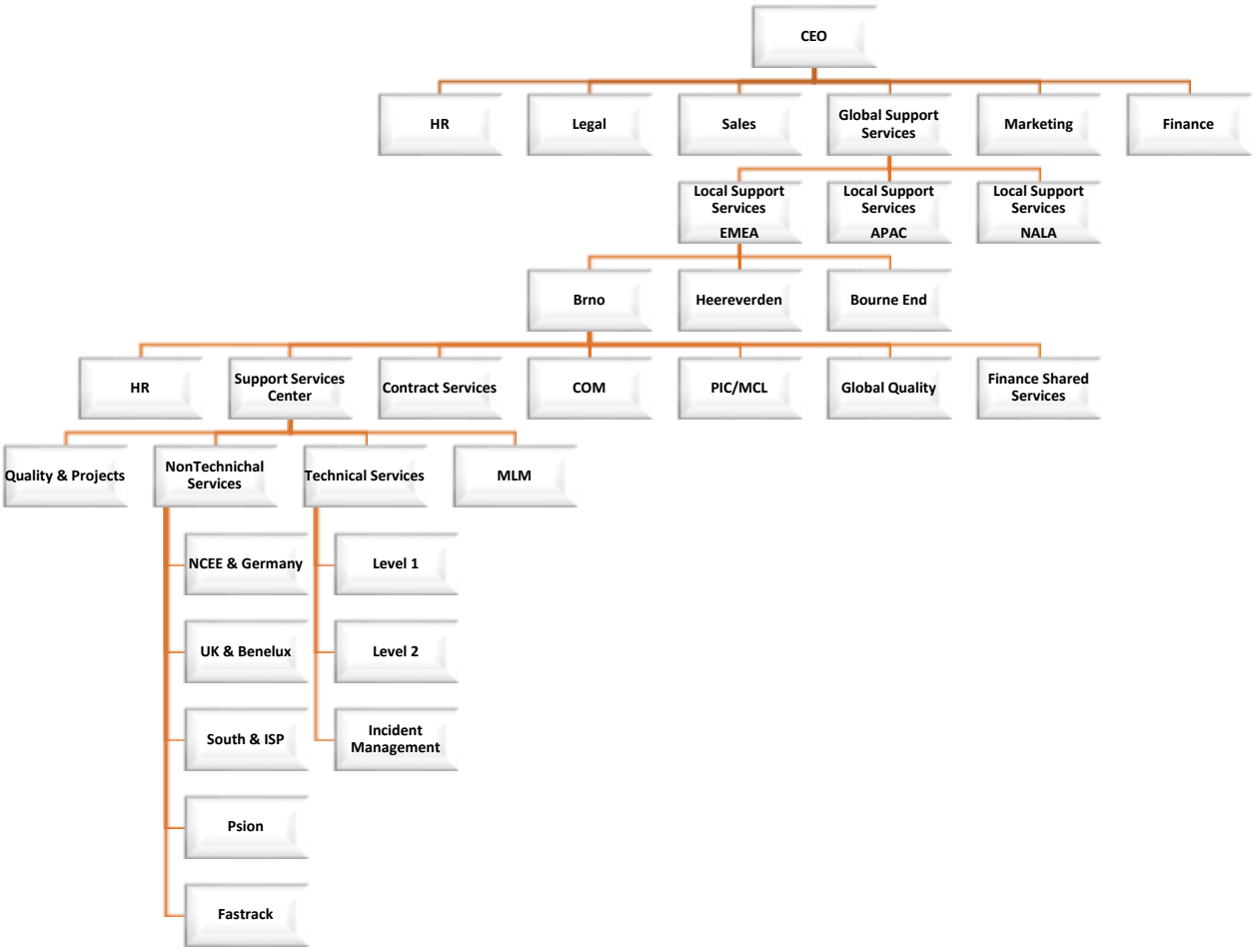
3.1.2 Počet zamestnancov, tržby

Počet zamestnancov sa globálne pohybuje cez hodnotu 7000 pracujúcich vo viac než 200 pobočkách v 40 krajinách, pričom podľa aktuálnej aprílovej štatistiky magazínu Forbes patrí spoločnosť medzi najlepších zamestnávateľov tohto roka. Podľa štatistík z konca roka 2015 boli v danom roku čisté predaje spoločnosti 3 668 milión dolárov a prevádzkový zisk bez odpisov (EBITDA) sa pohyboval vo výške 608 miliónov dolárov.

Obrázok 1 - Predajné pobočky spoločnosti Zebra, Zdroj: (1)

3.1.3 Organizačná štruktúra spoločnosti

Spôsob vnútorného usporiadania činností, procesov a právomocí Zebry je priamo závislý od jej hlavných cieľov. Vnútorné usporiadanie totiž vplýva na schopnosť organizácie pružne reagovať na zákaznícke požiadavky, na produktivitu, náklady a teda aj zisk. Každá zložka organizačnej štruktúry je teda súčasťou reťazca aktivít, ktorý prináša koncovému zákazníkovi určitú pridanú hodnotu. Globálna organizačná štruktúra spoločnosti Zebra je načrtnutá na nasledujúcom obrázku:



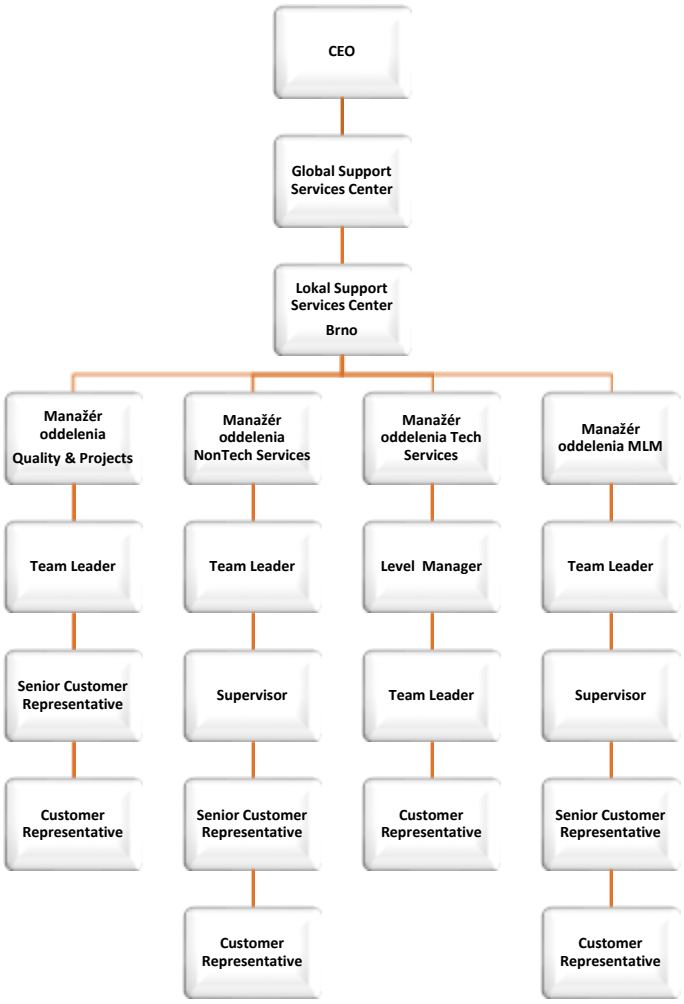
Obrázok 2 - Organizačná štruktúra spoločnosti Zebra, Zdroj: Interné materiály

Spôsob, akým je štruktúra spoločnosti Zebra usporiadaná je možné všeobecne zaradiť medzi účelovo neorganizované maticové štruktúry, pretože zamestnanec zodpovedá funkčnému manažérovi a zároveň manažérovi projektu. Zamestnanci s rovnakým pracovným zameraním sú situovaní v jednej lokalite, no popritom paralelne pracujú na rôznych projektoch. Zaisťuje to rýchly prenos znalostí a informácií, zvýšenie kvality a urýchlenie inovácií.

3.1.4 Riadiaci reťazec

Riadiaci mechanizmus v sledovanej spoločnosti definuje tok prideľovania právomocí, udeľovania rozhodnutí a formálnej komunikačnej postupnosti. Je priamo odvodený od organizačnej štruktúry spoločnosti a má 6-7 riadiacich úrovní. Počet úrovní riadenia v jednej

štruktúrovej línii ovplyvňuje rýchlosť rozhodovania ako aj možnosť iniciatívy, kreativity alebo inovačných návrhov pracovníkov.

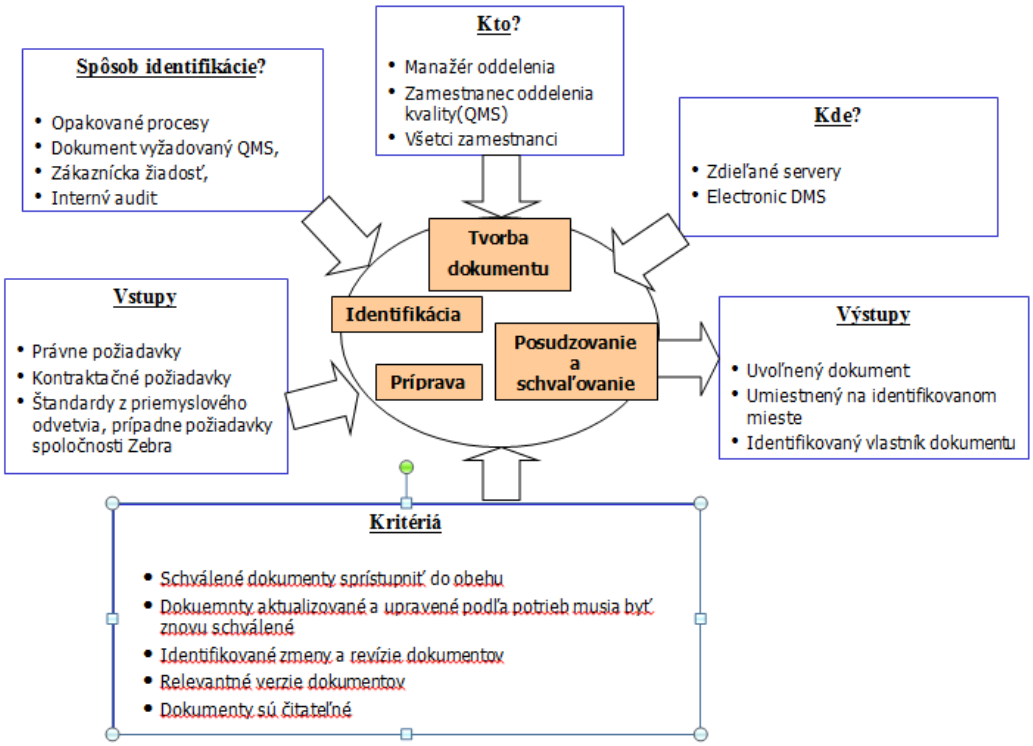


Obrázok 3 - Riadiaca hierarchia, Zdroj: Interné materiály

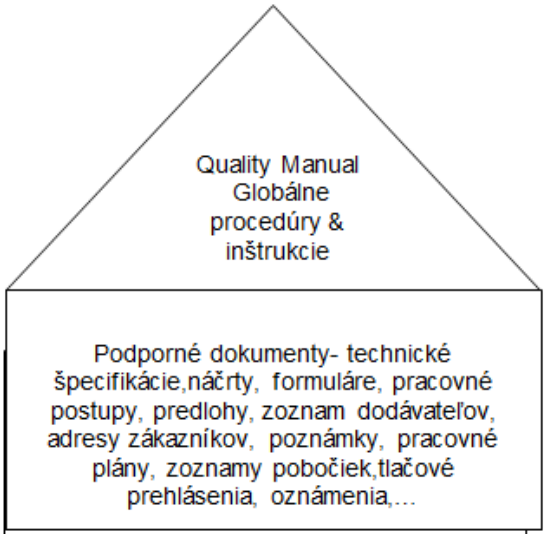
3.1.5 Systém práce s podnikovými dokumentami

Pre manipuláciu s dokumentami existuje v servisnom stredisku platná smernica, ktorá definuje proces práce s dokumentami: tvorbu, identifikáciu, základné požadované kritériá, schvaľovania a zodpovednosť za podnikové dokumenty. Je v nej popísaná aj štruktúra a rozdelenie interných podnikových dokumentov, proces verzovania, vytváranie vzorov často používaných dokumentov, povinné značenie pri identifikácii jednotlivých druhov dokumentov a schvaľovanie interných dokumentov.(viď Obrázok č 4. A Obrázok č.5)

Smernica ďalej definuje proces zaobchádzania s externými dokumentami. Stanovené sú aj spôsoby prideľovania zodpovednosti za jednotlivé typy dokumentov, spôsob a povinná dobu uchovávania záznamov dokumentov.



Obrázok 4 - Proces práce s podnikovými dokumentami, Zdroj: Interné materiály



Obrázok 5 - Štruktúra dokumentov podľa podnikovej smernice, Zdroj: Interné materiály

Spoločnosť Zebra využívala globálne pre spravovanie podnikových dokumentov systém SharePoint od Microsoftu. Koncom roku 2015 sa rozhodla zmeniť platformu tohto systému z On-premise lokálnej verzie do Cloudovej verzie. Spoločnosti to ušetrí náklady na zaobstaranie dostatočného hardwarového a softwarového vybavenia a za zaobstaranie dostatočne vyškoleného IT tímu v každej pobočke. Tieto vysoké nárazové investície sa zmenili do flexibilne upravovaných mesačných poplatkov za užívateľa, výhodnejších pre finančné účtovníctvo spoločnosti. Spoločnosť vďaka tomu užíva výhody 99,9% dostupnosti garantovanej Microsoftom, ako aj geografickú redundanciu dát v systéme.

Systém SharePoint Online je aktuálne využívaný formou centrálneho podnikového intranetu a hierarchickej štruktúry tímových stránok. Intranet slúži k prístupu všetkých pobočiek a oddelení naprieč svetom. Združujú sa tu základné informácie, oznamy, zdieľané politiky a smernice, definície podnikových procesov, atď. Tímové stránky si budujú postupne jednotlivé oddelenia a prístup k nim umožňujú len kompetentným zamestnancom. Systém SharePoint Online je zakúpený v rámci softwarového balíka Office 365 Enterprise E3, ktorý umožňuje firme mimo iného využívať pokročilé vyhľadávacie nástroje alebo analytické a business inteligence nástroje.

3.1.6 Systém zabezpečenia dokumentov

Naprieč spoločnosťou nie sú aktuálne nastavenené požiadavky na jednotný zabezpečovací systém dokumentov a preto si každá pobočka zálohuje najčastejšie lokálnymi diskami celé súborové servery alebo to, čo uzná za vhodné. Smernice zamerané na tvorbu a správu dokumentov a archivovaných záznamov im definujú požiadavky na doby ukladania jednotlivých typov dát do archívov, na povinné počty verzií jednotlivých typov, spôsoby tvorby dokumentov alebo zodpovedné osoby.

Centrálne požiadavky na tie pobočky, ktoré už v SharePointe Online pôsobia, nedefinujú žiadny jednotný systém lokálnych záloh a nepodnecujú teda zamestnancov vo vyvíjaní vlastných snáh o viacnásobné zabezpečenie potrebných dokumentov. S tým súvisí aj absencia globálneho vzdelávacieho programu zameraného špeciálne na manipuláciu s dokumentami, prípadne na zabezpečenia správania sa užívateľov pri zaobchádzaní s dokumentami v cloude. Určite je to nevýhoda minimálne pre pobočky, ktoré už majú alebo plánujú projekt implementácie systému SharePoint Online.

Čo sa týka čisto zabezpečenia internej siete voči externému dodávateľovi hostovaných serverov, má spoločnosť vypracovanú globálne platnú smernicu, ktorá definuje nasledovné požiadavky:

- Nasadenie Zebrou riadeného Firewallu oddeľujúceho dátové centrum poskytovateľa od internej počítačovej siete Zebry a IPS systém z internej strany Firewallu. Logy z činnosti obidvoch systémov musia byť interne zaznamenávané a systémy musia byť bezpečne fyzicky uložené s výlučným prístupom pre IT administrátorov.
- Pokiaľ vyžaduje externý poskytovateľ vlastné internetové pripojenie, musí byť FW a IPS aj na strane jeho datového centra. Konektivita medzi datacentrom a internou sieťou musí byť zašifrovaná, rovnako aj dáta uložené v ňom. Prístup musí byť umožnený len z internej siete Zebry, nie z verejného internetu.
- Každý administrátorský prístup k poskytovateľovým technológiám musí podliehať systému autentifikácie podľa systému riadenia prístupových oprávnení Zebry (IAM-Identity and Access Management) = dvoj- faktorová autentifikácia v prípade nezabezpečeného prístupu.
- Firma sa musí uistiť o poskytovateľovej schopnosti dodržiavať a nasledovať priemyselné zabezpečovacie štandardy v oblasti poskytovaných technológií

3.1.7 Systém riadenia podnikových zmien

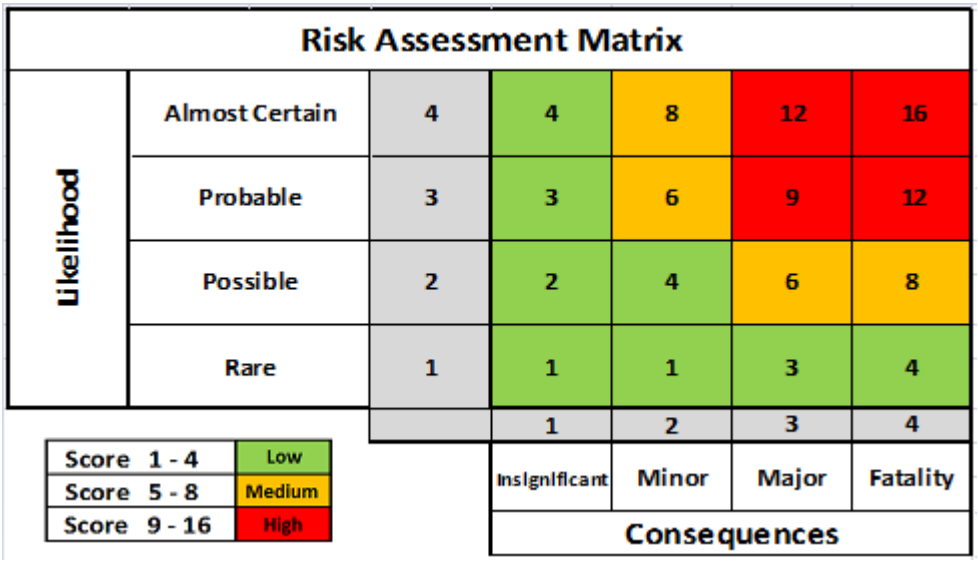
Spoločnosť má vypracovnú globálne platnú smernicu, ktorá stanovuje hlavné úlohy a k nim prislúchajúce povinnosti a právomoci, v prípade závádzania akýchkoľvek podnikových zmien. Tieto úlohy sú :

- **Vlastník zmeny –** osoba, ktorá je zodpovedná za celkové uskutočnenie zmeny a za tvorbu záznamov o nej
- **Manažér zmeny –** je v podstate osoba informovaná vlastníkom zmeny a má na starosti schvaľovanie, spracovanie požiadaviek plynúcich zo zavádzania zmeny
- **Inštalatér zmeny –** vykonáva konkrétne činnosti pre implementáciu zmeny do podniku, prípadne má na starosti výkon záložného plánu
- **Užívateľ –** môže byť v niektorých prípadoch aj iniciátor potreby zmeny, ináč sa prostredníctvom neho testuje správne zavedenie žiadanej zmeny

Presnejší postup alebo požiadavky na konkrétny systém zavádzania podnikových zmien formou projektového riadenia nie je smernicou definovaný.

V súvislosti so zavádzaním zmien je vo firme platná ešte smernica vyhotovenia analýzy rizík. V tomto procese je daná povinnosť manažérov konzultovať s odborníkmi, prípadne zamestnancami, potenciálne riziká a po odhalení nejakého poveriť zodpovedného koordinátora ohodnotením rizika podľa štandardizovaného postupu. Následne sa formou zamestnaneckých porád prerokováva možnosť eliminácie rizík s kompetentnými zamestnancami a schvaľuje sa implementácia opatrenia. Po aplikovaní opatrenia sa uskutoční spätné prehodnotenie rizík, aby bolo možné overiť, či opatrenie dostatočne eliminovalo riziká. Po úspešnom odstránení rizík sa uloží súvisiaca dokumentácia do DMS.

Smernica definuje tiež proces hodnotenia vzniknutého rizika, ako aj kritériá hodnotenia s hodnotiacou maticou. Matica odráža významnosť rizika podľa pravdepodobnosti, s akou môže nastať a podľa rozsahu dôsledkov, ktoré môže riziko spôsobiť.



Obrázok 6 - Hodnotiaca matica pri analýze rizík, Zdroj: Interné materiály

3.2 Analýza sledovanej organizačnej zložky spoločnosti

Podporné servisné cetrum Zebry v Brne vzniklo koncom roku 2014 po akvizícii, v ktorej Zebra odkúpila od Motoroly obchodnú časť „Motorola Enterprise“. Zo strany Zebry to bol logický krok, keďže firmy predstavovali dvoch najväčších hráčov na trhu v oblasti svojho podnikania, dlhodobo medzi sebou spolupracovali a svojimi portfóliami sa adekvátne dopĺňali.Servisné centrum dnes zamestnáva približne 400 zamestnancov a jeho priemerné mesačné čisté príjmy za servisné služby činia približne 4 milióny dolárov. Tieto príjmy mu

priebežne zabezpečujú servisné služby a príjmy z uskutočnených kontraktov na prioritné servisné služby, ktoré pobočka vykonáva pre priemerne viac než 5000 zákazníkov mesačne, z celej oblasti EMEA.

3.2.1 Hlavná podnikateľská činnosť

Produkty, ktoré Zebra predáva, sú všetko technológie s dlhým životným cyklusom, vysokou pridanou hodnotou, ako aj vysokou cenou. Je teda prirodzené, že sa firma zameriava hlavne na veľkých a globálnych zákazníkov, s čím je spojený nevyhnutný predpoklad na kvalitný popredajný servis. Zákazníci, ktorí investujú do produktov Zebry totiž očakávajú skutočne kvalitnú popredajnú starostlivosť a rýchle výmeny či opravy pokazených kusov, pretože ich podnikanie do istej miery závisí aj od produktov Zebry. Veľa zákazníkov preto využíva možnosť priplatiť si nadštandardný zákaznícky servis, ktorý im ručí za zvýšenú starostlivosť v podobe rýchleho, zmluvou stanoveného servisu a riešenia. V prípade prominentných zákazníkov sa jedná o zmluvne stanovenú maximálne 15 minútovú čakaciu dobu zo strany zákazníka. V takých prípadoch si spoločnosť skutočne nemôže dovoliť nespokojného zákazníka, čo tlačí na dôležitosť zefektívňovania procesov servisného centra v Brne.

3.2.2 Zákazníci a ich kategorizácia

Zákazníci servisnej pobočky sú v prvom štádiu kategorizovaný podľa typu uzavretej zmluvy so spoločnosťou. Vnútropodniková smernica presne stanovuje, akým spôsobom a postupom má v prípade jednotlivých zákazníkov prebiehať servisná podpora. V niektorých prípadoch môže totiž úvodná kategorizácia dokázať, že zákazník na žiadnu podporu nárok nemá.

Jednotlivé kategórie rozlišujú medzi priamymi a nepriamymi zákazníkmi a medzi predajným kanálom. Ďalej medzi existenciou partnerského programu, strategickej aliancie medzi firmou a zákazníkom, medzi objemami poskytovaných zakázok či subdodávateľským charakterom zmluvy.Smernica zahŕňa špeciálne výnimky z tejto kategorizácie a rovnako princípy prioritizácie zákazníkov.

Zákaznícke prípady sú ďalej v rámci technickej a netechnickej podpory interne kategorizované do 4 úrovní. Podľa určenej úrovne sa zákazníkovi a jeho prípadu alokujú

podnikové zdroje, prideľuje sa priorita a časový interval vypracovania potrebného riešenia. Rozdeľovanie servisných prípadov do jednotlivých kategórií je dané vnútropodnikovou smernicou. Tá stanovuje presný postup ohodnotenia, do ktorej kategórie zákazník so svojim prípadom spadá a rozlišuje pojmy „Customer Severity“ – technický dopad na podnikateľskú činnosť zákazníka a „Case Priority“ – časová urgentnosť.

V nasledujúcej tabuľke sú zeleným písmom vyznačené povolené kombinácie, ktoré môžu spadať pod klasickú servisnú službu vykonávanú technickým pracovníkom help-desk podpory. Zvyšné, nepovolené kombinácie prestavujú najurgentnejšie a najkritickejšie prípady, kedy zákazníci spadajú do prvých dvoch kategórií a ich prípadom sa urýchlene venuje výlučne oddelenie Incident Managementu. V takých prípadoch zvyčajne vplyvom poruchy produktov Zebry stagnuje zákazníkom ich obchodná činnosť a oni preto požadujú okamžitú nápravu.

Tabuľka 1 - Prideľovanie preferencií zákazníckym prípadom, Zdroj: Interné materiály

Povolené kombinácie		**Case Priority**			
		4	3	2	1
Customer Severity	4	**Yes**	**Yes**	**Yes**	**Yes**
	3	**Yes**	**Yes**	**Yes**	**No**
	2	**Yes**	**Yes**	**No**	**No**
	1	**Yes**	**Yes**	**No**	**No**

3.2.3 Hodnotový reťazec a z neho plynúca tvorba dokumentov

Podnikové činnosti, ktoré vykonáva servisná pobočka Zebry v Brne, je možné rozlišovať na hlavné, ktoré zabezpečujú hlavnú podnikateľskú činnosť, plnenie cieľov a generovanie tržieb a vedľajšie, ktoré generujú zisk len nepriamo svojou podporou hlavných procesov: (1)

Tabuľka 2- Podnikové procesy servisného strediska spoločnosti Zebra v Brne, Zdroj: Interné materiály

Podnikové procesy	
Hlavné procesy	**Podporné procesy**
– Prijímanie reklamácií – Poskytovanie platených opráv – Poskytovanie bezplatných servisných opráv v rámci reklamačného poriadku – Help desk podpora – Predaj nadštandardných kontraktov zabezpečujúcich nadštandarný servis	– Marketing – Správa dokumentov, HW, SW – Administratívna evidencia podnikových činností – Interný audit – Riadenie ľudských zdrojov – Správa financií, ekonomiky podniku

Servisné centrum má na starosti kontakt so zákazníkmi, ktorí už produkty Zebry kúpili a využívajú. Jadrom činností a základnými procesmi sú preto prijímanie reklamácií, poskytovanie platených opráv a iný popredajný servis, ako aj help desk podpora.Z pohľadu dokumentov sú to evidencie dokumentov týkajúcich sa všetkých zákazníckych reklamácií a opráv, ako aj dokumentov týkajúcich sa kontraktov, ktoré si zákazníci priplatili. Jedná sa taktiež o evidenciu záznamov komunikácie so zákazníkmi, ktorá sa vyskytuje vo forme e-mailov, ako aj záznamov telefonických rozhovorov, pre potreby interného auditu a skvalitňovania služieb. Významnou zložkou sú pre servisné služby dokumenty obsahujúce technologické špecifikácie a parametre produktov, metodologický postup servisnej podpory v rámci každého produktu a ďalšie technické dokumenty.

V servisnom centre samozrejme prebieha celá rada ďaľších štandardných procesov a postupov, ktoré produkujú dokumenty ako sú strategické a analytické dokumenty, interné smernice a normy, schválené objednávky a faktúry, evidencie obchodných zmlúv, evidencie a dokumenty o osobných údajoch zamestnancov a ďalšie.

3.2.4 Klasifikácia dokumentov

V aktuálnej globálne platnej podnikovej smernici viažúcej sa k dokumentom, spomenutej v podkapitole 3.1.5, je síce spracovaná štruktúra a obsahové rozdelenie dokumentov vznikajúcich v pobočke, no ich jednoznačná klasifikácia z hľadiska bezpečnosti spracovaná nie je. Pobočka teda v rámci svojich dokumentov nerozlišuje, ktoré dokumenty by jej v

prípade narušenia svojej dôveryhodnosti, dostupnosti alebo integrity spôsobili najväčší problém.

Napriek tomu sa však vďaka čiastočnej spolupráci s pobočkou Zebry a analýzou interných procesov a dokumentácie vytvorila nasledovná klasifikácia dokumentov. Niektoré typy dokumentov sú v tabuľke zahrnuté viackrát a to v prípade, že je ich vyhodnotený negatívny dopad na viacero bezpečnostných hľadísk rovnako vysoký:

Tabuľka 3 - Klasifikácia podnikových dokumentov, Zdroj: Vlastné spracovanie podľa interných materiálov

Bezpečnostné ciele	Potenciálny dopad na organizáciu v prípade narušenia jednotlivých bezpečnostných cieľov		
	Nízky	Stredný	Vysoký
Dostupnosť dokumentov	Zoznam pobočiek, Poznámky, Tlačové prehlásenia	Zoznam dodávateľov, Interné oznámenia, Všeobecné pracovné postupy, ISO normy	Interné cenníky služieb, Kontaktné informácie o zákazníkoch, Technické špecifikácie produktov a parametre, ktoré pomáhajú pracovníkom helpdesku, Procesný postup opráv, Knowledge management dokumentácia, Incident management procesy, Postupy kategorizácie zákazníkov a prideľovania servisných priorít, Šablóny komunikácie
Itegrita dokumentov, vymazanie, pozmenenie	Zoznam zamestnancov, Rozvrh pracovných smien	Všeobecné charakteristiky produktov, Všeobecné pracovné postupy	Kontaktné informácie o zákazníkoch, dodávateľoch, zamestnancoch, Výsledky interného auditu, Špecifická projektová dokumentácia, Špecifické pracovné postupy
Dôvernosť dokumentov, neautorizované prečítanie	Tlačové prehlásenia, Všeobecné oznámenia, Zoznamy podnikových udalostí, Program spoločenskej zodpovednosti	Všeobecné pracovné postupy, Zoznamy dodávateľov, Všeobecná projektová dokumentácia	Faktúry, Potvrdenia o zaplatení, Zmluvy o prioritných kontraktoch, Kontaktné a osobné informácie o zákazníkoch, dodávateľoch a zamestnancoch, Interné cenníky, Výsledky podnikových analýz, Výsledky interného auditu,Testovanie poruchovosti, Strategické zámery pobočky, Plány projektov, Analýzy rizík, SLA
	Kategória A	**Kategória B**	**Kategória C**

Keďže pre pobočku sú bezpečnostné hľadiská dostupnosti, integrity a dôveryhodnosti dokumentov uložených na Sharepointe rovnako dôležité, kategorizujú sa v rámci rovnakej výšky potenciálneho dopadu na organizáciu do rovnakých skupín. Na základe týchto skupín sa bude s dokumentami v rámci ich zaobchádzania a zabezpečovania rozlične pracovať. Samozrejme nie sú vylúčené výnimky, ktoré by sa tejto pomerne jednoduchej klasifikácii nevymykali a bolo by potrebné s nimi zaobchádzať špecificky.

3.2.5 Sučasný systém ukladania a správy dokumentov

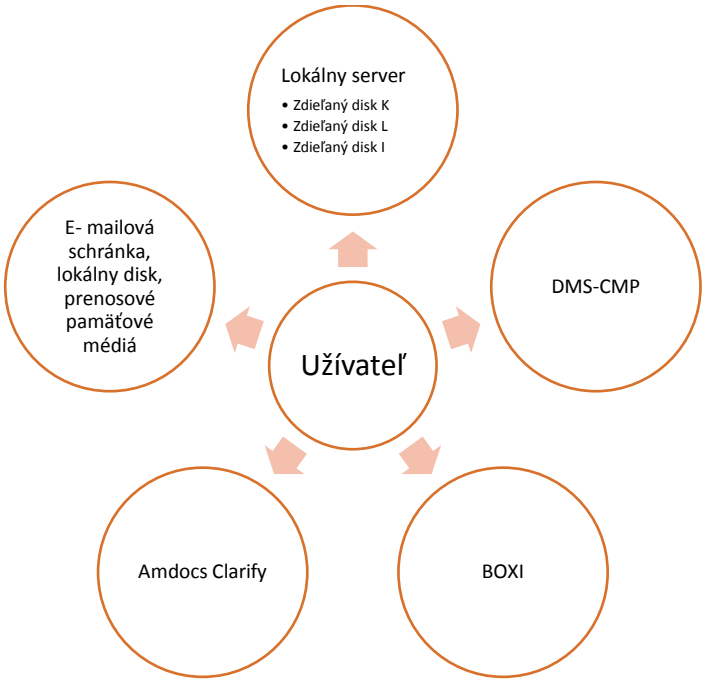
V závislosti od povahy svojej obchodnej činnosti pracuje servisné centrum denne s veľkými objemami prevažne neštruktúrovaných dokumentov. S dokumentami pracuje denne viac rôznych zamestnancov, často je potrebné vyhľadávať staršie dokumenty viažúce sa k histórii zákazníckych servisných opráv alebo je potreba presúvať dokumenty medzi firmou a externe spolupracujúcim opravárenským centrom. Pre efektívnu prácu s nimi je teda potrebný flexibilný a výkonný DMS.

Momentálny stav v podnikovej dokumentácii je veľmi decentralizovaný. Dokumenty sú ukladané do rôznych úložísk:

- **DMS - CMP** je korporátny systém pre správu dokumentov, poskytujúci webové užívateľské rozhranie vo forme portálu.Dokumenty a dáta z tohoto systému sú uložené na serveri spoločnosti Motorola v Severnej Amerike. V systéme CMP sa ukladajú oficiálne podnikové dokumenty vznikajúce z hlavných procesov servisného centra, ako napríklad potvrdenia o objednávke platenej opravy od zákazníkov, podnikové normy a smernice alebo dokumentácia k interným auditom. V knižnici dokumentov môžu oprávnení užívatelia - predovšetkým manažéri a teamleaderi, vytvárať zložky a prideľovať oprávnenia ostatným podľa riadiaceho systému. Jednotlivé oddelenia majú na portáli CMP vytvorenú svoju tímovú podstránku na ktorej zdieľajú základné a kontaktné informácie o svojich tímoch. Podnikové oddelenie Non-Technical support ukladá do systému CMP doklady o zákazníckych objednávkach požadované normou ISO 9001. DMS systém CMP je pôvodne navrhnutý software pre spoločnosť Motorola preto servisné centrum, ktoré akvizíciou odkúpila spoločnosť Zebra, musí definitívne všetku svoju dokumentáciu migrovať do iného, vlastného DMS systému. Mimo iného však systém nevyhovuje dostatočne požiadavkam servisného centra ako software pre správu dokumentov. Systém je ťažkopádny, málo prispôsobivý užívateľovi a nepodporuje rozšírenia o nové komponenty, ako workflow alebo online editovanie súborov.
- **BOXI – Business Objects Web Intelligence XI System –** slúži prevažne pre ukladanie obchodných reportov, ktoré vypracováva oddelenie dátových

analytikov a prístup užívateľom je definovaný v centrálnej databáze užívateľov Active Directory.

- **3 zdieľané súborové servery**, na ktorých majú jednotlivé oddelenia svoju zdieľanú zložku s dokumentami. Zdieľané zložky podliehajú prístupovým obmedzeniam len pre oprávnených užívateľov, ktoré sú definované v centrálnej databáze užívateľov Active Directory. Pre prístup k dokumentom svojho oddelenia musia mať užívatelia namapované tri sieťové zdieľané disky. Server, na ktorom sú momentálne zdieľané disky, je situovaný v Brne.
- **Mailbox, Lokálne disky zamestnancov, Pamäťové prenosové médiá-** ukladanie dokumentov tu prebieha intuitívne a samostatne, podĺa individuálneho uváženia zamestnancov, čo zvyšuje pravdepodobnosť zmätku v platných verziách dokumentov ako aj zbytočné zaťaženie pamäťovej kapacity.
- **Amdocs Clarify –** systém svojou funkciou predstavuje CRM software, ktorý poskytuje možnosť ukladaniu záznamov o zákazníckych opravách vo forme technických prípadov s unikátnym identifikačným číslom (Case Number).



Obrázok 7 - Decentarlizovaný systém správy podnikových dokumentov, Zdroj: Vlastné spracovanie podľa interných materiálov

3.2.6 Objemy podnikovej dokumentácie

V dôsledku vysokej pravdepodobnosti duplicít dokumentov a roztrieštěného systému ich ukladania nie je jednoduché presne vyčísliť momentálny objem dokumentov, ktoré je potrebné zmigrovať do nového DMS. Presne známy je len objem dokumentov potrebných na prevod zo systému CMP a predstavuje 13 TB. Dokumenty sú prevažne textových formátov, prípadne formátov tabuliek a grafov, multimediálne dokumenty sa vyskytujú v minimálnom množstve.

3.2.7 Spôsob práce s dokumentami

Dokumenty sú nositeľom informácii pre každého jedného zamestnanca servisnej pobočky.Každý k ich tvorbe v určitom pomere a s určitou frekvenciou prispieva a na dennej báze ich využíva. Zamestnanci technickej a netechnickej podpory vychádzajú pri svojej činnosti z dokumentov obsahujúcich metodiky a postupy zákazníckej podpory, zákaznícke údaje či technologické parametre produktov a možností ich opráv. Netechnická podpora zaznamenáva v dokumentoch priplatené kontrakty zákazníkov a na základe nich potom vyhodnocujú postup svojej podpory. Cenníky žiadaných servisných služieb či faktúry sú nimi tiež využívané na dennej báze.

V aktuálnej roztrieštenej dokumentovej štruktúre nie je možné hovoriť o nejakej systematickej správe dokumentov alebo o centralizovanom systéme ich riadenia. Užívatelia využívajú zvykom zaužívané spôsoby práce s nimi a ich zdieľania, čo s ich narastajúcim množstvom, spomalenými preplnenými úložiskami a vyskytujúcimi sa duplicitami môže vyvolávať časové prestoje a predlžovanie hlavných podnikových procesov - teda servisnej obsluhy zákazníkov. Ukazovateľom tohto negatívneho dopadu môžu byť penále vyplácané zákazníkom za nedodržanie zmluvou stanoveného času servisnej obsluhy, ktoré začiatkom tohto roka predstavovali mesačne približne 1000 dolárov. Napriek tomu, že v porovnaní s tržbami táto suma nie je veľká, pobočka by ju veľmi rada eliminovala k nule, keďže okrem finančného nákladu to so sebou prináša oveľa negatívnejší dopad – stratu zákazníckej dôvery.

3.2.8 Spôsob zabezpečenia podnikových dokumentov

Pobočka má momentálne nastavený veľmi roztrieštený systém ukladania dokumentov. Dostupnosť kriticky dôležitých dokumentov mala zabezpečenú tým, že boli jednak uložené v systéme CMP na serveroch spoločnosti Motorola uložených fyzicky v Amerike a v prípade

ich nedostupnosti mala kritické dokumenty (často v duplicitných alebo neaktuálnych verziách) uložené na lokálne zdieľaných diskoch na fyzicky prítomných serveroch v Brne. Servery, ktoré patria spoločnosti Motorola, však stratia v dohľadnej dobe svoje oprávnenie na využívanie a pobočka musí vytvoriť nový systém ukladania a zabezpečovania svojich dokumentov.

3.2.9 Vzdelávací program v oblasti manipulácie s dokumentami

V pobočke prebieha v intervale dvoch rokov pravidelné IT školenie užívateľov, ktoré zahrňuje základné bezpečnostné užívateľské povedomie ohľadom prístupových hesiel, e-mailovej komunikácie, fyzického zabezpečenia, atď. Školenie zamerané špecificky na manipuláciu, ukladanie a správu dokumentov v pobočke aktuálne chýba, o čom svedčí aj aktuálny decentralizovaný a nežiadúci stav.

3.3 Zhrnutie analýzy súčastného stavu

Mimo uvedených častí analýzy súčasného stavu servisnej pobočky Zebry v Brne bola vyhotovená ešte analýza SWOT, jej náhľad je uvedený v prílohe A. Analýza vychádza z porovnania aktuálne pôsobiacich interných, externých a konkurenčných faktorov, ktoré v diplomovej práci nie sú podrobnejšie rozobrané z dôvodu jej rozsahového obmedzenia.

Keďže stredisko je len servisnou pobočkou globálnej spoločnosti, jeho najväčším poslaním je vykonávať svoju činnosť čo najlepšie, najrýchlejšie a najefektívnejšie, čím udrží spokojnosť existujúcich zákazníkov Zebry. Všeobecne je možné usudzovať, že zákazníkov môže odplašiť buď nespokojnosť s činnosťou a ponúkanými službami alebo výhodnejšia konkurencia. Aktuálne konkurenčné riziko, ktorému pobočka podlieha, je však vplyvom jej jedinečne komplexného produktového a servisného portfólia pomerne nízke. Preto s cieľom dosahovania lepších výsledkov je vhodné upriamiť viac pozornosť na vlastnú činnosť strediska a snažiť sa o zefektívnenie procesov a tým aj skvalitnenie ponúkaných služieb.

Zo SWOT vyplynula pobočke ako výrazná slabina jej aktuálna situácia správy podnikovej dokumentácie po uskutočnenej akvizícii. Systém je nejednotný, decentralizovaný, pričom väčšina užívateľov stále používa pôvodné systémy, na ktoré stratí v blízkej dobe oprávnenie. Keďže s dokumentáciou pracujú zamestnanci helpdesku na dennej báze, neprehľadnosť systémov výrazne spomaľuje prácu a teda aj obslúženie požiadaviek zákazníkov. Ďalším

problémom je duplicita dokumetov a z nej odvodený zbytočne veľký objem dát potrebných k zálohovaniu. Pomalosť a zastaralosť tohto riešenia navyše výrazne demotivuje pracovníkov.

Implementovanie nového jednotného systému DMS je preto pre pobočku nie len výhodné, ale aj nevyhnutné.

3.3.1 Potrebná zmena v systéme pre správu dokumentov

K naplneniu zmyslu a podstaty akejkoľvek zmeny v servisnej pobočke Zebry je automaticky požadované dosiahnutie efektívnejšieho stavu, než je ten súčasný. K tomu je teda logicky potreba podrobne si zosumarizovať akých nedostatkov sa chce vedenie zbaviť a aké výhody zo súčasného riešenia chce ponechať aj v novom, zmenenom stave. Tento princíp je možné aplikovať aj na plánovanú zmenu systému pre správu dokumentov. Nedostatky súčasného riešenia už boli v práci načrtnuté, no v nasledujúcej tabuľke sú doplnené o porovnanie s pozitívnymi znakmi.

Tabuľka 4 - Porovnanie nedostatkov a výhod aktuálneho systému správy dokumentov, Zdroj: Vlastné spracovanie podľa interných materiálov

Nedostatky aktuálneho systému práce s podnikovými dokumentami	Výhody súčasného systému práce s podnikovými dokumentami
• Nejednotnosť, decentralizácia • Duplicity dokumentov • Slabý prehľad o aktuálnosti verzií • Časová neefektívnosť z dôvodu neprehľadnosti systému • Málo výkonný systém vyhľadávania v dokumentoch • Nespokojnosť užívateľov s rýchlosťou systému • Nutnosť využívať viac internetových prehliadačov	• Čiastočné portálové riešenie • Možnosť offline prístupu na zdieľané sieťové disky • Jednoduchosť práce so súbormi na platforme Windows vyžaduje minimálne nároky na školenia užívateľov

3.3.2 Požiadavky investora na zmenu

K uvedenému porovnaniu je potrebné ešte zahrnúť požiadavky vrcholového vedenia, ktoré aktuálny systém nespĺňa. Vedenie spoločnosti striktne požaduje globálne zjednotenie informačného systému pre správu dokumentov. To môže totiž priniesť zjednodušenie a zefektívnenie do všetkých oblastí, do ktorých zasahuje. Využívanie spoločných štandardizovaných rozhraní a služieb šetrí čas pre potrebu nových návrhov, riešení alebo

nezhôd. Jednotný systém mimo iného minimalizuje náklady na tvorbu distribučných kanálov so všetkými podnikovými stakeholderami, dáva príležitosť na úsporu pracovných síl, zefektívňuje podnikové procesy aj poskytované služby, čo všetko ústí k hlavnému cieľu všetkých podnikov – k zvyšovaniu zisku.

Tabuľka 5 - Požiadavky investora na nový DMS systém, Zdroj: Interné materiály

Požiadavky vedenia na nový systém pre správu dokumentov
• Centralizácia systému • Globálne jednotný systém • Možnosť využívania Business Intelligence nástrojov priamo v systéme • Workflow • Sociálne portálové nástroje pre jednoduchú interakciu užívateľov v rámci globálnej spolupráce • Kompatibilita s MS Office kancelárskym balíkom • Mobilný prístup k dokumentom • Flexibilita užívateľského rozhrania, možnosť kustomizácie • Možnosť offline prístupu • Efektívny systém vyhľadávania v dokumentoch

Z pohľadu architektúry IS je možné v tomto prípade hovoriť o požiadavke na systémovú integráciu na úrovni aplikačnej vrstvy a používateľského rozhrania, keďže sa do brnenskej pobočky musí implementovať nový systém správy dokumentov vo forme webovej aplikácie s globálne štandardizovaným užívateľkým rozhraním pre zamestnancov spoločnosti.

3.3.3 Výber konkrétneho systému

Tradičným postupom by sa v kroku výberu najvhodnejšieho riešenia konal prieskum trhu a ponuky v oblasti systémov pre správu dokumentov, zorganizovalo by sa výberové konanie, v ktorom by sa pozvala skupina najvhodnejších adeptov a vypočul sa návrh ich riešení a postupným vyraďovacím systémom by sa dospelo k najvhodnejšiemu riešeniu a dodávateľovi riešenia.

Tento krok bol však v prípade brnenského servisného centra skrátený. Hlavná časť firmy s ohľadom na celopodnikovú stratégiu a ciele už výberovým konaním pre výber najvhodnejšieho systému pre správu dokumentov prešla a globálne už istú dobu využíva systém SharePoint 2013 od spoločnosti Microsoft, po novom už cloudovú verziu SharePoint Online. Software Sharepoint svojou funkcionalitou ďaleko presahuje základný systém pre

správu dokumentov, obsahuje totiž mimo iného aj funkcionalitu ostatných komponent systémov ECM, možnosť využívania Business Inteligence nástrojov, databázy vo forme webových aplikácií alebo technológiu cloud computing.

SharePoint Online spĺňa požiadavky vedenia spoločnosti Zebra, dokonca ich presahuje a umožňuje technologický rozvoj a preto vedenie rozhodlo, že brnenské servisné centrum zavedie systém Sharepoint, ako svoj systém pre správu dokumentov a zmigruje všetky svoje podnikové dokumenty do jedného centrálneho systému. Systém sa tak stane globálne jednotným a zefektívni a urýchli globálnu spoluprácu v rámci firmy, ako aj mimo nej.

3.3.4 Vlastné zhodnotenie analýzy

Uskutočnená analýza aktuálnej situácie servisnej pobočky spoločnosti Zebra jasne preukázala nevyhnutnosť implementovania nového, centralizovaného systému DMS. Tlakom z vedenia sa presadilo riešenie vo forme cloudového systému SharePoint Online. Verím, že v danej situácii by pobočka lepšiu variantu než SharePoint od Microsoftu nenašla. Potrebná synchronizácia činností a spolupráca na globálnej úrovni by iným systémom nebola zaistená, navyše je tu veľká výhoda maximálnej spolupráce systému s kancelárskym balíkom Office, bez ktorého si dennú činnosť zamestnancov nie je možné ani predstaviť.

Otázkou však zostáva voľba cloudového riešenia. Jednoduchosť implementácie, flexibilita úprav úložného priestoru, mobilná dostupnosť 99,99%, transparentné mesačné paušálne náklady, automaticky aktualizovaný servis a množstvo ďalších výhod pobočke cloud bezpochýb prinesie. No na druhej strane tu stoja úplne nové otázky bezpečnostných hrozieb a závislosti od poskytovateľa, limitované administrátorské práva, úplná závislosť od internetového prístupu, či limitované analytické a aplikačné funkcie.

Osobne predpokladám, že pre pobočku v praxi prevážia uvedené výhody cloudového riešenia. Musí však prebrať taktiež iniciatívu a nenechať sa len pasívne viesť vedením zo strany poskytovateľa. K uvedeným rizikám a nevýhodám existuje rada možných opatrení, ktoré môže pobočka s minimálnymi nákladmi proaktívne zaviesť a využívať tak výhody centralizovaného cloudového DMS v maximálnej možnej miere. Týmto možným opatreniam sa bude venovať kapitola vlastného návrhu riešenia.

4 TEORETICKÉ VÝCHODISKÁ PRÁCE

Teoretická kapitola dodáva práci všeobecné východiská a definície, na ktorých sa zakladajú tvrdenia v analýze a návrhy v praktickej časti práce. Budú tu priblížené dokumenty aj systémy pre prácu s nimi, no rovnako aj stručné vysvetlenie cloudovej technológie či projektového riadenia. Obsaový rámec bol vybraný tak, aby dostatočne, no stručne ozrejmil všetky potrebné pojmy z ostatných častí práce.

4.1 Informácia, informačná spoločnosť

Slovo "informácia" používame všetci denne, bezprostredne a úplne intuitívne. Jeho počiatky siahajú až k roku 1274, kedy bol tento výraz zaznamenaný poprvýkrát, pričom vychádza z latinského slova "informare"= formovať, tvarovať. (2)

Počiatočné technické vnímanie informácie vo význame údaju, správy a potreby oznámiť niekomu niečo v čo najkratšom čase sa však vývojom doby zmenilo na spoločenské vnímanie. V tomto ponímaní chápeme informáciu ako súčasť informačného hodnotového reťazca, ktorý vedie ku znalostiam: Dáta→Informácie→Znalosti. (3)

Informáciu môžeme považovať za správu o uskutočnení istého javu, ktorá nám zníži resp. úplne odstráni neznalosť konkrétneho javu. (3)

Informovanosť a vytvorenie znalostí vnímame prirodzene ako všeobecnú výhodu, no v dnešnej technologicky pokročilej dobe sa z tejto výhody stáva skôr nutnosť. Globálnym prepojením sveta na konci 20. storočia sieťou Internet sa informácie, informačné systémy a informačné komunikačné technológie dostali do centra pozornosti, pretože možnosti získavania znalostí dosiahli úplne nové rozmery. Každé obdobie vývoja spoločnosti si so sebou nieslo charakteristickú vlastnosť a dá sa povedať, že súčasná etapa ľudského vývoja je charakteristická práve informáciami a preto sa dnes hovorí o informačnej spoločnosti. (2)

4.2 Úvod do podnikovej informatiky

Princípmi a metódami práce s informáciami sa zaoberá informatika. Informatika si našla svoje nezastúpiteľné miesto v dnešnej dobe a čím ďalej tým rýchlejšie sa dostáva do všetkých oblastí dnešnej spoločnosti. Najvýraznejšie prejavy tejto masívnej informatizácie vnímame v

obchodnej sfére a v dopade na podniky a ich riadenie. Pri vplyve informatiky na podniky hovoríme o podnikovej informatike. (4)

Už len pri bežnom pozorovaní nemôže nikomu ujsť, že spektrum produktov a služieb sa na trhu rozširuje. Toto rozširovanie je vo veľkej miere spôsobené hlavne nárastom ponuky informačných produktov a služieb, ktoré sú buď vo forme pridanej hodnoty k pôvodným produktom alebo predstavujú samostatnú, novú produktovú radu či službu. (4)

Informačné produkty a služby v obidvoch spomenutých formách predstavujú pre podnik obrovský potenciál. Umožňujú mu totiž rozšírenie hraníc svojho pôsobenia do nových segmentov, či už zákazníckych alebo geografických. Podnik tak môže pôsobiť v reálne globálnom obchodnom prostredí. Všetko má však viac uhlov pohľadu. Globalizácia obchodného prostredia so sebou prináša aj globálnu konkurenciu a podniky sú svojím spôsobom informačnými technológiami tlačené k prežitiu na trhu. Čo sa javilo ako voľba dosiahnutia konkurenčnej výhody sa začína stávať nevyhnutnosťou k udržaniu sa na trhu. (4)

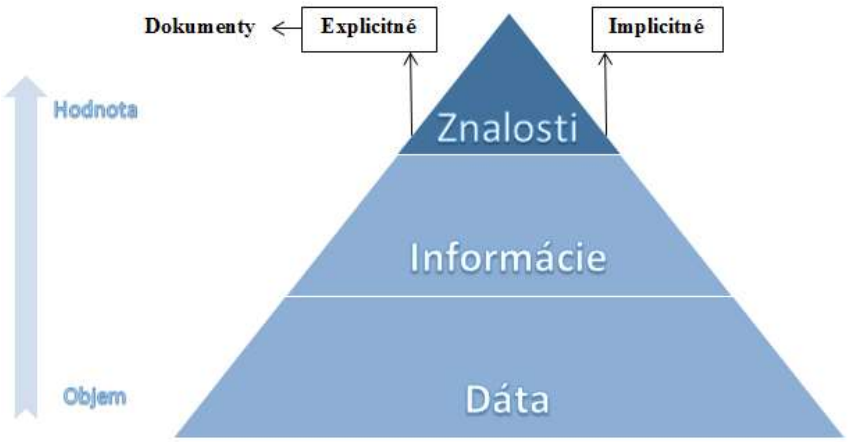
S narastajúcou konkurenciou však prirodzene rastie aj vyjednávacia sila zákazníkov či dodávateľov. Dlhodobá starostlivosť o zákazníka je jedinou možnosťou udržania si ho a k tomu nevyhnutne patrí nutnosť poznať ho a poznať jeho potreby. Dodávatelia musia na seba prevziať čo najviac starostí zákazníka, ako sú priebežná správa a kontrola dodávok, automatické poskytovanie potrebných informácií alebo udržovanie minimálneho stavu zásob na sklade. (4)

Tomuto všetkému sa bezpodmienečne musí podriadiť vedenie podniku. Vedenie sa musí snažiť integrovať poskytované služby pre zákazníka do takej miery, že zákazník môže byť na jednom mieste obslúžený bez toho aby si všimol, či je služba alebo produkt poskytovaný priamo od kontaktovaného obchodníka alebo od jeho subdodávateľov. Významnú úlohu hrajú samozrejme čas, kvalita a nízke náklady, k čomu môže automatizácia podnikových procesov výrazne prispieť. (4)

Pre podporu prispôsobovania sa všetkým týmto nutným zmenám slúžia v podniku informačné systémy a informačné technológie. Okrem podpory by však mali poskytnúť aj základ pre ďalší dynamický rozvoj v želaných oblastiach. (4)

4.3 Dokumenty ako podnikové aktívum

Informácie, ako už bolo spomenuté, sú súčasťou informačného hodnotového reťazca, ktorý vedie ku znalostiam. Touto problematikou sa zaoberá znalostný manažment, ktorý kladie dôraz na rozlišovanie medzi spomenutými kategóriami a zvýrazňuje potrebu rozdielného riadenia informácií a znalostí. (5)



Obrázok 8 - Znalostná pyramída, Zdroj: Vlastné spracovanie podľa (5)

Dáta sa v tomto modeli chápu ako všetko, čo môžeme vnímať zmyslami. Nie sú závislé od ľudského vedomia, sú objektívne a majú podobu faktov. Informácie považujeme za tú časť dát, ktorým človek priradí nejaký význam alebo dôležitosť. Informácie sa už považujú za subjektívne, pretože im človek pridelil nejaký konkrétny účel. Znalosť chápeme ako niečo ”navyše pridané” ku informácii. Je to určitý súbor informácií, ktoré sú zmysluplne zasadené do určitého kontextu a predurčujú nás k nejakej činnosti. Činnosť už následne predstavuje určitú pridanú hodnotu. (5)

Znalosti delíme podľa možnosti ich vyjadrenia na: (3)

- Implicitné/Tacitné
- Explicitné

Implicitné/tacitné znalosti nie sú ľahko vyjadriteľné. Sú to nevyjadrené schopnosti, skúsenosti, intuície, ktoré sú buď získané vzdelaním či tréningom, no v niektorých prípadoch

ani nevieme odkiaľ ich máme, resp. nevieme, že ich vôbec máme. Príkladom na to môže byť úloha: Slovne opíšte, ako vyzerá zelená farba? (3)

Explicitné znalosti sú ľahko formulovateľné, dajú sa ľahko vyjadriť formalizovaným spôsobom (písmenami, znakmi alebo slovami), vďaka čomu sa ľahko komunikujú a zdieľajú. Zaznamenávajú sa formou dokumentov, v databázach a v informačných systémoch. Ukladajú sa napríklad do systémov pre správu dokumentov. Pre organizáciu, ktorá využíva v širokej miere informačné technológie bývajú prioritné explicitné znalosti. Ich riadenie prebieha ukladaním znalostí vo forme dokumentov do systémov pre správu dokumentov. (3)

Dokumenty teda vďaka svojej schopnosti uchovávať a prenášať informácie a znalosti, sú považované za podnikové aktívum. Aktívum sa v tomto prípade chápe ako hmotný alebo nehmotný majetok podniku a je mu prisudzovaná určitá hodnota. Tá sa v prípadoch informačných aktív určuje podľa nákladov vzniknutých pri narušení dôvernosti, dostupnosti alebo ich integrity. V praxi sa tento prístup zvykne počítať tzv. súčtovým algoritmom: (6)

$$\textbf{Hodnota aktíva} = (\textbf{Dostupnosť} + \textbf{Dôvernosť} + \textbf{Integrita}) / 3 \qquad (6)$$

Viac o týchto pojmoch bude spomenuté ďalej v podkapitole 4.9.3.

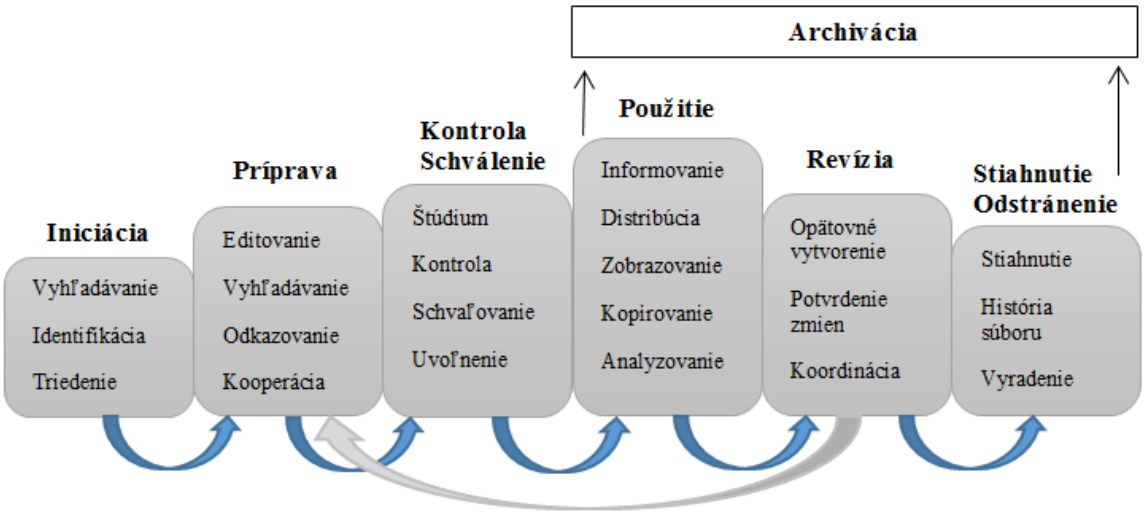
4.4 Životný cyklus dokumentov

Dokumenty, ako nositelia explicitných znalostí alebo informácií všeobecne, prechádzajú postupne svojím životným cyklom, ktorý je možné rozdeliť do 6-tich krokov, pričom každý spĺňa rozdielnu funkciu. Jednotlivé kroky sú spracované podľa normy ČSN EN 82045-1 o správe dokumentov: (7)

1. **Iniciácia** – z úvodnej fázy vzniká tzv. Pracovný rámec, ktorý slúži na vypracovanie daného dokumentu. V rámci toho musí byť dokument jednoznačne indetifikovaný metadátami, ktoré nebudú závislé od jeho fyzického umiestnenia. V tejto fáze prebieha aj triedenie dokumentov podľa želaných podmienok alebo špecifikovaných systémov triedení.
2. **Príprava –** Vývoj obsahovej stránky dokumentu
3. **Ustanovenie-kontrola a schválenie –** Procedúram schvaľovania a kontroly sa dokument môže podrobiť vo vnútri príslušnej organizácie. Pokiaľ to však vyžaduje kontrakt, môže

byť nutný dodatočný krok externého schvaľovacieho procesu od externej zodpovednej organizácie. (stanovené podľa ISO 9000)

4. **Použitie –** Fáza použitia dokumentu začína uvoľnením schváleného dokumentu do systému využívania. Znamená to, že dokument môže byť použitý pre sledovaný účel.
5. **Revízia –** Vo fáze revízie sa mení a prispôsobuje obsah dokumentu tak aby nasledoval vývoju procesov a činnostiam užívateľov, ktorí s ním pracujú.
6. **Archivácia** - Po určitom čase každý dokument dokončí svoj účel a stáva sa nepoužiteľným. V takom prípade sa stiahne. Dokument sa však musí v každom prípade po dlhšiu dobu uchovávať, ako archívny. Dobu archivácie stanovujú právne požiadavky, no vzniknú sa značne meniť. Minimálna právne vyžadovaná doba archivácie (často najmenej 10 rokov) sa môže odlišovať aj podľa podmienok kontraktov. Z dôvodu dlhodobého uchovávania a opätovného využívania dokumentov a informácií by sa mali informácie zbavovať logických závislosti a väzieb na fyzických osobách, ktoré ich vytvorili a rovnako na technickej báze ich tvorby (SF,HW,pamäťové médium). Na technickej úrovni sa musí zabezpečiť vyhľadávanie a výber použitím stálych formátov dát a médií. Dáta preto musia byť často transformované do odlišnej skladby formátu kvôli prispôsobeniu sa novým technickým prostriedkom. Metadáta musia byť doplnené zvlaštnymi metadátami spojenými s procesom archivovania.
7. **Stiahnutie a odstránenie** - Vyradenie a odstránenie dokumentu z archívu znamená, že sa dokument vrátane jeho pridružených metadát vyradí a už ďalej nebude sledovaný ani fyzicky ani logicky. (7)



Obrázok 9-Činnosti v priebehu životného cyklu dokumentu v DMS, Zdroj:Vlastné spracovanie podľa (7)

4.5 Zálohovanie dokumentov

Popri dlhodobej, často zákonom nariadenej archivácii dokumentov, ktorá slúži pre opätovné zistenie v akom stave boli dáta v určitom minulom okamihu, existuje ešte zálohovanie dokumentov. Pojmy sú napriek ich odlišnému významu často zamieňané. Význam zálohovania je totiž vytváranie tzv. živej kópie dát, ktorá slúži pre okamžité obnovenie potrebných dát v prípade ich straty, výpadku systému alebo iného poškodenia. Záloha sa môže vytvárať automaticky alebo manuálne, najideálnejšie v pravidelných intervaloch. Zálohou sa rozumie taká kópia dát, ktorá je uložená na odlišnom médiu než pôvodné dáta. Tieto média bývajú najčastejšie: (6)

- Optické médiá – CD,DVD – rýchle, cenovo nenáročné riešenie s pomerne krátkou životnosťou
- Pamäťové karty a flash pamäte – ľahká prenositeľnosť, nízka cena, obmedzený počet zápisov, náchylnosť, krátkodobosť
- Pevné disky a ich zapojenie do viacnásobných diskových polí (RAID) – vysoká kapacita, rýchlosť, spoľahlivosť proti fyzickému zlyhaniu pevného disku (RAID),
- Pásky – nižšie náklady než pevné disky, extrémna životnosť, odolnosť a vysoká kapacita, automatické zálohovanie serverov sieťovo pripojených na páskové zariadenie.

Systém, akým sa dáta a dokumenty v stanovených intervaloch na úložné médium ukladajú, závisí od zvoleného zálohovacieho spôsobu: (6)(28)

- *Plná záloha* – Pri každom prevedení sa vytvára plná kópia dát, nezávislá od tej predchádzajúcej. To vyvoláva najväčšie kapacitné nároky a preto sa zvykne používať len v úvode zálohovania a na ňu nadväzujú inkrementálne alebo rozdielové zálohy.
- *Inkrementálna záloha* – pri zálohe sa zaznamenávajú len zmeny, ktoré vznikli od predchádzajúcej inkrementálnej zálohy. Je preto najviac kapacitne úsporná, no pri potrebe obnovy systému je potrebná prvá plná záloha a na ňu chronologicky nadväzujúce všetky inkrementálne zálohy. Keďže sú medzi sebou navzájom závislé, v prípade poškodenia jedenej z nich vznikne problém s nadväznosťou tých nasledujúcich.
- *Rozdielová záloha* – Zaznamenáva zmeny vzniknuté od poslednej plnej zálohy. Jednotlivé rozdielové zálohy nie sú teda na sebe závislé, a v prípade poškodenia sa neovplyvnia. Pri obnove je potrebná posledná plná záloha a posledná rozdielová záloha.

4.6 Správa podnikového obsahu

Pod pojmom podnikový obsah rozumieme všetky informačné zdroje, ktoré sa vyskytujú v podniku bez ohľadu na ich formu (elektronické alebo listinné dokumenty) a formát (text, obraz, zvuk, atď). Kvantitatívny nárast objemov získavaných dát vplyvom dnešnej informatizácie je natoľko výrazný, že bez kvalitatívnej zmeny spracovávania dát by bol neúnosný. Väčšia kvantita prijímaných dát nám totiž neprinesie žiadnu kvalitatívnu výhodu, pokiaľ nemáme dostatočné vhodné prostriedky na ich spracovávanie a spravovanie. Práve z tohoto dôvodu sa zvýšil záujem o aplikácie pre správu podnikového obsahu ako je napríklad Document Management System (DMS), ktoré vyššiu kvalitu spracovávania informácií môžu poskytnúť. (8)(27)

Všeobecne sa teda správa podnikového obsahu (Enterprise Content Management-ECM) chápe ako stratégia, postupy alebo nástroje slúžiace k získavaniu, riadeniu, spracovávaniu, zdieľaniu a distribúcii obsahu a dokumentov vzťahujúcich sa k podnikovým procesom. (8)

Elektronické informácie, ktoré majú svoju pevnú štruktúru sú pre výpočtovú techniku veľmi ľahko zvládnuteľné.Význam takýchto dát je daný a popísaný ich štruktúrou a preto ich počítačové spracovanie môže byť podporované veľkým množstvom aplikácií. Hovoríme tu

napríklad o účtovníckych aplikáciách alebo aplikáciách pre správu majetku. V bežnej organizácii sa však mnohonásobne viac vyskytujú neštruktúrované dáta (napr. Texty, obrázky, grafy, prezentácie, atď), ktoré sú pre jej činnosť nevyhnutné a nedokážu byť spracovávané bežnými aplikáciami transakčného charakteru ako napríklad spomínané účtovníctvo. (8)

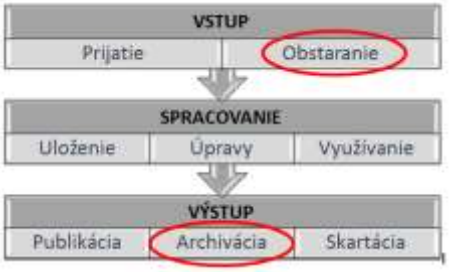
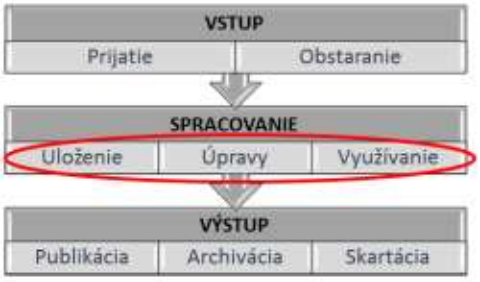
Práve kvôli neštruktúrovaným dátam vznikli aplikácie pre správu podnikového obsahu. Tieto aplikácie umožňujú neštruktúrované dáta charakterizovať a popísať ich tzv. metadátami, čo im umožní s nimi ďalej efektívne pracovať. Podľa normy ČSN EN 82045-1 charakterizujeme metadáta ako popisné dáta pre správu dokumentov, resp. dáta o obsahu dokumentu, potrebné pre jeho spravovanie v elektronickom systéme správy dokumentov DMS alebo v akomkoľvek inom platnom systéme. (8)

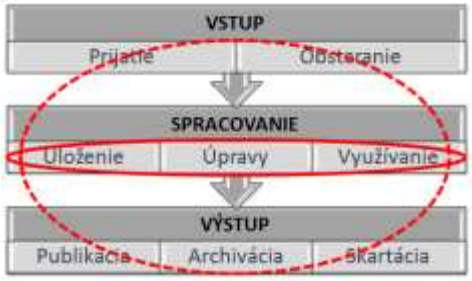
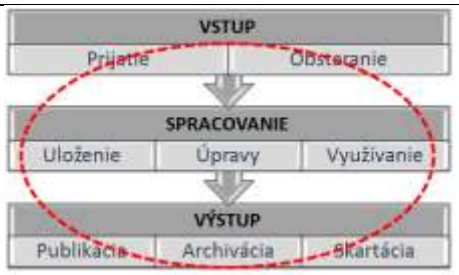
4.6.1 Architektúra systémov pre správu podnikového obsahu

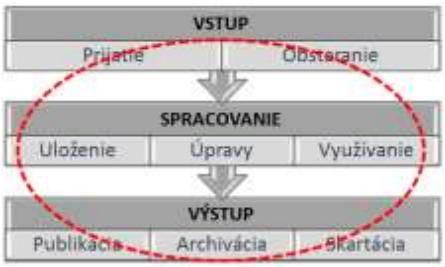
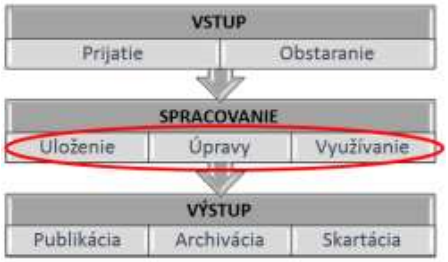
Pri spätnom pohľade na vývoj aplikácií v oblasti správy obsahu je zrejmé, že ECM predstavuje do istej miery len zastrešenie pre už existujúce samostatné aplikácie so špecifickými funkciami. Tieto aplikácie sa špecializovali len na jednu funkciu ako napríklad aplikácia pre digitalizáciu dokumentu, aplikácia pre workflow alebo aplikácia pre správu dokumentov. Prirodzenou snahou o efektívnejšie uspokojovanie zákazníckych potrieb sa začali tieto funkcionality rozširovať, resp. spájať do jednej aplikácie a do jedného produktu. (8)

Aby tieto systémy zabezpečili skutočne efektívnu správu dokumentov, musia byť stanovené presné pravidlá a procesy pre zaobchádzanie s dokumentami, ktoré budú zahrňovať ich celý životný cyklus. ECM teda v dnešnej podobe pozostáva z viacerých komponent, ktoré je možné odlíšiť ich rozdielnou funkcionalitou a pokrytím rozdielnych častí životného cyklu podnikového obsahu. V nasledujúcej tabuľke sú komponenty bližšie popísané. V rozličných literatúrach sa uvádzajú rôzne preklady uvedených komponent, preto z dôvodu lepšej prehľadnosti je pod slovenským názvom vždy uvedený aj anglický názov. (8)

Tabuľka 6- Základné komponenty ECM, Zdroj:Vlastné spracovanie podľa (8)

Názov komponenty	**Hlavný účel komponenty**	**Pokrytie fázy životného cyklu podnikového obsahu**
Digitalizícia dokumentov Imaging	Prevod listinných dokumentov do elektronickej podoby, či už do podoby editovateľného elektronického súboru alebo do formátu obrázku.	
Vyťahovanie dát Data Capture	Automatizované získavanie štruktúrovaných dát z rôznych listinných dokumentov a zabezpečenie ich uloženia do databázy.	
Systém pre správu dokumentov Document Management System	Integrované, centralizované úložisko dokumentov. Umožňuje viacnásobný užívateľský prístup k dokumentom, ich spracovávanie, manipuláciu s nimi a riadenie.	
Správa záznamov Records Management	Systematická kontrola vytvárania, prijímania, správy, údržby a sprístupňovania záznamov. Záznam sa chápe ako doklad o tom, čo spoločnosť robí, vrátane všetkých obchodných aktivít, firemnej korešpondencie, osobných súborov atď…	

Správa elektronickej pošty E-mail Management	Triedenie a presúvanie elektronických správ vrátane priložených súborov z osobných elektronických poštových schránok zamestnancov smerom do centralizovaného úložiska. Následne sa tieto získané informačné zdroje stanú zdieľané.	
Archivácia Archiving	Dôveryhodné a bezpečné uloženie dokumentov, ich spracovanie, sprístupňovanie a následné vyraďovanie podľa stanovených podmienok.	
Automatizácia procesov Workflow	Automatizácia procesu alebo jeho časti, behom ktorého sú informácie, dokumenty alebo úlohy zadávané naprieč organizáciu od jedného zamestnanca k druhému podľa požadovaných pravidiel príslušného procesu.	
Tímová spolupráca Groupware	Zabezpečenie komunikácie a spolupráce ľudí na spoločnom cieli ako aj koordinácie jednotlivých aktivít k jeho dosiahnutiu.	
Správa webového obsahu Web Content Management	Tvorba, schvaľovanie a automatické zverejňovanie informácií rozličnými informačnými kanálmi ako sú internet, intranet, extrane atď…	

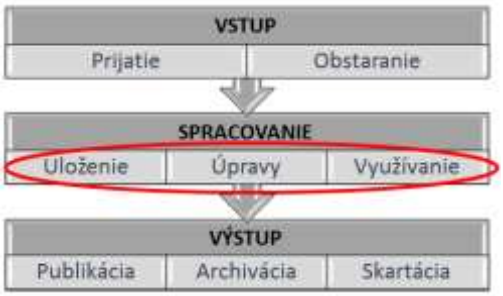
Správa znalostí Knowledge Management	Priebežné získavanie, spracovávanie, zdieľanie, využívanie a rozvíjanie znalostí pracovníkov a skupín pracovníkov s cieľom ich kontinuálneho zvyšovania podnikovej výkonnosti a efektívnosti.	
Správa multimediálneho obsahu Digita Asset Management	Vkladanie, triedenie, vyhľadávanie, ukladanie a zabezpečovanie prístupu ku všetkým formám multimediálnych dát.	

Diplomová práca sa bližšie zaoberá komponentou Systému pre správu dokumentov- DMS a preto podrobnejšia charakteristika ostatných komponent ECM nie je obsiahnutá v tejto práci. Pre podrobnejší popis viď. (8)

4.6.2 Systém pre správu dokumentov - DMS

DMS systém sa v rámci ECM považuje za akési jadro riešenia, pretože práve on zastrešuje centrálnu fázu životného cyklu podnikového obsahu. DMS predstavuje centrálne úložisko podnikových dokumentov a dát s rôznym typom formátu a poskytuje ich ostatným ECM komponentám, ostatným podnikovým aplikáciám ako aj všetkým oprávneným užívateľom. Prístup k potrebným dokumentom, ktorý poskytuje, musí byť bezpečný a okamžitý. (2) (8)

Ako už bolo spomenuté, DMS pokrýva fázu spracovania v rámci životného cyklu podnikového obsahu. Znamená to, že dokumenty sa v systéme nevytvárajú ale vstupujú už hotové, čím sa DMS líši od ostatných komponent ECM. Systém umožňuje prácu s dokumentami ako s celkom, riadenie prístupu k nim, používanie a ukladanie a všetky tieto činnosti automaticky sleduje a riadi. Nemá však na starosti prácu s obsahom súboru. (2) (8)



Obrázok 10- Pokrytie fázy životného cyklu podnikového obsahu komponentou DMS, Zdroj:Vlastné spracovanie podľa (8)

4.6.2.1 Prínosy DMS

Rastúce množstvo dokumentov v každej jednej spoločnosti je prirodzenou odozvou na informatizáciu našej spoločnosti. Pokiaľ firma nechce zaostávať, zisťuje, že efektívnym zaobchádzaním s dokumentami všetkých druhov je možné zjednodušiť a hlavne zrýchliť firemné procesy, čo vedie k úsporám, ako časovým tak aj finančným. Až keď má človek veci pod kontrolou, môže ich efektívne riadiť. Mnohé firmy sa preto v snahe riadiť dokumenty schyľujú k najjednoduchším riešeniam a využívajú napríklad zdieľanie adresárov na súborových serveroch. Pravidlá o ukladaní, pomenovávaní a práci s dokumentami sú predávané často len ústne medzi zamestnancami, čomu zvyčajne vďačí vzniknutý chaos. Príklady možných problémových situácií v podnikoch a spôsobov ich riešenia vďaka systémom DMS je uvedený v nasledujúcej tabuľke: (2) (8)

Tabuľka 7 - Výhody DMS, Zdroj:Vlastné spracovanie podľa (2) (8)(27)

Problém v organizácii	Riešenie pomocou DMS
Plytvanie času pri vyhľadávaní uložených dokumentov	– Efektívne vyhľadávanie a výber určitých dokumentov vďaka systému tvorby metadát,
Strata času v dôsledku použitia nesprávnej verzie dokumentu	– Rýchle a priame premietanie zmien vďaka systému verzovania
Nedostatočná komunikácia medzi jednotlivými oddeleniami spoločnosti	– Podpora centrálnej výmeny a centrálneho zdieľania dát – Podpora spolupráce pri procesoch
Nesprávne rozhodnutia na základe neznalosti existencie dokumentu	– Jediné centrálne úložisko dokumentov pochádzajúcich zo všetkých podnikových procesov a aplikácií – Metadáta – Offline režim – Aplikácia formou webového rozhrania
Nedostatočná evidencia kópií dokumentov, nedostupnosť dokumentov	
Zbytočné zaberanie pamäťového priestoru z dôvodu duplikácii dokumentov	
Nedostupnosť dokumentov pre potrebu ich mobilného využívania	
Nedostatočné plnenie zákonných požiadaviek na prácu s dokumentami	– ČSN EN 82045-1 norma od Českého normalizačného inštitútu presne popisuje zásady a metódy pri spáve dokumentov v systémoch pre správu dokumentov
Zbytočné časové a finančné náklady vznikajúce neefektívnou činnosťou	– Zredukovanie administrácie vplyvom integrácie produkovania a správy dokumentov, – Automatizácia pracovných postupov

4.6.2.2 Základné princípy a funkcie DMS

Existujú všeobecné princípy, na základe ktorých sa vytvárajú systémy pre správu obsahu: (8)

- Súbor, resp. dokument sa v DMS vyskutuje len jedenkrát aj keď užívatelia k nemu môžu pristupovať z rôznych adresárov.
- DMS vystupuje ako centrálne úložisko dokumentov a sústreďujú sa v ňom dokumenty zo všetkých aplikácií, ktoré organizácia využíva.
- DMS je previazané s kancelárskymi aplikáciami typu MS Word, MS Excel, z ktorých je nasmerované ukladanie dokumentov priamo do DMS
- Elektronické dokumenty sú do DMS ukladané formou formulárov, ktoré okrem daného dokumentu obsahujú aj nevyhnutné informácie o dokumente a umožnia evidovať a manipulovať s dokumentom, tzv. metadáta.

Hlavné funkcie systémov pre správu obsahu sa dajú kategorizovať nasledovne: (8)

- **Dokumentačné funkcie** - prehliadač dokumentov, uzamykanie, správa verzií, sledovanie histórie a väzieb medzi dokumentami, riadenie zmien, tvorba statických aj dynamických zložiek a dokumentov
- **Užívateľské funkcie** - prístup cez webovú aplikáciu, personálne prispôsobenie užívateľského prostredia, offline režim
- **Integračné funkcie** - intergácia s firemnými aplikáciami, s firemnou poštou a firemnou administratívou
- **Bezpečnostné funkcie** - prístupové práva, správa užívateľov, centrálna správa súborov
- **Vyhľadávacie a identifikačné funkcie** – vyhľadávanie dokumentov pomocou metadát alebo fulltextové vyhľadávanie, systém tvorby metadát

Systém tvorby metadát spĺňa v prostredí DMS veľmi významnú funkciu. Štruktúrovaným spôsobom totiž charakterizujú neštruktúrované dokumenty, čo umožňuje ich vyhľadávanie či analytické spracovávanie a tak zvyšujú celkovú hodnotu dokumentu. Tvorba metadát je preto hlavnou zásadou správy dokumentov, ktorú popisuje norma ČSN EN 82045-1, ktorá je českou verziou európskej normy EN 82045-1:2001. Norma vysvetľuje, čo všetko môže byť za metadáta považované aj ako rozličným spôsobom pripojenia metadát k dokumentom rozlišujeme medzi jednotlivými, kombinovanými, zoskupenými a súborovými dokumentami. (7)

Uvedená norma správy dokumentov definuje aj kritéria pre tvorbu verzií dokumentov. Verzia dokumentu je definovaná ako určitý stav dokumentu v jeho životnosti zaznamenaný tak, aby ho bolo možné vyhľadať ako záznam alebo použiť k distribučným účelom. V praxi sa rozlišujú postupne alebo súbežne účinné verzie (pre viac informácií viď. (7))

4.6.3 Dostupné systémy DMS

Situácia na súčasnom trhu so systémami DMS alebo všeobecne ECM systémami odráža zvýšený dopyt po týchto produktoch. Ako už bolo viackrát spomenuté, organizácie sú konkurenčne tlačené do zvyšovania efektívnosti svojej činnosti, do zvyšovania kvality. A implementácia systému pre správu a riadenie podnikového obsahu je jednou z ciest, po ktorej sa musia skôr či neskôr vydať. Situácia na trhu ECM systémov z októbra 2015 vyzerá podľa

agentúry Gartner nasledovne. Agentúra mapuje schopnosť podnikov spĺňať potreby zákazníka, tvoriť zmysluplné vízie a schopnoť realizovať ich. (9)

Obrázok 11 - Situácia na trhu ECM, Zdroj: (9)

Z predchádzajúcich hodnotení je možné určiť za najväčších hráčov na trhu systémov pre správu podnikového obsahu spoločnosti IBM, Microsoft, EMC alebo Oracle. Čo sa týka produktov čisto zameraných len na komponentu správy a riadenia dokumentov, pohybuje sa podľa agentúry G2Grid produkt Sharepoint na trhu s konkurenčnými produktami Evernote, Brandfolder a eFax. (10)

Uvedený náhľad produktov a firiem pôsobiacich na trhu v oblasti ECM a DMS je v tejto práci použitý hlavne pre predstavu aktuálneho vývoja konkurenčnej situácie. V oblasti tak širokej a pestrej ponuky produktov je ťažké robiť jednoznačné objektívne závery a vyhodnocovať najlepšie produkty, kedže každý zákazník využíva produkt veľmi individuálne

a kustomizovane. Táto práca sa však bude zaoberať podrobnejšie implementáciou produktu SharePoint Online od Microsoftu a preto je v nasledujúcej kapitole podrobnejšie popísaný práve tento produkt.

4.6.4 Microsoft Sharepoint 2013

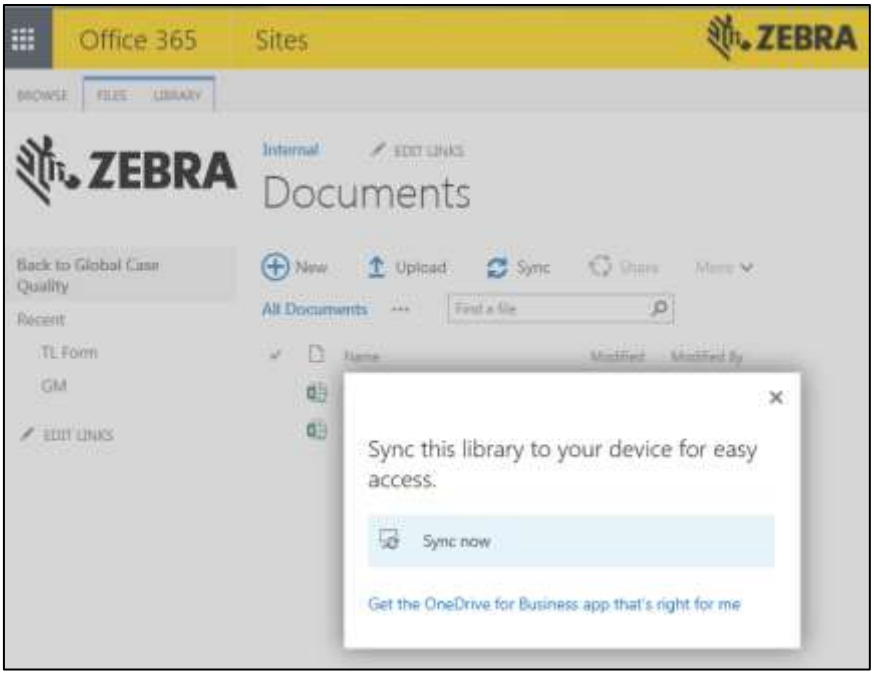
Systém pre správu podnikového obsahu SharePoint od spoločnosti Microsoft býva predstavovaný ako vrchol kancelárskeho balíku MS Office. Systém vychádza z hlavnej myšlienky umožniť centralizovane ukladať, spravovať, organizovať a zdieľať dokumenty zo všetkých aplikácií a nástrojov v MS Office (Word, Excel, PowerPoint, Visio, Outlook, Access,…). A to všetko prostredníctvom jedinej webovej aplikácie a internetového prehliadača, ktorý umožní aj netechnicky zameraným užívateľom budovať pomerne jednoducho a rýchlo webové stránky bez potreby hlbšieho skúmania systému. Cieľom SharePointu je navyše umožniť užívateľom pokračovať a rozvíjať prácu s dokumentami priamo v prostredí webu. (11)

4.6.4.1 Funkcionality systému

V tejto podkapitole budú priblížené funkcionality systému SharePoint, ktoré sú z hľadiska ich využitia zaujímavé pre sledovanú servisnú pobočku.

OneDrive

Technológia OneDrive umožní užívateľom lokálne si ukladať potrebné knižnice dokumentov zo SharePointu, lokálne s nimi zaobchádzať podľa pridelených prístupových práv, zdieľať nové alebo existujúce dokumenty s ostatnými a čo je najpodstatnejšie, offline prístup v prípade nedostupnosti internetu alebo Sharepointu. Zmeny, ktoré vykoná užívateľ v offline režime sa navyše vždy po pripojení do systému automaticky synchronizujú, takže užívateľ nemusí vynakladať čas a úsilie na pravidelnú aktualizáciu. Zdieľané priečinky navyše nenavyšujú diskovú kapacitu zdieľajúcich užívateľov, zaťažujú len vlastníka zložky. (12)

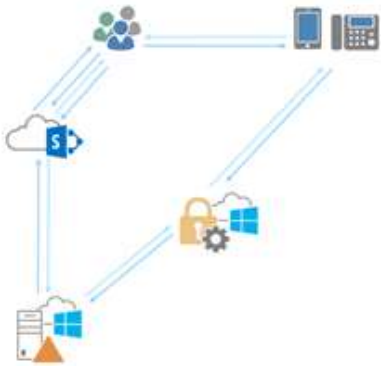


Obrázok 12- Systém zdieľania dokumentov technológiou OneDrive, Zdroj: (12)

Po nazdieľaní konkrétnej zložky dokumentov sa zobrazia súbory vo Windows Exploreri a užívateľ s nimi pracuje ako s tradičnými lokálnymi dokumentami.

Viac-faktorová autentifikácia

Technológia, ktorá vytvára viacnásobné overovanie užívateľského prístupu do Sharepointu. Návrhom v tejto práci je preto zabezpečiť 2-faktorovú autentifikáciu užívateľov. Tí sa teda po zadaní prístupového hesla do systému musia legitimovať ešte raz. Logickou možnosťou sú v podobných prípadoch špecifické informácie, ktoré vie len užívateľ, doklad o niečom, čo vlastní len užívateľ alebo nejaký fyziologický prvok (odtlačok prsta,…). Konkrétne zabezpečovacie riešenia sú napríklad HW/SW jednorázové heslo, telefonát, SMS, PKI certifikát, Smart karty s PKI, biometrické zabezpečenie, atď. Systém autentifikácie je znázornený na nasledujúcom obrázku: (13)



1.Žiadosť o prístup do aplikácie
2. Vyžiadané overovacie údaje
3. Overovacie údaje prijaté
4. Druhý faktor cloudového servisu skontaktovaný
5. Klientov druhý faktor doručený
6. Klient prezentuje druhý faktor
7. Overenie klienta
8. Aplikácia prístupná

Obrázok 13 - Dvoj-faktorová autentifikácia prístupu do SharePointu, Zdroj: (13)

Management prístupových oprávnení RMS

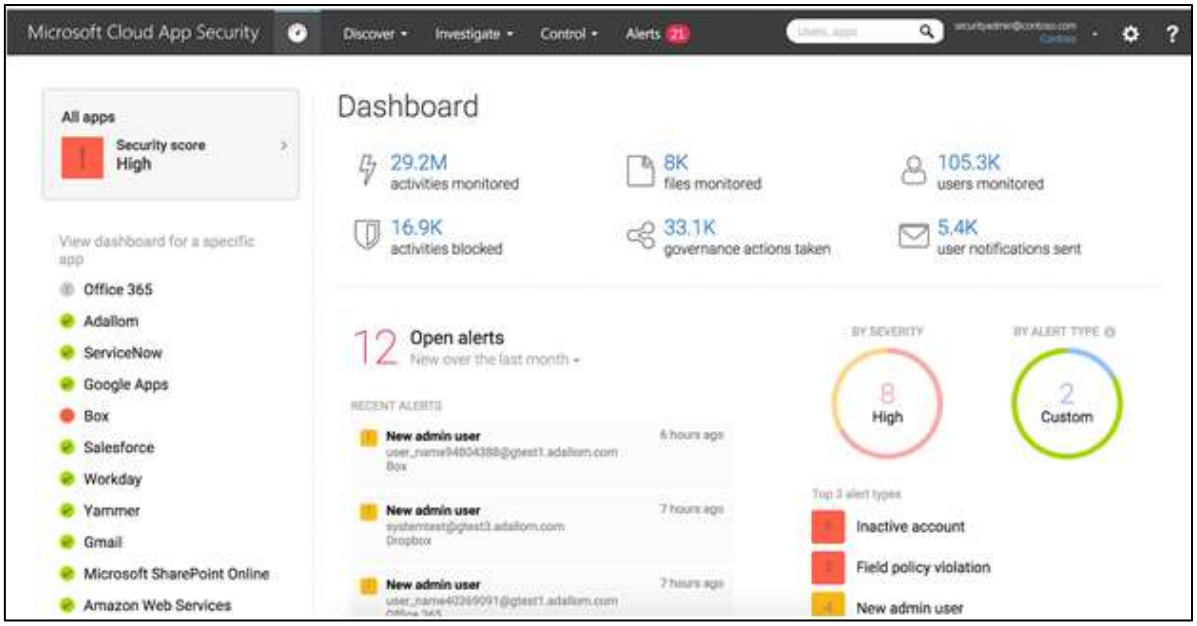
Systém Microsoft Azure Rights Management je riešenie pre ochranu potrebných zdieľaných dokumentov a informácií, pričom nijako neobmedzuje hlavnú výhodu cloudového riešenia a teda priestorovo aj hardwarovo flexibilný prístup k systému. Dokáže teda zlúčiť efektívnosť a bezpečnosť manipulácie s dôležitými dokumentami. (14)

Veľkou bezpečnostnou výhodou je skutočnosť, že zabezpečenie konkrétnych dokumentov s nimi ostáva späté aj mimo materskú organizáciu, takže ochrana pred neoprávneným čerpaním informácií dostáva úplne nový rozmer. Neautorizovaná osoba, či už interná alebo externá, dokument neotvorí. (14)

SECaaS

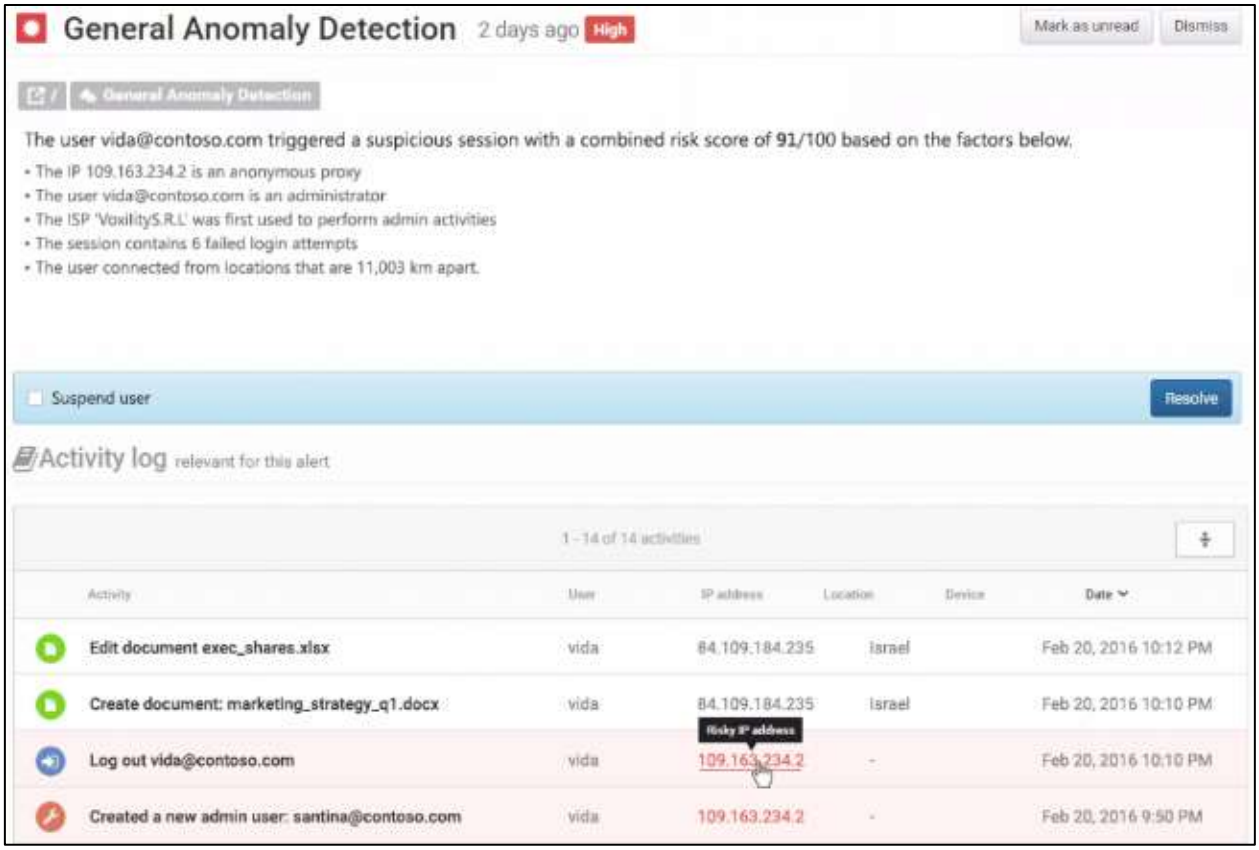
Aplikáciu Microsoft cloud app Security je možné zaradiť do novovznikajúceho servisného modelu SECaaS (Security as a service- Bezpečnosť ako služba). Táto služba formou softwarovej technológie poskytuje vyššiu viditeľnosť do cloudových aplikácií, komplexný kontrolný mechanizmus a rozšírený systém ochrany aplikácií. Sprostredkované služby sú rozdelené do 4 kľúčových konzol: (15)

- **Objavovať**- sleduje a vyhodnocuje rizikovosť všetkých cloudových aplikácií- schválených aj neschválených, IP adresy, ktoré sa na ne prihlasujú, analyzuje rizikovosť na základe získaných informácií z Firewall a Proxy serverov.



Obrázok 14 - Cloud App Security, Zdroj: (15)

- **Vyšetrovať** - zaznamenáva anomálie v cloudovom prostredí.
- **Kontrolovať/Auditovať**- možnosť vybrať si prednastavené šablóny politík a smerníc, prípadne si vytvoriť vlastné pravidlá a na základe nich aplikácia kontroluje správanie sa užívateľov, vyhodnocuje a zobrazením logov upozorňuje na podozrivé správanie sa užívateľov.
- **Oznamovať**- priebežný systém výstrah a oznámení o využití cloudovej kapacity, download, upload, najaktívnejších užívateľov. (15)



Obrázok 15 - Automatická detekcia v prostredí Cloud App Security, Zdroj: (15)

4.6.4.2 Dostupné verzie a platformy systému MS Sharepoint

Poslednou verziou systému je momentálne Microsoft SharePoint 2013. Jeho jediná integrovaná platforma dokáže zabezpečiť internetové, intranetové ako aj extranetové využívanie s platným pravidlom, že externí užívatelia licencie nepotrebujú platiť. Systém je možné zakúpiť v rôznych typoch licencií, ktoré závisia od želaných funkcií, spôsobu nasadenia a formy hostovania, pričom cena sa vždy viaže na počet užívateľských prístupov. (16)

- SharePoint – Online s cloudovým riešením, cena v závislosti od počtu užívateľov
- SharePoint – On-Premise, lokálne využitie s riešením klinet-server. Ku každému Sharepointovému softwaru je preto ešte potreba licenie k SharePoint Serveru 2013

Tabuľka 8- Dostupné licencie lokálneho softwaru MS SharePoint 2013, Zdroj: (16)

	SharePoint On-Premise	SharePoint Online
Výhody	SharePoint server je v internej korporátnej sieti Technické funkcie - full text dotazy, SQL, LDAP, Kontrola vlastnej výkonnosti Užívateľsky prispôsobivy a flexibilný	Dostupnosť 99,99% Uloženie dát v rôznych dátových centrách Geografická redundancia Správa a servis od profesionálneho poskytovateľa Automatický update Paušálne náklady, flexibilne prispôsobiteľné Nízke požiadavky na kvalifikovaný IT personál Rýchle zavádzanie Škálovateľnosť Lacné úložisko veľkých objemov dát
Nevýhody	Vysoké náklady na vlastné interné zdroje- Dodatočné náklady na geografickú redundanciu Nutnosť interného krízového plán Náročnejšia konfigurácia pre externú Vyššie jednorázové náklady Spoľahnúť sa len sám na seba	Závislosť od poskytovateľa Limitovaná kustomizácia Riziká plynúce z SLA zmlúv a legislatívy poskytovateľa Závislosť od internetového pripojenia Bezpečnostné riziká narušenia DID Chýbajúci prístup k serveru Limitované aplikácie, analýzy, funkcionalita Limitované administrátorské oprávnenia

Investíciou do SharePointu sa podnikom naskytajú možnosti využitia širokej škály funkcií, nie len základných komponent DMS systému, ale aj správa webového obsahu, workflow, tvorba vlastných podnikových aplikácií, tvorba reportov, komunikačná platforma a predovšetkým maximálna kompatibilita s nástrojmi z MS Office. MS Sharepoint 2013 môžeme svojou funkcionalitou preto zaradiť medzi systémy pre správu celopodnikového obsahu- ECM. (16)

4.7 Cloud Computing a virtualizácia

Spomenutá Online verzia systému SharePoint využíva pre svoje služby technológiu Cloud Computing (skr. CC). Pod výrazom Cloud Computing sa rozumie model, ktorý na požiadanie zabezpečuje sieťový prístup k zdieľaným výpočtovým zdrojom (sieť, servery, úložiská, aplikácie či služby). Tieto zdroje môžu byť užívateľovi poskytnuté s minimálnymi nárokmi na jeho interakciu s poskytovateľom, či na riadiace činnosti so strany užívateľa. Cloud Computing využíva technológiu virtualizácie. (6) (17)

Virtualizácia predstavuje využitie zvyčajne vysokokapacitných hardwarových prostriedkov hostiteľského stroja(tzv. Hypervisor) pre jeden alebo viac hostovoaných strojov (tzv. Virtual Machine- VM), čo teda zjednodušene znamená prevádzkovať na jednom fyzickom počítači

viaceré virtuálne počítače. Predpokladá sa pritom dostatočný hardwarový výkon hostiteľa, aplikácie zabezpečujúce samotnú virtualizáciu a záväzné licenčné pravidlá. (6) (17)

4.7.1 Modely nasadenia CC

- Privátny cloud – cloudová infraštruktúra je navrhnutá a poskytnutá jednej organizácii. Infraštruktúra je organizáciou vlastnená, riadená alebo spravovaná
- Verejný cloud – Infraštruktúra je poskytnutá na voľné použitie verejnosti
- Hybridný cloud - Kombinácia dvoch a viacerých predchádzajúcich modelov
- Komunitný cloud –Infraštruktúra je poskytnutá na výlučné použitie organizáciami, ktoré spolu zdieľajú záujmy- (17)

4.7.2 Servisné modely CC

- SaaS – Užívateľ má možnosť využívať aplikácie poskytovateľa s jeho HW aj SW infraštruktúrou. Užívateľ v takomto prípade nemá možnosť riadiť server, úložiská, operačný systém, sieť a aplikáciu len v obmedzenej miere
- PaaS – Užívateľovi sa oproti prechádzajúcemu modelu zvyšuje možnosť kompletného ovládania alebo návrhu aplikácie a konfigurácií
- IaaS – Kontrola užívateľa nad operačným systémom, dátovým úložiskom, aplikáciám a limitovaná kontrola výberu sieťových prvkov (napr. hostované Firewally). (17)

4.7.3 Bezpečnostné hrozby plynúce z technológie Cloud Computing

Keďže je technológia Cloud Computing založená na virtuálnom prostredí, je potrebné okrem vlastných hrozieb tejto technológie zvážiť ešte hrozby virtualizácie ako takej. Tieto spoločné hrozby sú za každých okolností dodatočné k bežným hrozbám, vplývajúcim na dáta v nich uložené a v prenesenom význame teda aj na dokumenty uložené v podnikových informačných systémoch. (6)

Tabuľka 9 - Bezpečnostné hrozby informácií, Virtualizácie a Cloud Computingu, Zdroj: Vlastné spracovanie podľa (6)(28) (29)

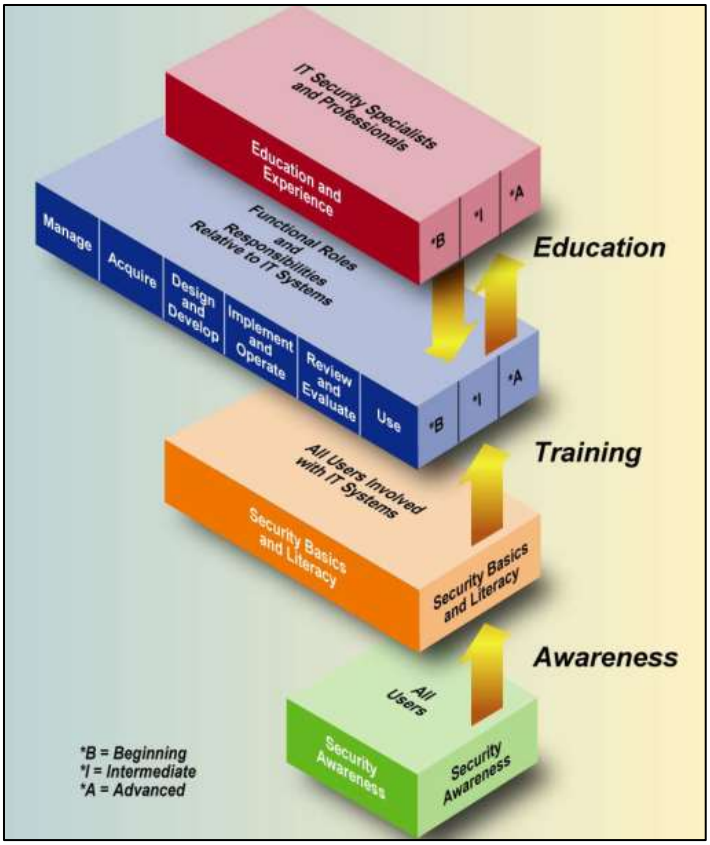
Bezpečnostné hrozby informácií - dokumentov		
Narušenie dôvernosti	Prístup k informáciám neoprávneným užívateľom	
Narušenie dostupnosti	Znemožnenie prístupu oprávnených užívateľov k informáciám v požadovanom okamžiku	
Narušenie integrity	Narušenie správnosti a úplnosti informácií	
+ Bezpečnostné hrozby Virtualizácie		**+Bezpečnostné hrozby CC**
Slepé miesta komunikácie	Tradičné sieťové zabezpečenia nesledujú komunikáciu medzi VM na jednom hostiteľskom Hypervisorovi	**Verejné cloudové prostredie zdieľané rôznymi nájomníkmi**
Vzájomné útoky medzi VM	V prípade absencie virtualizačných zabezpečení sa nákaza z jedného VM šíri do ostatných VM	**Nešifrované dáta alebo komunikácia, Pohyblivosť dát medzi rôznymi datacentrami**
Rôzne úrovne dôveryhodnosti VM	Kritické a nedôležité dáta môžu byť na jednom hostiteľovi	**Legislatívne rozdiely medzi poskytovateľom a užívateľom**
Zraniteľnosť pri spúšťaní strojov	Nárazové aktivácie a deaktivácie VM spôsobujú oslabenie	**Prístup z nezabezpečených prístrojov**
Súperenie o prostriedky Hypervisora	Hromadné požiadavky napr. na aktualizácie spôsobujú extrémne zaťaženie systému	**Dostupnosť v závislosti od poskytovateľa alebo internetového pripojenia**

4.7.4 Bezpečnostné opatrenia v rámci technológie Cloud Computing

Opatrení, ktoré umožnia eliminovať negatívne dopady hrozieb uvedených v predchádzajúcej tabuľke, je celá rada ale nie je v rozsahu tejto diplomovej práce venovať sa všetkým podrobnejšie. (v prípade zájmu viď (6)) V práci budú použité len niektoré z nich a preto pre lepšie pochopenie problematiky budú ešte charakterizované nasledovné pojmy s nimi súvisiace:

- **Business Continuity Management – BCM** – riadiaci proces iniciovaný vedením spoločnosti, ktorého cieľom je vytvoriť plán činností, ktoré v prípade výpadku systému umožnia zaistiť kontinuity a obnovu kľúčových procesov spoločnosti. Plán teda zastrešuje záujmy všetkých podnikových stakeholderov. Presné definície a postup vytvorenia takéhoto plánu je definovaný normami ČSN ISO/IEC 27001 a NIST 800-34. (18)

- **Riadenie prístupu –** základné princípy riadenia prístupu do systému sa podľa normy ČSN ISO/IEC 27001 riadia nasledovnými základnými princípmi:
    - **Identifikácia –** systémové rozpoznanie entity
    - **Autentifikácia –** overenie identity entity
    - **Autorizácia –** proces overovania oprávnení pre vstup do systému (6)
- **Viac-faktorová autentifikácia – u**žívateľ pre prístup do systému zadá okrem uživateľského mena a hesla ešte minimálne jeden ďalší overovací parameter. Faktory by mali zastrešovať niečo, čo vie len oprávnená osoba (heslo) a niečo čo má len oprávnená osoba (karta, čip, mobil), prípadne dôkaz, kým je oprávnená osoba (odtlačok prstu). (6)
- **Audit -** nezávislý, systematický a dokumentovaný proces objektívneho hodnotenia objektov alebo subjektov podľa predom nastavených kritérií. (6)
- **Security Awareness Education - SAE –** program budovania informačného bezpečnostného povedomia a tréningového programu, ako súčasť bezpečnostného programu informačných technológií v podnikoch. Progam by mal byť kontinuálny a jeho obsah pravidelne odovzdávaný cieľovým skupinám. Norma NIST SP-800-50 definuje jednotlivé kroky návrhu, tvorby aj aplikácie tohto programu. Program rozdeľuje postupne do častí povedomie(Awareness), tréning(Training) a vzdelávanie(Education), viď. nasledujúci obrázok. Vrámci každej časti rozlišuje norma cieľovú skupinu užívateľov, na ktorých by mal byť program aplikovaný. Povedemie sa spravidla buduje u všetkých zamestnancov, tréning sa rozlišuje podľa stupňa pokročilosti a funkčného zamerania a vzdelávací program sa špecializuje len na odborníkov danej oblasti. (19)



Obrázok 16 - Postup budovania bezpečnostného vzdelávacieho programu, Zdroj: (19)

4.8 Projekt a projektové riadenie

4.8.1 Základné definície

Uskutočňovanie zmeny môže byť v podnikoch riešené formou projektu. Týmto pojmom sa rozumie jedinečný, časovo, zdrojovo a nákladovo obmedzený proces uskutočňovaný za účelom dosiahnutia konkrétneho výstupu, v požadovanej kvalite a za splnenia stanovených požiadaviek. (20)

Typickou charakteristikou projektov je snaha o naplnenie stanoveného cieľa. Ten sa určuje na začiatku projektu a ideálne spĺňa tzv. SMARTcharakteristiky:

- S – špecifický
- M - merateľný
- A – prijateľný/odsúhlasený
- R – realizovateľný
- T – časovo ohraničený (20)

Projektovým riadením sa chápu činnosti, ktoré zahŕňajú plánovanie a realizáciu zvyčajne jednorázových akcií. Na takúto akciu býva pevne stanovený termín a rozsah použiteľných nákladov. Predpokladá sa tu zmena pôvodného, zvyčajne nežiadúceho, na stav nový, ktorý je kvalitatívne vyhovujúcejší. Táto zmena je výrazná a dosahuje sa skokovým postupom. (22)

Projekt býva vykonávaný sledom na seba nadväzujúcich činností, ktoré musia mať presne stanovené poradie v závislosti od technologického či organizačného postupu projektu. V projektovom modeli sa často vykonávajú časové, zdrojové alebo nákladové analýzy, napríklad metódou sieťových analýz, ako je PERT. (21)

Sieťové analýzy sú spoločným názvom pre metódy založené na teórii grafov a pravdepodobnosti, ktoré sa zvyknú využívať v plánovaní projektov v rôznych oblastiach, ako aj implementácia informačných systémov do podniku. V sieťovej analýze sa vytvára tzv. sieťový graf, ktorý predstavuje model projektu. Sú v ňom súvislo, orientovane a uzlovo alebo hranovo vyznačené závislosti jednotlivých činností projektu a doby ich trvania. (21)

4.8.2 Metóda sieťovej analýzy PERT

Metóda PERT využíva hranovo definované sieťové grafy, teda jednotlivé činnosti sú predstavované orientovanou úsečkou smerujúcou od jedného uzlu k druhému. Doby trvania jednotlivých činností sa považujú za náhodnú veličinu s určitým rozdelením pravdepodobnosti. Pre výpočet strednej doby trvania činností (t_e) sa prepočítavajú optimistické(a), najpravdepodobnejšie(m) a pesimistické(b) časové odhady nasledovným vzorcom: (21)

$$t_e = \frac{a + 4m + b}{6} \tag{21}$$

Pravdepodobnú odchýlku od očakávanej hodnoty celkového trvania projektu je možné vypočítať nasledovne:

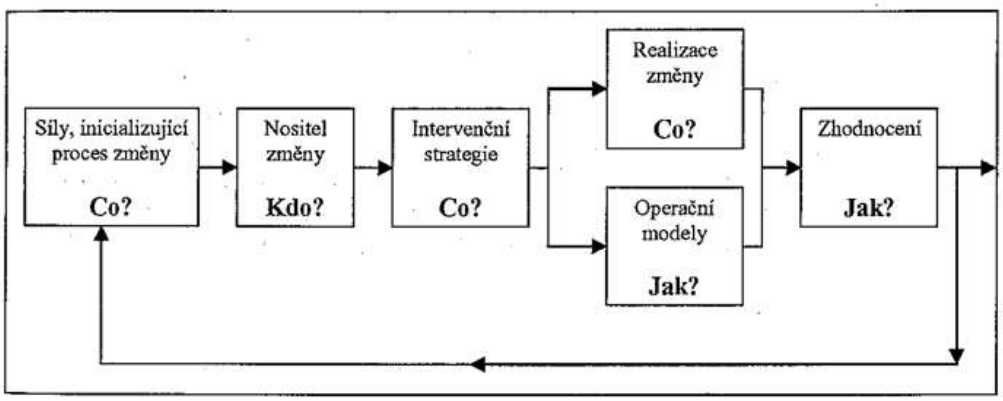
$$\sqrt{D(t_{ij})} = \frac{b - a}{6} \tag{21}$$

Ďalším postupom býva uskutočnená časová analýza. Tá postupným sčítavaním doby trvaní jednotlivých činností, za udržania následného predpokladu, že niektoré činnosti môžu byť uskutočnené až keď sú predchádzajúce skončené, vyhodnotí celkový čas trvania projektu a aj činnosti, ktoré majú na svoje vykonanie časovú rezervu. Ostatné činnosti, tzv. kritické, musia byť v záujme včasného dokončenia projektu vykonané bez omeškania. (21)

Využitie metódy PERT je vďaka uvedeným charakteristikám aplikovateľné hlavne pre projekty jedinečné a neopakovateľné, kedy nie je dopredu známy presný čas trvania projektových činností. K takýmto prípadom sa počíta aj projekt implementácie DMS systému do podniku. (21)

4.8.3 Lewinov model plánovanej zmeny v podniku

Podniky pravidelne uskutočňujú plánované zmeny s cieľom udržania svojej životaschopnosti, efektívnosti či konkurencieschopnosti. To platí aj pre plánované zmeny, ako napríklad implementácia cloudového riešenia informačného systému SharePoint Online do podniku. Pre zabezpečenie dosiahnutia požadovaných výstupov zavádzanej zmeny vznikol Lewinov model, ktorý vymenováva sled základných otázok, ktoré by sme si mali ešte pred zahájením konkrétneho procesu zmeny zodpovedať: (23)(29)



Obrázok 17 - Lewinov model riadenej zmeny, Zdroj: (23)

V úvode plánovania zmeny je potrebná analýza a stanovenie hlavných požiadaviek, čo chcem zmenou dohiahnuť. Fáza agenta zmeny nás prinúti uvažovať nad konkrétnym relizátorom alebo nositeľom zmeny. Ten býva zvyčajne podporovaný sponzorom zmeny. Intervenčné oblasti sú všetky oblasti, ktorých sa realizovaná zmena určitým spôsobom dotkne. Uvedomenie si, kam až bude plánovaná zmena siahať, môže totiž pomôcť jednotlivým

oblastiam lepšie sa pripraviť a stanoviť potrebné opatrenia. Nasleduje fáza realizácie vlastnej zmeny a teda samotného projektu. Uskutočňujú sa tu zvyčajne modely sieťovej analýzy, analýzy rizík alebo návrhy opatrení v rámci implementácie. Vyhodnotenie úspešnosti zavedenia plánovanej zmeny by malo byť optimálne zhodnotením dosiahnutej úrovne merateľného cieľa. (23)

5 VLASTNÉ NÁVRHY RIEŠENIA

Vlastný návrh spôsobu zavádzania systému DMS do servisnej pobočky Zebry vychádza z jej aktuálnej potreby zmigrovať decentralizovanú a duplicitnú podnikovú dokumentáciu z úložísk, na ktoré jej končia zmluvné licencie, do nového a jednotného DMS systému. Od tradičného postupu implementácie sa bude dané riešenie svojím obsahom líšiť od bežných implementačných projektov. Je to z dôvodu pevne stanovených kritérií aj požadaviek zo strany amerického vedenia, ktoré pevne určilo, že DMS bude cloudové riešenie systému SharePoint Online vo verzii Enterprise E3. Systém bude poskytnutý formou priplatených licencií a teda pobočka sa pripojí do už navrhnutej a zaužívanej globálnej štruktúry, kde si už celkom nenáročne vytvoria jednotlivé tími svoje podstránky. Tieto konkrétne požiadavky teda limitujú pobočku vo vlastnej iniciatíve nie len v rámci objektívneho výberu alternatívnych riešení ale aj v návrhu konkrétnych požadovaných funkcionalít, komponent či právomocí prispôsobiť si štruktúru DMS systému.

Z tohto dôvodu som sa rozhodla upriamiť návrh na možnosti, v ktorých sa môže pobočka sama aktívne pričiniť o hladký priebeh zavedenia systému Sharepoint do jej podnikového prostredia. Návrhom bude, ako môže pobočka pomocou projektového riadenia zabezpečiť transparentný a časovo aj nákladovo efektívny priebeh danej implementácie. V rámci projektového riešenia bude vypracovaná analýza rizík, ktoré môže pobočke nový systém priniesť a za účelom zníženia negatívnych dopadov týchto rizík budú navrhnuté možné opatrenia. V závere návrhovej časti budú navrhované riešenia zhodnotené z pohľadu ekonomickej efektívnosti.

5.1 Štúdia uskutočniteľnosti

Pred návrhom samotnej implementácie DMS je potrebné zosumarizovať si východiskový stav so všetkými požiadavkami na plánovanú zmenu a s ohľadom na finančné a ľudské zdroje spoločnosti vyhodnotiť, či je plán realizovateľný. K tomu je vypracovaná nasledujúca štúdia:

<table>
<tr><th colspan="2">Aktuálny stav</th><th>Očakávaný stav</th></tr>
<tr><th>Nedostatky systému</th><th>Legislatívne požiadavky</th><th>Požiadavky investora</th></tr>
<tr><td>Decentralizovaný systém práce s dokumentami, minimálne 5 rozdielnych úložísk dokumentov</td><td rowspan="2">SLA s Motorolou stanovuje konečný termín poskytnutia svojich serverov a systému pre správu dokumentov CMP</td><td>Globálne jednotný, centralizovaný systém správy, zdieľania, úpravy a využívania dokumentov pomocou SharePoint Online, formou tímových podstránok obsahujúcich knižnice dokumentov</td></tr>
<tr><td>Duplicitné dokumenty → pomalé vyhľadávanie → Pomalá servisná obsluha</td><td>Efektívny workflow → Zrýchlenie servisnej obsluhy zákazníkov</td></tr>
<tr><th colspan="3">Rámcový rozpočet</th></tr>
<tr><td colspan="2">Licenčné náklady</td><td>CZK 474/užívateľ/1 mesiac => CZK 189 600/1 mesiac</td></tr>
<tr><td colspan="2">Personálne náklady</td><td>Implementačný tím- Migračný tím , Školiaci tím, IT odborníci na SP, Hlavný administrátori SP</td></tr>
<tr><th colspan="3">Uskutočniteľnosť</th></tr>
<tr><td colspan="2">Finačné zdroje</td><td>Mesačné licenčné náklady predstavujú približne 0,20% priemerných čistých mesačných príjmov servisnej pobočky</td></tr>
<tr><td colspan="2">Personálne Zdroje</td><td>Pobočka má zamestnaných 3 pracovníkov IT oddelenia,nikto nie je školený na cloud computing ani SharePoint, zvyšok IT outsourcuje v rámci firemných prípadne komerčných IT personálnych zdrojov</td></tr>
<tr><td colspan="3">Pri plnom rešpektovaní vyššie uvedených skutočností a požiadaviek je možné konštatovať, že zámer implementácie systému SharePoint Online do brnenskej servisnej pobočky spoločnosti Zebra je realizovateľný, s prihliadnutím na nasledujúce odporúčania.</td></tr>
<tr><th colspan="3">Odporúčania</th></tr>
<tr><td colspan="3">Z dôvodu nedostatku odborne zaškolených pracovníkov, ktorý by implementáciu mohli koordinovať, vykonávať a následne udržiavať systém a školiť užívateľov je pobočke vysoko doporučované zaistiť zvýšenie počtu odborne zaškolených zamestnancov, výpomoc z iných pobočiek , ktoré už implementáciou prešli, prípadne zabezpečiť profesionálnu podporu od poskytovateľa SharePointu</td></tr>
<tr><td colspan="3">Z dôvodu časového ohraničenia oprávnení prístupu k serverom a systémom spoločnosti Motorola navrhujem pobočke stanoviť si v plánovanej implementácii Sharepointu za jeden z cieľov SMART cieľ , ktorý vytvorí dôraz na požiadavku úspešne zavedeného Sharepointu v časovo kratšej dobe, než je koniec SLA zmluvy s Motorolou (presné podmienky SLA sú interne známe v rámci hlavného vedenia spoločnosti). Možné znenie cieľa : Zmigrovať všetku podnikovú dokumentáciu z aktuálne využívaných systémov do SharePointu v danom termíne (interne známy) bez vzniku dodatočných nákladov za predlžovanie licenčnej zmluvy s Motorolou. Pre splnenie cieľa bude v návrhu práce vypracovaná časová analýza projektu metódou diagramu PERT.</td></tr>
</table>

Obrázok 18 - Štúdia uskutočniteľnosti, Zdroj: Vlastné spracovanie

5.2 Model implementácie systému DMS

Samotnú implementáciu DMS Sharepoint 2013 navrhujem uskutočniť projektovou formou z dôvodu jej jedinečnosti a časovej ohraničenosti. Takáto výrazná podniková zmena musí byť sprevádzaná sledom uvedomených činností, ktorých konkrétny postup bude odvodením z Lewinovho modelu riadenej zmeny prebiehať v nasledujúcich krokoch: (23)

Obrázok 19 – Postup implementácie potrebnej zmeny, Zdroj:Vlastné spracovanie podľa (23)

5.2.1 Špecifikácia požiadaviek

Potreba zmeny vychádza z uskutočnenej analýzy aktuálnej situácie podniku a následných konkrétnych požiadaviek na jej uskutočnenie špecifikovaných vedením spoločnosti, viď podkapitola 3.3.1 a 3.3.2.

5.2.2 Agent zmeny

Vedenie Zebry požaduje, aby každá organizačná jednotka servisného centra mala individuálne na starosti implementáciu SharePointu v stanovenom čase. Aplikácia Sharepoint má slúžiť užívateľom ako webová platforma a preto každý tím sám najlepšie vie, aké má požiadavky na nový systém. Keďže v tejto platforme už zvyšok firmy funguje, vedenie len dokúpi potrebné licencie, globálne IT oddelenie poskytne platformu a do istej miery znalosti. Zahŕňa to tvorbu vlastnej štruktúry každého oddelenia, migráciu dokumentov zo všetkých zdrojov do tejto jednotnej štruktúry, ako aj vytvorenie vlastného užívateľského rozhrania podľa individuálnych požiadaviek oddelení.

Oprávnenia k prístupu a k tvorbe štruktúry dostanú v prvom rade manažéri najvyššej línie jednotlivých oddelení a tí ďalej v rámci riadiacej hierarchie sami uznajú, ktorému zamestnancovi pridelia práva a povinnosti súvisiace s implementáciou SharePointu. Nesie to

so sebou aj výhodu, že sa môžu k iniciatíve dostať aj rádoví pracovníci, ktorí so systémami denne pracujú a vedia navrhnúť efektívne a potrebné vylepšenia nového systému.

5.2.3 Identifikácia intervenčných oblastí

Implementácia nového DMS systému zasiahne bezpochyby všetky oblasti, ktoré pracujú s podnikovou dokumentáciou. V konečnom dôsledku sú to všetky časti organizačnej zložky brnenského servisného strediska, keďže v záujme firmy je vytvoriť centralizovanú platformu formou webového portálu, cez ktorý budú môcť jednotlivé oddelenia efektívnejšie spolupracovať. Komunikačné a organizačné toky budú teda výrazne danou implementáciou ovplyvnené tiež.

Oblasť ľudských zdrojov bude bezpochýb najvýraznejšie zasiahnutá uvažovanou zmenou. Zamestnanci budú totiž musieť zmeniť svoju dennú rutinu aj spôsob práce s dokumentami a začať fungovať v úplne novom, neznámom prostredí. Ľudský faktor sa navyše zmenám najviac bráni a preto bude pri implemetácii potrebné zamerať sa na podnikovú agendu, propagáciu a odôvodnenie zmeny, či dostatočné zaškolenia.

5.2.4 Návrh projektu zmeny

Pre naplnenie navrhovaného cieľa, ktoré stanovuje snahu zaviesť systém SharePoint a zmigrovať doňho všetky podnikové dáta skôr, než bude musieť platiť pobočka pokuty za nedodržanie SLA zmluvy s Motorolou, je návrhom vypracovanie časovej analýzy postupnosti jednotlivých projektových činností. K uskutočneniu plánovanej zmeny je potrebné vykonať činnosti uvedené v nasledujúcej tabuľke. Každá činnosť má svoje označenie a určeného nasledovníka, ktorý predstavuje činnosť, ktorá musí nasledovať bezprostredne až po dokončení tej predchádzajúcej.

Jednotlivé činnosti sú ďalej spracované metódou sieťovej analýzy do diagramu PERT, ktorý uľahčuje sledovanie a optimálne rozvrhnutie potrebných zdrojov v časovom intervale pre jednotlivé činnosti a tým umožňuje šetrenie nákladov projektu. K tomu sú stanovené časové odhady, ktoré určujú optimistkú (a), očakávanú (m) a pesimistickú (b) variantu doby trvania jednotlivých činností. Práca s rôznymi dobami trvaniu projektu je v danom projekte vhodná kvôli neurčitosti trvania jednotlivých činností pri projekte zavádzania nového DMS systému do užívania servisnej pobočky. Tieto doby boli stanovené na základe konzultácie s internými

pracovníkmi servisného strediska, ktorí sa na realizácii projektu budú podieľať, prípadne už majú skúsenosti z predošlých obdobných projektov. Na základe týchto hodnôt je prepočítaná stredná doba trvania jednotlivých činností aj ich smerodatná odchýlka.

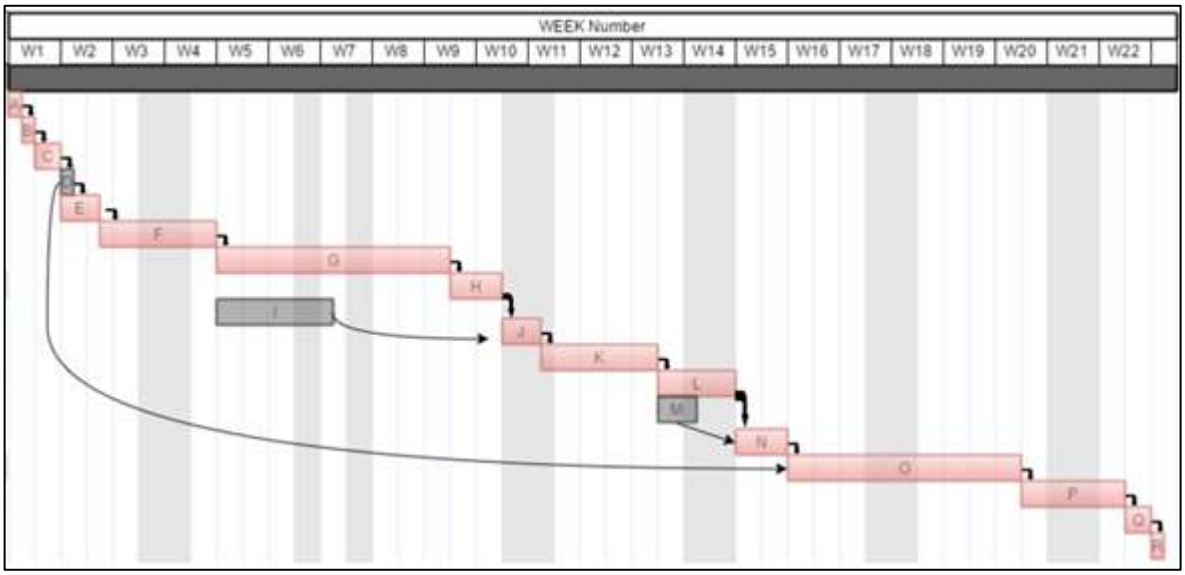
Tabuľka 10 - Projektové činnosti, Zdroj: Vlastné spracovanie

	Ozn.	Činnosť	Nasl.	a	m	b	Te	Rozptyl
(1-2)	**A**	Definovať aktuálnu situáciu s podnikovými dokumentami	B	1	1	5	2	0,44
(2-3)	**B**	Definovať presnú predstavu o novom DMS	C	1	1	5	2	0,44
(3-4)	**C**	Stanoviť si ciele, myľníky	D,E	2	3	7	4	0,69
(4-12)	**D**	Informovať zamestnancov o plánovanej zmene	O	1	1	3	1	0,11
(4-5)	**E**	Určiť ľudí, ktorí budú za implementáciu zodpovední	F	2	5	7	5	0,69
(5-6)	**F**	Dať vybraným kompetentným ľuďom školenie	G,I	10	14	21	15	3,36
(6-7)	**G**	Tvorba základnej štruktúry na poskytnutej platforme	H	21	30	40	30	10,03
(7-8)	**H**	Tvorba designu jednotlivých podstránok	J	5	7	14	8	2,25
(6-8)	**I**	Kategorizácia aktuálnych dokumentov	J	5	10	20	11	6,25
(8-9)	**J**	Plán novej dokumentovej štruktúry- adresáre, súbory, priečinky	K	3	5	10	6	1,36
(9-10)	**K**	Migrácia dokumentov zo všetkých aktuálnych úložísk	L,M	10	15	20	15	2,78
(10-11)	**L**	Vymazanie duplicít dokumentov	N	5	10	14	10	2,25
(10-11)	**M**	Finálna úprava designu a funkčnosti tímových podstránok	N	2	5	10	5	1,78
(11-12)	**N**	Definovanie politiky, skupín užívateľov a prístupových oprávnení	O	5	5	14	7	2,25
(12-13)	**O**	Spustenie do testovacej paralelnej prevádzky užívateľom	P	30	30	45	33	6,25
(13-14)	**P**	Úpravy podľa požiadavkov užívateľov	Q	7	14	21	14	5,44
(14-15)	**Q**	Zavedenie jednotnej prevádzky	R	1	2	5	2	0,44
(15-16)	**R**	Zrušenie prístupu do pôvodných úložísk	-	1	1	1	1	0,00

Výsledný diagram PERT je k náhľadu v Prílohe B**.** Celková doba trvania je týmto spôsobom odhadnutá na 154 dní so smerodatnou odchýlkou v približnej hodnote 6, ktorá hovorí o možnosti odchýlenia sa od odhadovanej časovej hodnoty. Z grafu je možné vypozorovať, že väčšina činností na seba plynulo nadväzuje a časová rezerva vzniká len pri činnostiach D,I a M.

5.2.5 Časový plán

V nasledujúcom grafe je znázornený časový harmonogram jednotlivých činností projektu v týždňoch. Červené činnosti na seba plynule nadväzujú a predstavujú kritické činnosti bez voľných časových rezerv. Šedé činnosti (D,I,M) sú tie, ktoré majú voľnú časovú rezervu a je možné ich preto vykonať aj s časovým oneskorením a ušetriť tým potrebné zdroje pre efektívnejšiu alokáciu k iným činnostiam.Pre podrobnejší obrázok viď. príloha F.



Obrázok 20 – Diagram časového sledu činností projektu, Zdroj: Vlastné spracovanie

5.3 Analýza rizík

Vo firme Zebra je proces analýzy rizík plánovaných zmien jasne definovaný podnikovou smernicou, ktorá bola bližšie spomenutá v podkapitole 3.1.7. Na jej základe je vypracovaná aj nasledujúca analýza rizík súvisiacich s navrhovanou implementáciou DMS Sharepoint.

Tabuľka 11- Hodnotenie rizík, Zdroj: Vlastné spracovanie podľa interných materiálov

Hodnotenie rizík	
Hodnota rizika	**Výsledné riziko**
<0,00-1,00>	Nízke riziko
(1,00-2,00>	Vysoké riziko
(2,00-4,00>	Kritické riziko

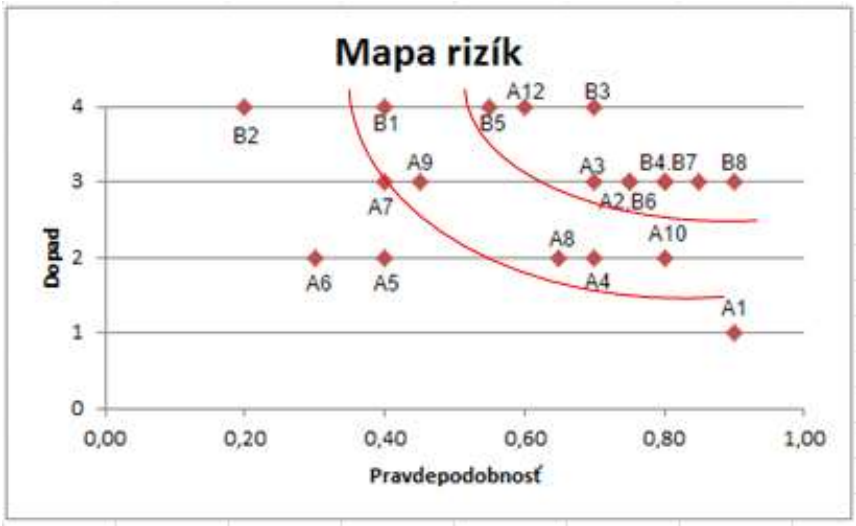
Hodnotenie pravdepodobnosti rizík						
Pravdepodobnosť	Vysoko pravdepodobné 71%-100%	0,71-1,00	0,71-1,00	1,42-2,00	2,13-3,00	2,84-4,00
	Pravdepodobné 41%-70%	0,41-0,70	0,41-0,70	0,82-1,40	1,23-2,10	1,64-2,80
	Málo pravdepodobné 11%-40%	0,11-0,40	0,11-0,40	0,22-0,80	0,33-1,20	0,44-1,60
	Nepravdepodobné 0%-10%	0,00-0,10	0,00-0,10	0,00-0,20	0,00-0,30	0,00-0,40
			1	2	3	4
			Nevýznamný (0%-3% rozpočtu)	Malý (3%-10% rozpočtu)	Významný (10%-30% rozpočtu)	Kritický (Nad 30% rozpočtu)
			Dopad			

Obrázok 21 - Hodnotiaca matica pri analýze rizík, Zdroj: Vlastné spracovanie podľa interných materiálov

Z implementácie nového systému do podnikovej informačnej infraštruktúry môže vzijsť viacero rizík. V nasledujúcej tabuľke sú uvedené hrozby, ktorým projekt čelí a konkrétne scenáre, ktoré z jednotlivých hrozieb vyplývajú. Uvedené sú aj ohodnotenia pravdepodobnosti ich výskytu a dopadu podľa podnikovej smernice. Tieto hodnoty boli konzultované s pracovníkmi internej kvality a zamestnancami podieľajúcimi sa na realizácii implementácie DMS. Výsledná hodnota rizika sa vypočíta násobením hodnoty pravdepodobnosti a dopadu a čím vyššia hodnota vyjde, tým väčšiu pozornosť treba potenciálnemu riziku venovať a zamerať sa na možné opatrenia jeho eliminácie. Grafické zobrazenie nájdených rizík je zobrazené v Mape rizík na Obrázku č.22, ktorá červenými krivkami oddeľuje riziká nízke, vysoké a kritické.

Tabuľka 12 – Analýza rizík súvisiacich s implementáciou DMS, Zdroj: Vlastné spracovanie

Analýza rizík súvisiacich s implementáciou DMS					
Číslo	**Hrozba**	**Scenár**	**Pravd.**	**Dopad**	**Hodnota rizika**
A	**Funkčné hrozby**				
A.1	Nedostatočné oboznámenie a zaškolenie užívateľov	Nevyužitý potenciál a funkcionalita DMS	0,90	1	0,90
A.2		Neustála decentralizovaná manipulácia s dokumentami	0,75	3	2,25
A.3		Neefektívny workflow v novom prostredí	0,70	3	2,10
A.4		Nesystematická a príliš rozvetvená štruktúra podstránok	0,70	2	1,40
A.5	Odlišné užívateľské verzie MS Office	Neefektívna spolupráca / workflow	0,40	2	0,80
A.6	Nedostatok úložného miesta	Nutnosť využívať iné úložiská	0,30	2	0,60
A.7	Neschopnosť orientovania sa a vyhľadávania dokumentov	Časové náklady a spomalené podnikové procesy	0,40	3	1,20
A.8	Zaneprázdnenosť zodpovedných ľudí	Dlhá doba trvania implementácie	0,65	2	1,30
A.9	Vysoká fluktuácia zamestnancov	Strata nadväznosti a neefektívny prenos kompetencií	0,45	3	1,35
A.10	Nedbalosť životného cyklu jednotlivých stránok	Nevyužívané stránky zaberajúce priestor	0,80	2	1,60
A.11	Vysoký počet nekompetentných administrátorov	Nedostatočný dohľad, správa sa vymkne z rúk, ohrozená správna	0,85	3	2,55
A.12	Nesystematický presun dokumentov	Strata niektorých dokumentov	0,60	4	2,40
B	**Bezpečnostné hrozby**				
B.1	Narušenie integrity dokumentov	Modifikácia, zničenie, strata dokumentov	0,40	4	1,60
B.2	Výpadok internetového pripojenia	Nedostupnosť SharePointu	0,20	4	0,80
B.3	Narušenie dôveryhodnosti dokumentov	Prístup neoprávnených subjektov	0,70	4	2,80
B.4	Rastúci počet administrátorov	Nesystematické prideľovanie prístupových oprávnení	0,80	3	2,40
B.5	Narušenie dostupnosti dokumentov	Nedostupnosť dokumentov v požadovaných lehotách	0,55	4	2,20
B.6	Neschopnosť auditovať užívateľské a administratívne zaobchádzanie s DMS	Exponenciálny nárast chýb a exponenciálny pokles efektívnosti práce s DMS	0,75	3	2,25
B.7	Absencia dozoru nad pridávaným obsahom	Nežiaduci a bezpečnostne nevyhovujúci obsah	0,80	3	2,40
B.8	Nekorešpondujúca legislatíva s cloudovým poskytovateľom	Nedostupnosť, narušená integrita, dôveryhodnosť,	0,90	3	2,70



Obrázok 22- Mapa rizík, Zdroj:Vlastné spracovanie

5.4 Návrh eliminácie rizík

Riziká sprevádzajú každý jeden projekt a nikdy nie je možné úplne sa ich zbaviť. Vďaka opatreniam však môže podnik znížiť dopad rizika na preňho akceptovateľnú úroveň. Voľba konkrétnych opatrení by mala vychádzať z postupnosti priorít, ktoré sa s projektom viažu, pričom podnik nesmie zabúdať na ekonomickú efektívnosť navrhovaného opatrenia. V prípade projektu implementácie systému Sharepoint do brnenskej pobočky Zebry sú požiadavky a s nimi spojené možné opatrenia na výsledný systém Sharepoint usporiadané do nasledovných priorít:

Tabuľka 13 - Oblasti možných opatrení vrámci projektu implementácie DMS, Zdroj: Vlastné spracovanie

Priorita	Oblasti možných opatrení
1. **Dostupnosť dát a dokumentov**	○ Redundantné internetové pripojenie ○ BCM plán ○ Zálohovanie
2. **Dôvernosť a Integrita dát a dokumentov**	○ Prístupové oprávnenia-Identity and access management ○ Zásady zadávania hesiel do DMS, dvoj-faktor. autentifikácia ○ Data ownership ○ SAE ○ Audit
3. **Funkčnosť systému**	○ SAE ○ politika,procedúry, štandardy ○ Auditný mechanizmus a nástroje na zaistenie spĺňania nastavených procesov
4. **Právna zodpovednosť**	○ Naštudovať legislatívu, z ktorej vychádza Microsoft cloud

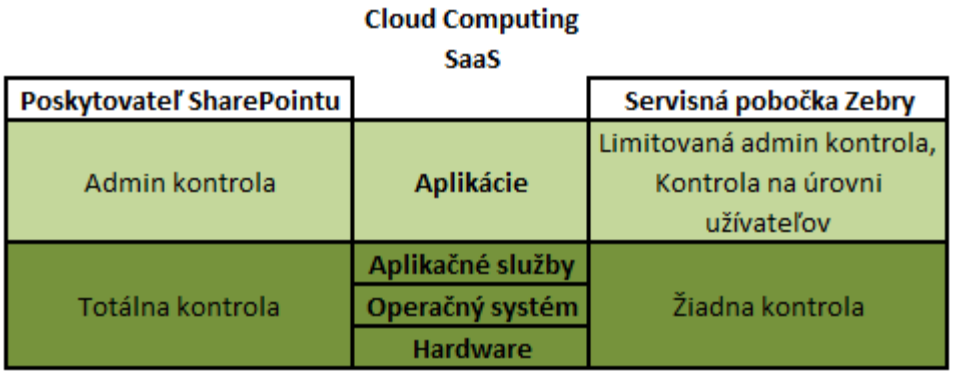
Vychádzajúc z uvedenej postupnosti priorít som sa v časti návrhu opatrení rizík súvisiacich s projektom implementácie DMS, aj vrámci rozsahového obmedzenia diplomovej práce, rozhodla zaoberať sa výlučne problematikou cloudového riešenia. Považujem túto obasť za významnú pre sledovanú servisnú pobočku Zebry, nie len na základe výsledkov analýzy rizík ale aj vďaka aktuálne rastúcej popularite tejto problematiky, pričom je predpokladané využitie návrhov aj pre budúce potenciálne projekty pobočky.

Systém Cloud computing, ako aj všeobecné odporúčania pri práci s ním, sú spracované normami NIST z rady 800-145 (viď.(17)) a na základe nich bude vypracovaný aj môj konkrétny návrh opatrení pre pobočku Zebry. Tá bude totiž zavádzať nový DMS systém MS Sharepoint 2013 rovno v cloudovej verzii a teda bude migrovať svoju dokumentáciu priamo do cloudu Microsoftu. Pre pobočku je to úplne nové prostredie, pričom veľa zamestnancov nemá aktuálne dostatočné povedomie ani o význame tejto technológie.

Navyše predpokladám, že návrhom opatrení vychádzajúcich z odporúčaní podľa uvedených noriem bude možné eliminovať naraz hneď niekoľko kritických rizík implementácie DMS a zabezpečiť tak hladký priebeh projektu a dosiahnutie požadovaných výsledkov.

5.5 Návrh opatrení pre elimináciu rizík vyplývajúcich z Cloud Computingu

DMS, ktorý bude implementovaný do pobočky Zebry, bude poskytnutý formou verejného cloudového riešenia MS Sharepoint 2013, v servisnom modely SaaS. Toto prevedenie so sebou prinesie jasne stanovený rozsah kontroly nad systémom pre poskytovateľa, ako aj užívateľa DMS systému, teda servisnú pobočku. Tá bude mať v systéme len veľmi malé kontrolné právomoci, zahrňujúce limitované administrátorské oprávnenie k aplikácii a kontrolu nad jednotlivými užívateľmi aplikácie, ako je znázornené na nasledujúcom obrázku:



Obrázok 23- Právomoci poskytovateľa a užívateľa cloudového servisného modelu SaaS, Zdroj: Vlastné spracovanie podľa (17)

Takýto model preto nedáva všeobecne príliš veľké možnosti užívateľovi aplikácie, aby si sám svojou činnosťou zabezpečoval požadovanú úroveň zabezpečenia svojich dát v aplikácii a väčšinou sa musí spoliehať na adekvátnosť vyhotovenej SLA zmluvy s poskytovateľom, ako aj na jej dodržiavanie. Za normálnych podmienok si preto v SLA zmluve podnik nastaví, prípadne priplatí požadovanú bezpečnostnú úroveň dostupnosti, integrity či dôvernosti svojich dát.

V navrhovanom projekte implementácie cloudového riešenia DMS pre servisnú pobočku Zebry je však situácia trochu rozdielna. Pobočka je vo svojich vlastných proaktívnych návrhoch zabezpečení DMS systému limitovaná americkým vedením spoločnosti, ktoré v cloudovom prostredí MS Sharepoint 2013 už krátku dobu funguje a rozšírením počtu lincencií poskytne hotovú platformu svojej pobočke v Brne, bez ďalších možností konkrétneho prispôsobovania SLA zmluvy.

Návrhy opatrení, ktoré zahŕňajú vyjednávanie bezpečnostných parametrov s poskytovateľom cloudového riešenia, budú preto v práci vynechané, pričom pobočka bude na riziká s tým súvisiace reagovať len formou vedomej retencie rizík. Práca sa zameria len na reálne aktivity a možnosti zabezpečenia zo strany servisnej pobočky, ktorými sa sama môže pričiniť o elimináciu nežiadúcich dopadov implementácie cloudovej verzie DMS do jej podnikového prostredia. Vychádzať sa pritom bude z už uvedenej postupnosti priorít, ktoré pobočka kladie na DMS systém.

5.5.1 Návrh plánu obnovy systému Sharepoint Online- BCM

Najvyšší dôraz pri návrhu opatrení sa kladie na dostupnosť dát a dokumentov v Sharepointe. Systém bude totiž implementovaný formou užívateľsky prispôsobeného webového portálu, ktorý bude centrálou zamestnaneckej dennej činnosti a vzájomnej komunikácie či spolupráce. Zamestnanci budú teda denne pri obsluhe zákazníkov využívať portál Sharepointu a dokumenty v ňom uložené a rovnako budú doň denne ukladať nové dokumenty. Keďže sa tu však jedná o cloudové prostredie, v ktorom tieto dáta budú fyzicky uložené u cloudového poskytovateľa v jeho dátovom centre situovanom v zahraničí, je potreba počítať so situáciou, kedy Sharepoint a potrebné dokumenty v ňom nebudú dostupné. Nedostupnosť najdôležitejších dokumentov môže spôsobiť neschopnosť obsluhy zákazníkov, pričom niektorí prestížni zákazníci majú zazmluvnené maximálne čakanie na vyriešenie ich problému do 15 minút. Ich nespokojnosť môže preto vyústiť k znižovaniu zisku alebo prípadným pokutám za nedodržanie zmluvnej doby obsluhy.

V rámci opatrení pre elimináciu rizika nedostupnosti Sharepointu a potrebných dát v Sharepointe navrhujem vypracovať plán obnovy systému - "Contingency Plan", ktorý v konkrétnych krokoch uvedených v nasledujúcej tabuľke, poskytne pobočke plán činností a možnosti obnovy nedostupného DMS systému. Návrh bude vychádzať z odporúčaní normy NIST 800-34 (viď. (18))**.**

Tvorba politiky pre plán obnovy	*Tvorba Analýzy dopadu na podnikanie*	*Tvorba stratégie obnovy*	*Plánovanie tréningu a testovanie systému obnovy*	*Spôsob udržiavania plánu obnovy*
Hlavný cieľ	Obchodné procesy a kritickosť ich obnovy	Stratégia obnovy dokumentov	Plán testovania obnovovacieho plánu	Zhodnotenie plánu
Role a Zodpovednosti	Ohodnotenie dopadu výpadku	Zálohovací systém a požiadavky	Plán tréningu vrámci plánu obnovy	Aktualizácia, adaptácia plánu
Požiadavky na zdroje	Časové požiadavky na obnovu		Plán cvičení vrámci obnovy	Úprava dokumentácie
	Požiadavky na obnovu zdrojov			Podnikové smernice

Obrázok 24 - Plán obnovy systému DMS, Zdroj: Vlastné spracovanie podľa (18)

5.5.1.1 Tvorba politiky pre plán obnovy systému DMS

K naplneniu podstaty celého plánu obnovy DMS systému je potrebné v úvode zabezpečiť transparentnosť a uzrozumenie všetkých kompetentných podnikových zamestancov s obnovovacou politikou. Táto politika definuje hlavné ciele plánu obnovy, rámec konkrétnych požiadavkov, ako aj kompetencie zodpovedných ľudí za ne. V ideálnom prípade sa na jej tvorbe aktívne podieľa CIO. V tejto politike je nutné zahrnúť nasledovné body:

- **Hlavný cieľ plánu obnovy** informačného systému Sharepoint Online 2013, je zabezpečiť plynulý chod na ňom závislých kritických procesov, v prípade jeho výpadku. Plynulým chodom sa myslí zabezpečenie dostupnosti požadovaných dát zo Sharepointu v dobe kratšej, ako je maximálna prípustná doba nedostupnosti jednotlivých kritických procesov.
- **Zodpovednosti a úlohy** súvisiace s plánom obnovy musia byť pridelené špeciálne vyškolenému tímu zamestnancov. V rámci tohoto tímu sa budú rozlišovať nasledujúce role:

Tabuľka 14 - Role a zodpovednosti v súvislosti s BCM, Zdroj: Vlastné spracovanie

Názov role	Zodpovednosť	Návrh konkrétnych predstaviteľov
Systémový vlastník, Hlavný manažér obnovy DMS	Všeobecná manažérska zodpovednosť za plán obnovy DMS Sharepoint	**Podnikový CIO**
Koordinátor obnovy DMS	Zodpovednosť za dohľad nad obnovou a reorganizáciou, šírenie potrebného povedomia, koordinácia testovania a tréningu osôb, koordinácia s ostatnými tímami zaoberajúcimi sa obnovou iných informačných systémov	**Hlavný Sharepoint Administrátor**
Tím technickej podpory obnovy DMS	Technicky vyškolený tím, ktorý má na starosti praktickú obnovu DMS systému a všetky technické činnosti s ňou súvisiace, rovnako ako vykonávanie pravidelného testovania.	**Vyškolený tím technickej podpory a správy Sharepointu + zastúpenie z IT oddelenia**

- **Požiadavky na zdroje** -V uvedenom pláne je potrebné definovať požadované zdroje, ktoré zabezpečia životaschopnosť procesov a činností potrebných k obnove DMS Sharepoint. V návrhu budú uvedené len technické IT zdroje, ktoré je potrebné vynaložiť navyše od bežne využívaných zdrojov a to v závislosti od potrebných činností a aktivít obnovy DMS systému. Potrebné ľudské, informačné a finančné zdroje sú spracované v rámci iných podkapitol.

Tabuľka 15 - Požiadavky na IT zdroje v súvislosti s BCM, Zdroj: Vlastné spracovanie

Činnosť	Typ zdrojov	Konkrétne zdroje
Zostavenie plánu, manažment, budovanie povedomia	IT Zdroje	SW nástroje pre šírenie povedomia, školení, informácií
Priebežné trénovanie a testovanie	IT Zdroje	SW nástroje trénovania a testovania obnovy DMS, virtuálny server pre účely testovania
Obnovovacie činnosti v prípade výpadku DMS	IT Zdroje	Záložné diskové polia a lokálny server + konektivita
		Záložná prípojka do internetu, záložný internetový poskytovateľ
		SW nástroj OneDrive

5.5.1.2 Tvorba Analýzy dopadu na podnikanie

Cieľom analýzy dopadu na podnikaie- BIA (Business Impact Analysis) je analyzovať, aké negatívne dopady môže priniesť narušenie systému DMS Sharepoint na sledovanú servisnú pobočku Zebry. Na základe analýzy najzávažnejších následkov narušenia pracovných procesov sa stanovia priority, z ktorých bude vychádzať BCM plán. K jednotlivým kritickýcm procesom budú priradené aj zdroje potrebné pre zavedenie plánu obnovy. Tvorba BIA podľa normy NIST 800-34 (viď. (18)) začína krokom definície business procesov a ich kritickosti, kde analyzuje všetky podnikové procesy, ktoré budú závisieť alebo podporovať DMS Sharepoint.

Tabuľka 16 - Dopad neschopnosti vykonávania obchodných procesov, Zdroj: Vlastné spracovanie

Business proces	Potenciálny dopad v prípade neschopnosti činnosi				Celkový dopad (M-S-V)
	Nespokojnosť zákazníkov (M-S-V)	Nespokojnosť dodávateľov (M-S-V)	Nespokojnosť zamesnancov (M-S-V)	Fin. nákl./Kč (M < 30 000, S < 100 000, V > 100 000)	
Technická podpora zákazníka	V	S	S	V	**V**
Netechnická podpora zákazníka	V	S	S	V	**V**
Tvorba faktúry za poskytnuté servisné služby	S	M	M	V	**S**
Kontaktovanie zákazníka	S	M	M	S	**S**
Vymáhanie fyzických pohľadávok od zákazníka	M	S	M	V	**S**
Vzájomná spolupráca jednotlivých tímov	S	M	V	S	**S**
Komunikácia vrámci tímu/tímov	S	S	V	S	**S**
Kontaktovanie dodávateľov	M	V	M	M	**M**
Prezentácia jednotlivých tímov	M	M	S	M	**M**
Vyhodnotenie interného auditu	M	M	S	M	**M**

Každému z vyznačených business procesov je potrebné stanoviť maximálne prípustnú dobu nečinnosti v prípade výpadku systému Sharepoint. Slúžia nato v hodinách vyjadrené charakteristiky uvedené v nasledujúcej tabuľke. Hodnota MTD (Maximum Tolerable Downtime) predstavuje maximálnu dobu, ktorú je systémový vlastník ochotný akceptovať pre výpadok business procesu, pričom zváži aj celkový dopad, ktorý to na pobočku prinesie. RTO (Recovery Time Objective) predstavuje maximálne dobu, po ktorú môže ostať proces alebo systém nefunkčný, pred tým než spôsobí neakceptovateľný dopad na iný proces. RPO (Recovery Point Objective) vyjadruje maximálnu toleranciu k možnej strate dát, teda v podstate, ako rýchlo musí byť neaktívny proces po výpadku znova spustený.

Tabuľka 17 - Maximálne prípustné doby nečinnosti, Zdroj: Vlastné spracovanie

Business proces	MTD/hours	RTO/ hours	RPO/ hours
Technická podpora zákazníka	1	0,25	0,25
Netechnická podpora zákazníka	8	2	0,25
Tvorba faktúry za poskytnuté servisné služby	48	12	1
Kontaktovanie zákazníka	30	8	0,5
Vymáhanie fyzických pohľadávok od zákazníka	72	24	2
Vzájomná spolupráca jednotlivých tímov	24	8	2
Komunikácia vrámci tímu/ vrámci viacerých tímov	24	8	3
Kontaktovanie dodávateľov	24	12	0,5
Prezentácia jednotlivých tímov	120	72	12
Vyhodnotenie interného auditu	120	120	12

Identifikácia požadovaných zdrojov a ich priorít vymenováva, aké prvky je nevyhnutné zabezpečiť pre znovuobnovenie najzávažnejších procesov v prípade výpadku Sharepointu. Jednotlivým zdrojom sa priradí charakteristika RTO, ktorá určí, za akú maximálnu dobu musí byť zdroj sprístupnený a z toho vyplývajúce priority pri zavádzaní obnovovacieho plánu.

Tabuľka 18 - Maximálna doba sprístupnenie vypadnutých zdrojov, Zdroj: Vlastné spracovanie

IT Zdroje	RTO/hours	Priorita (M-S-V)
Internetové pripojenie	0,25	V
Dokumenty kategórie C	0,25	V
Email Server	0,5	V
Dokumenty kategórie B	12	S
Dokumenty kategórie A	48	M

5.5.1.3 Tvorba stratégie obnovy DMS Sharepoint

V rámci stratégie obnovy DMS systému Sharepoint pre prípad jeho výpadku, navrhujem pobočke Zebry zaistiť zálohovací systém dokumentov, ktorý zohľadní výsledky BIA analýzy. Vychádzajúc z analýzy je zrejmé, že jednotlivé kategórie dokumentov majú v prípade ich nedostupnosti rôzne veľký dopad na podnikateľskú činnosť pobočky, čo vyvoláva odlišné nároky na svoje zabezpečenie a preto budú na ne aplikované aj odlišné metódy zálohovania.

Tabuľka 19 - Návrh zálohovacieho systému, Zdroj: Vlastné spracovanie

Dokumenty	Metóda zálohovania	Stratégia zálohovania	Umiestnenie zálohy
Kategória A	Lokálne diskové polia	Hot Site	Onsite
Kategória B	Lokálne diskové polia	Hot Site	Onsite
Kategória C	Lokálne diskové polia + lokálna užívateľská kópia	Hot Site + Offline lokálne kópie	Onsite

Navrhovaným zálohovacím systémom je primárne lokálne externé sieťové diskové úložisko. V tejto lokálnej zálohe sa budú ukladať všetky kategórie dokumentov, celá dokumentová štruktúra zo Sharepointu sa tu bude teda v podstate zrkadliť. Pre dokumenty kategórie C nie je však táto lokálna forma zálohovania dostatočná, hlavne kvôli dlhšej dobe sprístupnenia konkrétnych dokumentov užívateľom, v hodinovom merítku. Proces uvedenia zálohy do chodu by bol navyše vysoko závislý od administrátora. To všetko môže nepriaznivo ovplyvniť plynulý chod obsluhy (hlavne prioritných) zákazníkov a preto bude v návrhu obsiahnutá aj tvorba lokálnych kópií kritických dokumentov kategórie C, dostupných offline v prípade výpadku Sharepointu, prípadne internetu a riadených priamo užívateľmi.

Dokumenty kategórie C podporujú kritické procesy pobočky a podľa normy NIST 800-34 (viď. (18)) je v takých prípadoch odporúčané splniť pravidlo zálohovania kritických dát 3-2-1, 3 rôzne kópie dát, 2 rôzne typy ukladacích médii, prípadne nezávislé ukladacie disky a 1 kópia uložená mimo priestory pobočky. Dokumenty kategórie C majú toto pravidlo vytvorením lokálnej kópie splnené. V rámci zálohovania nesmieme totiž zabúdať, že spoločnosť Microsoft, ako cloudový poskytovateľ, zálohuje všetky zverené dáta vlastnými technológiami, pričom poskytuje automaticky fyzické uloženie dát do 3 geograficky oddelených oblastí. Aktuálne figuruje Microsoft dvoma európskymi datacentrami v Dubline

a v Amsterdame, čo by mohla pobočka Zebry využiť a priplatiť si umiestnenie svojich dát v obidvoch európskych datacentrách.

V nasledujúcich podkapitolách budú priblížené charakteristiky navrhovanej onsite zálohy.

ONSITE záloha na zdieľaných diskových poliach

Zavedenie zálohovacieho systému na lokálnych diskových poliach bude v pobočke vypracované formou samostatného projektu a preto budú v uvedenom návrhu načrtnuté len návrhy základných charakteristík a parametrov, ktoré by mal zálohovací systém splniť, nie konkrétne hardwarové prvky či sofwtarové technológie.

- **Metódy zálohovania**
    - *Stratégia* – V lokálne umiestnenej zálohe sa navrhuje tzv. "Hot site" stratégia náhradného procesného vybavenia. Tá podľa normy NIST 800-34 znamená, že lokácia umiestnenia zálohy je vybavená potrebným operačným vybavením a kapacitou tak, aby mohla rýchlo prebrať v prípade potreby funkciu pôvodného systému a umožniť tak priebeh kritických procesov. Znamená to, že záloha sa v prípade výpadku Sharepointu sprístupní zamestnancom a poskytne im najaktuálnejšiu verziu dát z nedostupného systému.

    - *Umiestnenie* - V uvedenom návrhu je zálohovanie riešené formou úložiska dát na externých sieťových diskových poliach umiestnených v servisnej pobočke Zebry v Brne, teda disky nebudú priamo súčasťou serverov, ale servery sa k nim budú redundantne pripájať tak, aby výpadok časti siete neobmedzil funkčnosť zálohy. Takéto diskové úložisko by malo byť umiestnené v oddelenej časti internej počítačovej siete určenej na prenos požadovaných zálohovaných dát, vďaka čomu by nebola primárna sieť dodatočne zaťažovaná transférom veľkých objemov dát.

    - *Typ zálohy* - Centralizovaná záloha na lokálnom disku bude zrkadlovo kopírovať adresárovú štruktúru dokumentov zo Sharepointu, odkiaľ ich bude naprogramovaným skriptom (napríklad v Powershall) v pravidelných intervaloch kopírovať do namapovaných zdieľaných diskov na vyhradenom serveri. Jedným z návrhov je z dôvodu veľmi veľkých objemov dát tvorba plnej zálohy a následná tvorba rozdielových záloh formou zmien vzniknutých od poslednej plnej zálohy.

    - *Frekvencia zálohovania, čas zálohovania* - Interval kopírovania môže byť nastavený rôzne, podľa potrieb pobočky. Návrhom je uskutočňovanie rozdielovej zálohy každý večer v pracovnom týždni po 19,30, teda po pracovnej dobe a plnú

zálohu raz do týždňa, ideálne cez víkend. V prípade obnovy bude potom použitá plná záloha a k nej príslušná rozdielová.

- *Uchovávanie záloh* - Štruktúra zálohovaných dokumentov na zdieľanom disku bude previazaná z Active Directory a počas bežného fungovania systému Sharepoint nebude zdieľaný disk užívateľom sprístupnený. Je to tak z dôvodu snahy o zamedzenie decentralizovaného zaobchádzania užívateľov s dokumentami. V prípade výpadku Sharepointu bude zdieľaný záložný disk užívateľom sprístupnený, napríklad formou aplikačného rozhrania, z ktorého pošlú klienti svoj požiadavok na server a ten na konkrétny disk na diskovom poli. Plná záloha by mala byť ideálne uchovávaná 31 dní, rovnako aj rozdielové zálohy. Tvorené zálohy budú v podstate zrkadlenou kópiou dokumentov na Sharepointe a preto bude doba uchovávania jednotlivých dokumentov, rovnako ako Sharepoint, podliehať podnikovej smernici. Tá jasne stanovuje potrebnú dobu uchovania v závislosti od typov dokumentov, či nastavené pravidlo uchovávania 5 verzií dokumentov.

- *Predpokladané objemy* – Objem celkovej migrovanej dokumentácie je z dôvodu vysokej decentralizácie a duplicity náročné presne odhadnúť. Známy je len objem dokumentov uložených v aktuálne využívanom DMS systéme, približne 13 TB. Pri zahrnutí aj ostatných aktuálne využívaných úložísk je preto potrebné počítať s objemom minimálne 18 TB.

- **Hardware -** Kapacita diskových polí, ktoré by dokázali zabezpečiť zálohovanie za navrhovaných parametrov, by musela byť skutočne nadmerne vysoká a teda aj nákladná. Môže byť preto vhodné v rámci tvorby zálohovacieho projektu uvažovať nad kombináciou úložných médii a niektoré verzie záloh z diskov skladovať na finančne menej náročných páskach.

- **Náklady –** S ohľadom na navrhované parametre a konzultáciu s IT pracovníkom v pobočke by sa odhadované náklady mohli pohybovať okolo 3 mil CZK, samozrejme v závislosti od vybraných technológií.

- **Testovanie –** Overovanie správnej funkcionality lokálneho zálohovacieho systému je nevyhnutným prvkom plánu obnovy. Očakávnia, ktoré by malo splniť, ako aj frekvencia jeho uskutočňovania, bude priblížená v podkapitole 5.5.1.5.

ONSITE záloha vo forme lokálnych, užívateľsky spravovaných kópií dokumentov

- **Stratégia** – Kategória dokumentov C si vyžaduje okamžitú dostupnosť oprávnených užívateľov v prípade výpadku Sharepointu. Na dosiahnutie okamžitej dostupnosti a zachovania plynulosti kritických procesov sa odporúča zaviesť synchronizovaný systém využívania SharePoint technológie OneDrive od Microsoftu. Vďaka offline prístupu k zvolenej časti dokumentov sa v prípade nedostupnosti internetu alebo Sharepointu totiž nenaruší kontinuita servisnej činnosti pobočky**.**

- **Kompetencie –** pre využívanie Onedrive technológie je potrebné definovať presné kompetencie a systém ukladania lokálnych kópii. Cieľom je pritom zamedziť nežiadúcemu decentralizovanému zaobchádzaniu s dokumentami, ukladaniu nesynchronizovaných lokálnych kópií nekritických dokumentov a zbytočnému navyšovaniu diskovej kapacity. V každom tíme by mal byť team leaderom, prípadne ním povereným zástupcom definovaný okruh kritických dokumentov, ktoré sú v prípade výpadku systému nevyhnutné k požadovanej obsluhe zákazníkov. Tá skupina dokumentov by vytvorila knižnicu, s pridelenými prístupovými oprávneniami a bola by prostredníctvom teamleadera alebo zástucu zdieľaná s potrebnými užívateľmi.

Návrh OFFSITE zálohy

V prípade budúcej potreby pobočky poistiť si uloženie svojich dát z hľadiska dôveryhodnosti aj inde, než u cloudového poskytovateľa a na svojich lokálnych diskoch, odporúča norma NIST 800-34 (viď. (18)) okrem komerčných poskytovateľov aj uloženie kritických dát na úložiská inej pobočky, vrámci spoločnosti Zebra. Táto možnosť so sebou prináša samozrejme viacero organizačných a komunikačných komplikácií, no na druhej strane výhody z nezávislosti od komerčného externého poskytovateľa a zachovaní dôverných informácií vo vnútri firmy. Otázky zabezpečenia však nesmú byť opomenuté.

5.5.1.4 Kompetentné osoby

Aby celý zálohovací systém fungoval podľa nastavených požiadavok a bolo možné odvolať sa na kompetentných ľudí v prípade potreby, je nutné jednoznačne definovať, aké úlohy majú jednotliví zamestnanci spĺňať. Zodpovední v tomto ponímaní predstavujú ľudí, ktorí budú potrebné činnosti priamo vykonávať, poverení sú tí, ktorí sú za vykonanie zodpovední. O ostatných kompetenciách vypovedajú ich názvy samé.

Tabuľka 20 - Kompetencie za jednotlivé zálohovacie systémy, Zdroj: Vlastné spracovanie

Záloha	Kompetentné osoby			
	Zodpovedná	Poverená	Informovaná	Konzultovaná
Lokálne disky	IT tím	Koordinátor plánu obnovy	lokálny CIO	IT support
Lokálne užívateľské kópie	TL, tímový SP administrátor	Koordinátor plánu obnovy	lokálny CIO	IT support, Microsoft Support

5.5.1.5 Plánovanie tréningu a testovania systému obnovy DMS

5.5.1.5.1 Tréning

V časti plánovania tréningu je potrebné zamerať sa na zamestnancov, ktorým boli pridelené zodpovednosti a úlohy týkajúce sa celého plánu obnovy DMS Sharepoint, teda aj zálohovacieho systému. Tréning je určený na ich podrobné zaškolenie s problematikou, s ich úlohami a s plánom testovaní. Výstupom je stav, kedy kompetentní zamestnanci vedia presnú postupnosť činností, ktoré majú v prípade výpadku systému Sharepoint vykonať. Tréning bude uskutočňovaný interaktívnou formou, prednášaním a priebežne doplňovaný samoštúdiom.

Harmonogram trénovania bude previazaný s harmonogramom testovania systému DMS a jeho obnovy a rovnako aj s harmonogramom SAE týkajúceho ho sa cloudového riešenia či štandardných periodických IT tréningov pre všetkých zamestnancov. Navrhovaná periodickosť bude po uskutočnení úvodného tréningu podľa odporúčaní normy NIST 800-50 (viď. (19)) v minimálne ročnom intervale. Viac o tréningu bude spomenuté v podkapitole 5.5.2.

5.5.1.5.2 Testovanie

Testovanie bude používané ako hodnotiaci nástroj, ktorý pomocou očakávaných hodnôt z plánu obnovy DMS bude vyhodnocovať reálnu operabilitu plánu. . Informačné systémy, technológie ale hlavne potenciálne hrozby sa rýchlo vyvíjajú a staticky nastavenému plánu môže rýchlo ubúdať na účinnosti. Testovať sa bude z hľadiska bezpečnostných dopadov na dôležité dokumenty, ktoré môžu vzniknúť v krízovom prípade výpadku Sharepointu – narušenie dostupnosti a integrity.

Na testovaní sa budú podieľať príslušní kompetentní zamestnanci, podľa tabuľky č.14 a v niektorých prípadoch aj nepriamo všetci zamestnanci. Testovací proces stavia na skutočnosti, že zamestnanci, čo ho budú vykonávať, úspešne absolvovali tréningovú časť. Časový plán testovania musí byť preto zosúladený s tréningovým a zároveň musí dbať na nenarušenie bežného chodu pobočky. Keďže testovať sa bude DMS systém Sharepoint, ktorý bude denne využívaný zamestnancami pri poskytovaní služieb zákazníkom, optimálne by bolo testovať systém a jeho obnovu v rámci víkendov, resp. voľných dní, pokiaľ sa nejdená o testovanie schopnosti zamestnancov pohotovo reagovať na výpadok Sharepointu.

Plán testovania bude pozostávať z nasledujúcich krokov:

- **Design** - v rámci návrhu testovania sú definované obsahové oblasti, techniky testovania a očakávané výsledky. Po uskutočnení testovania sa nasledujúca tabuľka rozšíri o ďalšie stĺpce predstavujúce zaznamenanie skutočných výsledkov a následne potrebných zmien. Fáza designu testovania by mala byť ukončená presným zoznamom činností, dátumom ich uskutočnenia a kontrolným mechanizmom postupného spĺňania činností, pričom tento zoznam by si mal zachovať flexibilný charakter umožňujúci priebežné úpravy.

Tabuľka 21 - Oblasti testovania výpadku systému, Zdroj: Vlastné spracovanie

Oblasť	Scenár	Forma testu	Očakávaný výsledok	Frekvencia
Dostupnosť	Výpadok internetu	Manuálny test	Plynulé nadviazanie na záložného poskytovateľa v prijateľnom časovom limite podľa RTO/RPO	min. 1x mesačne, mimo pracovnú dobu
	Výpadok Sharepointu	Manuálny test schopnosti obnoviť dáta zo záložných diskových polí.	Sprístupnenie dát z lokálneho zdieľaného disku so zálohami v prijateľnom časovom limite podľa RTO/RPO	min. 1x mesačne
		Kontrola offline dostupnosti dokumentov kat.C	Dokumenty kat.C sú offline dostupné u každého kompetentného užívateľa	2 x mesačne
Integrita	Vymazanie, strata, pozmenenie dokumentov v Sharepointe	Zabezpečenie prístupu k lokálnej zálohe na diskoch ako aj offline užívateľských kópií, porovnanie veľkostí cieľových zložiek a zdrojových zložiek	Sprístupnenie dát z lokálneho zdieľaného disku so zálohami v prijateľnom časovom limite podľa RTO/RPO	min. 1x mesačne

- **Rozvoj** - ďalším krokom prípavy testovania je zabezpečiť testovaciu dokumentáciu, ktorá sa bude spracovávať pred, počas a po skončení testovania. Typická dokumentácia môže

pozostávať z úvodného prehľadu a cieľov testovania, konkrétneho plánu, návodu k jednotlivým testom a report zaznamenávajúci výsledky testovania.

- **Správa a hodnotenie** - Uskutočnením testovania podľa prechádzajúceho plánu a jeho finálnym zhodnotením končí jeden testovací cyklus. Na základe jeho vyhodnotenia sa určí ďalší vývoj testovania, ako aj prípadné okamžité nápravné opatrenia.

5.5.1.6 Spôsob udržiavania plánu obnovy DMS

Aby prinášal navrhnutý plán obnovy DMS Sharepoint v pobočke správny efekt, je potrebné ešte pridať posledný krok – zabezpečiť kontinuálne udržiavanie BCM plánu. V rámci udržiavania sa chápe aktualizačná činnosť, ktorá zabezpečí súlad vývoja životného cyklu systému Sharepoint a plánu na jeho obnovu. Udržiavanie musí myslieť na vývoj HW,SW, technických procesov, bezpečnostné a operačné požiadavky, či na aktualizáciu v zozname ľudí zodpovedných za DMS Sharepoint a plán jeho obnovy. Aktualizovanie plánu je možné nastaviť v pravidelných intervaloch podľa požiadavkov spoločnosti, ideálne v polročnom intervale, pričom v prípade akýchkoľvek výrazných systémových zmien, ktoré môžu mať dopad alebo súvis s podnikovým SharePointom, je aktualizácia nevyhnutnosťou.

5.5.1.7 Podniková smernica

Plán obnovy systému SharePoint Online musí byť v pobočke spracovaný internou smernicou. Tá plánu dodá presný rámec pravidiel a postupov, ktorých sa kompetentní zamestnanci môžu držať a manažérom kontrolný nástroj, na ktorý sa je možné v prípade nesúladov odvolávať. Pobočka by bez smernice v prípade straty dát alebo systémových porúch nemala na koho previesť zodpovednosť a všetky riziká by znášala ako celok na vlastný účet. Preto musí byť v smernice navrhnutý aj spôsob znášania následkov nedodržania stanovených pravidiel. Možným riešením je prvé napomenutej zodpovednej osoby a následne v závislosti od výšky spôsobenej škody percentuálne zrážky z vyplácaných finančných bonusov.

Interné smernice majú v podniku presne stanovenú štruktúru (viď. príloha C) a sú vypracovávané v anglickom jazyku. Obsahová náplň danej smernice bude pozostávať z chronologicky usporiadaných návrhových informácií uvedených v celej podkapitole 5.5.1, pričom musia byť rozlíšené konkrétne scenáre a konkrétne postupy znovuobnovy. Jednotlivé kroky, v prípade rôznych scenárov, ako napríklad zálohovací systém, môžu byť vypracované

formou samostatných priložených procesných dokumentov. Všetky zmeny v pláne či stratégii obnovy budú organizované pod vedením koordinátora obnovy DMS, ktorý každú zmenu zaznamenáva do smernicovej dokumentácie, s dátumom jej odsúhlasenia a s pridelenou zodpovednou osobou za konkrétnu zmenu.

V rámci udržiavania plánu obnovy SharePointu v servisnej pobočke je nevyhnutné myslieť aj na kópiu a zálohu plánu uložených na bezpečnom mieste, ku ktorému sa v prípade krízovej udalosti bude možné rýchlo dostať.

5.5.2 Vzdelávací program a SAE

Už snáď známou skutočnosťou v oblasti zabezpečenia podnikových informačných systémov je jeho najslabší článok - ľudský faktor. Je to oblasť, ktorú si už dnes žiadna globálna organizácia, akou je Zebra, nemôže dovoliť zanedbať a ohroziť tak dostupnosť, integritu a dôvernosť svojich informačných systémov, či dát. Každý užívateľ, ktorý prichádza do styku s podnikovými IT systémami, musí rozumieť, aká je rola a zodpovednosť IT v ohľade na hlavnú podnikovú misiu, akú IT politiku a procesy firma presadzuje a ako má správne s IT nástrojmi zaobchádzať a využívať ich pri svojej činnosti.

Vzhľadom k implementácii nového DMS systému do servisnej pobočky Zebry, navyše priamo vo forme cloudového riešenia, je nevyhnutnosťou zvýšiť povedomie zamestnancov a poskytnúť im adekvátny tréning na porozumenie tejto zmeny a rizík, ktoré so sebou prináša. Cieľom tejto časti je preto navrhnúť systém budovania povedomia a tréningového programu špecializovaného na cloudové riešenie MS SharePointu 2013, v ktorom budú zamestnanci čoskoro denne pracovať. Tento vzdelávací program by mal v sebe zahrnúť predovšetkým informácie o bezpečnostných hrozbách, ktoré s novým systémom prichádzajú a ako nim prechádzať, o pláne obnovy systému v prípade jeho výpadku. Program by mal však zahrnúť aj informácie o Sharepointe ako takom a o jeho funkcionalite. Spracovaný bude najskôr návrh programu, jeho rozvoj, implementovanie a poimplementačná fáza.

5.5.2.1 Návrh programu

- **Model programu**

Program budovania bezpečnostného povedomia by mal v prvom rade nasledovať potreby a ciele celej spoločnosti Zebra a korešpondovať s podnikovou kultúrou a IT architektúrou

brnenskej servisnej pobočky. Návrhom je, aby systém, akým bude aplikovaný do servisnej pobočky, bol plne decentralizovaný systém. V takom prípade centrálna autorita zaoberajúca sa bezpečnostnou politikou firmy a hlavný CIO Zebry poskytnú hlavné očakávania, no všetko ostatné, zahŕňajúc ohodnotenie potreby budovania povedomia, rozdeľovanie prideleného rozpočtu, plán tréningov, materiály aj implementáciu, má na starosti samotná pobočka. Takýto model si priamo žiada vytvorenie lokálneho bezpečnostného programu a lokálnej pozície CIO v rámci pobočky, ako určitý podsystém zodpovedajúci sa centrálnemu bezpečnostnému vedeniu v Amerike. Navrhovaný model tvorby vzdelávacieho programu je načrtnutý na nasledujúcom obrázku.

Obrázok 25 - Decentralizovaný model nasadenia vzdelávacieho programu, Zdroj: Vlastné spracovanie podľa (19)

- **Zodpovedné osoby**

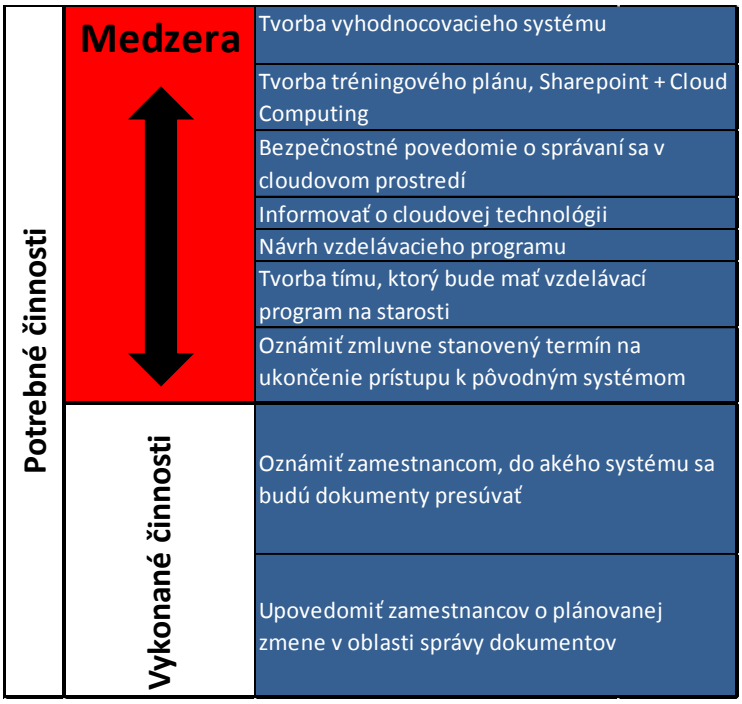
V úvode návrhu programu je prvoradé stanoviť zodpovedné osoby za celý program navrhovaného vzdelávania. Spoločnosť Zebra, ako celok, má oddelenie zaoberajúce sa IT bezpečnosťou, poskytujúce podporu a základné školenia zamestnancom v tejto oblasti. V brnenskej pobočke však zatiaľ žiadna zodpovedná osoba, ktorá by mala na starosti IT bezpečnosť nie je. Ako už bolo v úvodnej analýze spomenuté, lokálne IT oddelenie pozostáva v súčasnosti len z 3 zamestnancov, ktorí riešia prevažne pobočkovú operatívu bez hlbšieho zaoberania sa bezpečnostnými otázkami. Novovzniknuté hrozby z implementácie cloudového riešenia DMS preto ostávajú neriešené.

Rovnako, ako v návrhu plánu obnovy Sharepointu z prechádzajúcej podkapitoly, by bolo v ideálnom prípade riešením vytvorenie osobitnej lokálnej CIO pozície, ktorá by prevzala zodpovednosť za komplexné riadenie IT bezpečnosti v servisnom stredisku. Vzhľadom k šetreniu nákladov, jednak časových, ako aj finančných, je možnosťou aj prispôsobenie činností aktuálneho lokálneho manažéra IT oddelenia na problematiku bezpečnosti IT. Manažér by predstavoval následne aj rolu CIO, pričom výhodou je jeho aktuálna vysoká znalosť a prehľad miestnych IT technológii a prostredia.

Mať osobu zaoberajúcu sa otázkami bezpečnosti IT je podľa môjho názoru pre pobočku veľmi potrebné, keďže bezpečnostný incident môže v reálnom čase spôsobiť pobočke veľké problémy a CIO a IT Security vedenie v Amerike sa o problémoch dozvie až s časovým posunom niekoľko hodín. Spoločnosť je navyše dodávateľom svojich produktov do subjektov kritickej infraštruktúry, čo s ohľadom na aktuálne rozvíjajúcu sa legislatívu bude do budúcna nie len veľmi potrebné ale aj nevyhnutné. Chýbajúcu pracovnú silu v oddelení IT by spoločnosť mohla doplniť najatím nových pracovných síl na operatívnu IT činnosť.

Ohodnotenie potrieb spoločnosti a jednotlivých skupín užívateľov

Potreba tréningu a programu budovania povedomia o nových bezpečnostných hrozbách plynúcich z migrácie celopodnikovej dokumentácie do cloudu Sharepointu vyplýva pobočke automaticky. Z nasledujúceho obrázku je zrejmé, aké činnosti pre oboznámenie zamestnancov s plánom zavedenia Sharepointu v cloude pobočka aktuálne vykonáva a aké činnosti sú potrebné aby vykonávala. Vzniká teda veľká medzera, ktorú je potrebné správnym programom SAE vyplniť.



Obrázok 26 - Potrebné vs. vykonané činnosti v rámci vybudovania vzdelávacieho povedomia ohľadom nového DMS, Zdroj: Vlastné spracovanie podľa (19)

5.5.2.2 Plán programu SAE

Plán programu SAE vzťahujúceho sa k pripravovanej implementácii sa musí podriadiť celkovému časovému harmonogramu projektu. Informovanie a vzdelávanie sú projektové činnosti, na ktoré nadväzujú podmienečne ďalšie činnosti a preto sú pevne určené priority a poradie, koho je potrebné vyškoliť a kedy. Hlavná priorita po všeobecnom Awereness programe je pridelená tréningu stredne pokročilých a pokročilých užívateľov, teda administrátorom, manažérom a vedeniu, ako aj tým, ktorí budú pripravovať štruktúru, prístupové oprávnenia v Sharepointe. Tréning bežných užívateľov je potrebný až po vybudovaní hlavnej štruktúry webového portálu.

V nasledujúcich dvoch tabuľkách sú uvedené postupne plány vzdelávania ohľadom funkcionality SharePointu a následne plán programu SAE ohľadom technológie cloud Computing a jej zabezpečeniu.

Tabuľka 22 - Plán vzdelávacieho programu, Zdroj: Vlastné spracovanie

Vzdelávací plán	Awareness	Training			Education
Hlavná téma	MS Sharepoint 2013 Online	Bezpečnosť v prostredí Cloud Computingu			MS Sharepoint 2013
Obsahová náplň	Hlavný cieľ zmeny DMS, Hlavný účel MS SP, možnosti, výhody, nové hrozby	Charakteristika CC, výhody a nevýhody, bezpečnostné hrozby, bezpečnostné tipy, zoznam bezpečnostných zodpovedností a povinností			Vývoj, nové trendy, možnosti customizácie, business intelligence v SP,...
Úroveň	**Všetci zamestnanci**	**Začiatočníci**	**Stredne pokročilí**	**Pokročilí**	**Špecialisti na Sharepoint a Cloud Computing**
		Funkčné rozdelenie			
Cieľové skupiny	Všetci zamestnanci	Budúci užívatelia systému	Administrátori, IT oddelenie	Manažéri, TL, CIO, IT Security	Priraďovaný v závislosti od aktuálnych potrieb a rozdelené podľa profesne vykonávaných činností a funkcií
Požadovaný výstup	Zamestnanci sú si vedomí pripravovanej zmeny, rozumejú funkčným výhodám a bezpečnostným hrozbám nového riešenia	Identifikovať, Definovať, Participovať	Rozumieť, Interpretovať, Spracovať	Analyzovať, Určovať, Schvaľovať	Rozvíjať, Odhadovať, Plánovať,
Účasť	Povinné	Povinné			Voliteľné
Frekvencia	V závislosti od potreby	min 1xRočne	min 1xRočne	min 1xRočne	V závislosti od potreby

Tabuľka 23- Plán programu SAE, Zdroj: Vlastné spracovanie

Plán SAE	Awareness	Training			Education
Hlavná téma	Cloud Computing	Bezpečnosť v prostredí Cloud Computingu			Bezpečnosť v prostredí Cloud Computingu
Obsahová náplň	Definícia technológie, Výhody a Hrozby, Optimálne správanie sa užívateľov v prostredí CC	Charakteristika CC, výhody a nevýhody, bezpečnostné hrozby, bezpečnostné tipy, zoznam bezpečnostných zodpovedností a povinností			Vývoj zabezpečovacích opatrení, nové hrozby, nové trendy CC,..
Úroveň	**Všetci zamestnanci**	**Začiatočníci**	**Stredne pokročilí**	**Pokročilí**	**Špecialisti na Sharepoint a Cloud Computing**
		Funkčné rozdelenie			
Cieľové skupiny	Všetci zamestnanci	Budúci užívatelia systému	Administrátori, IT oddelenie	Manažéri, TL, CIO, IT Security	CIO, IT Security, Priraďovaný v závislosti od aktuálnych potrieb zamestnancov podľa ich funkcií
Požadovaný výstup	Zamestnanci sú si vedomí pripravovanej zmeny, rozumejú funkčným výhodám a bezpečnostným hrozbám nového riešenia	Identifikovať, Definovať, Participovať	Rozumieť, Interpretovať, Spracovať	Analyzovať, Určovať, Schvaľovať	Rozvíjať, Odhadovať, Plánovať,
Účasť	Povinné	Povinné			Voliteľné
Frekvencia	V závislosti od potreby	min 1xRočne	min 1xRočne	min 1xRočne	V závislosti od potreby

Vypracovaný plán je potrebné komunikovať s vyšším vedením zodpovedným za schválenie financovania programu. Lokálny CIO zo servisnej pobočky práve pomocou uvedeného plánu komunikuje požiadavky na finančný rozpočet. Ten môže byť vyjadrený napríklad formou percentuálneho vyjadrenia z celkového IT rozpočtu prideleného pre brnenskú pobočku.

5.5.2.3 Rozvoj programu

V časti rozvoja konkrétneho programu sa vypracováva návrh obsahovej štruktúry a s tým súvisiaca príprava vzdelávacích materiálov a ich zdrojov. Rozlišuje sa rozvoj budovania povedomia a rozvoj tréningového programu.

Budovanie povedomia

Povedomie musí byť budované u všetkých zamestnancov pobočky. Musí ich totiž všetkých oboznámiť s ich spoločnými zodpovednosťami v rámci zavádzania nového DMS a informačnej bezpečnosti s tým súvisiacej.

- **Výber hlavných tém**- Zmena v systémoch so správou dokumentov, plánovaná migrácia, centralizácia (online v cloude), Výhody nového riešenia a cloudu, Ako to môže prospieť ich činnosti, aké nové hrozby môžu ich činnosť ohroziť.
- **Príprava materiálov** – chceme zamestnancov oboznámiť s plánovaným projektom migrácie všetkých podnikových dokumentov do nového DMS systému Sharepoint v cloudovom prostredí.
- **Zdroje materiálov** – online akadémie- Microsoft Virtual Academy, Národné centrum kybernetickej bezpečnosti ČR, normy NIST- odporúčania pre zabezpečenie cloudových riešení, odporúčania budovania SAE, poskytovateľ SW riešenia- Microsoft a jeho materiály, periodiká, konferencie, semináre, kurzy.

Rozvoj tréningového programu

Tréning je na rozdiel od povedomia určený len čisto špecifickej skupine, v ktorej sa v rámci úrovne jej pokročilosti školia účastníci ohľadom všetkého, čo sa týka funkčnosti a bezpečnosti Sharepointu a cloudu, v rámci ich špecifických pracovných povinností.

- **Príprava materiálov** – materiály budú obsahovať informácie o softwarovom produkte Sharepoint 2013, o spôsobe jeho implementácie do podniku, o jeho údržbe, vývoji a funkcionalite. Materiály budú predávané formou školení, seminárov, online seminárov, prípadne poskytnutím potrebných zdrojov k samoštúdiu.

- **Zdroje materiálov** - navrhovanou možnosťou pre pobočku je kombinácia interných a externých zdrojov. Pobočka by mala využiť znalosť interných pracovníkov spoločnosti, ktorí už podobné projekty absolvovali v rámci iných pobočiek a spravujú Sharepoint v Zebre na globálnej úrovni. V rámci efektívnosti tréningu, by bola najoptimálnejšia ich osobná účasť, fyzická alebo formou webových seminárov. Rovnako by sa mali využiť dostupné materiály od spoločnosti Microsoft. Tá formou Microsoft Virtual Academy zdarma sprostredkováva množstvo potrebných informácii o svojich produktoch. S ohľadom na bezpečnosť v cloudovom prostredí sú dobrými zdrojmi vzdelávacích materiálov americké normy NIST, ktoré sú zdarma dostupné na internete a vďaka americkému pôvodu spoločnosti Zebra aj informačne vhodné.

- **Spracovanie tréningového rozpisu** - nasledujúce tabuľky predstavujú plány tréningov v oblasti cloudovej bezpečnosti aj funkčnej špecializácie systému Sharepoint. Plán rozlišuje rozdielne fuknčné zameranie sa zamestnancov v sledovanej oblasti.

Bezpečnosť v cloudovom prostredí

Funkčné zameranie

Oblasť tréningu	A Manažment (+ CIO)	B Implementácia, Administrátorstvo	C Design, Vývoj	D Audit	E Užívatelia	F Externí užívatelia	G Ostatní
1.Zákony a regulácie	1A	1B	1C	1D	1E	1F	
2.Bezpečnostný program	2A	2B	2C	2D	2E	2F	
2.1 Plánovanie, BCM	2.1A	2.1B	2.1C	2.1D			
2.2 Manažment	2.2A	2.2B		2.2D			
3.Bezpečnostný systém v Cloude	3A	3B	3C	3D	3E	3F	
3.1 Zahájenie	3.1A	3.1B	3.1C	3.1D			
3.2 Rozvoj	3.2A	3.2B	3.2C	3.2D			
3.3 Test a hodnotenie	3.3A	3.3B	3.3C	3.3D			
3.4 Implementácia	3.4A	3.4B	3.4C	3.4D			
3.5 Operatíva	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	
3.6 Ukončenie	3.6A	3.6B		3.6D			
4. Ostatné							

Obrázok 27 - Plán tréningu v oblasti bezpečnosti cloudového prostredia, Zdroj: Vlastné spracovanie

	Funkčná špecializácia v prostredí DMS Sharepoint Funkčné zameranie						
Oblasť tréningu	A Manažment (+ CIO)	B Implementácia, Administrátorstvo	C Design, Vývoj	D Audit	E Užívatelia	F Externí užívatelia	G Ostatní
1.Hlavná politika, smernice	1A	1B	1C	1D	1E	1F	
2.Program implementácie SP	2A	2B	2C	2D	2E	2F	
2.1 Plánovanie	2.1A	2.1B	2.1C				
2.2 Manažment	2.2A	2.2B		2.2D			
3.Implementácia SP	3A	3B	3C	3D	3E	3F	
3.1 Zahájenie	3.1A	3.1B	3.1C				
3.2 Rozvoj	3.2A	3.2B	3.2C				
3.3 Test a hodnotenie	3.3A	3.3B	3.3C	3.3D	3.3E	3.3F	
3.4 Úpravy, údržba	3.4A	3.4B	3.4C	3.4D			
3.5 Ukončenie, spustenie	3.5A	3.5B	3.5C				
3.6 Vývoj	3.6A	3.6B	3.6C				
4.Funkcionalita SP	4A	4B	4C	4D	4E	4F	
4. Ostatné							

Obrázok 28 - Plán tréningu v oblasti funkčnej špecializácie v prostredí SharePoint Online, Zdroj: Vlastné spracovanie

5.5.2.4 Implementovanie programu

Implementačná fáza plynulo nadväzuje na predchádzajúce kroky procesu budovania bezpečnostného povedomia. Spôsob, akým bude vzdelávanie predávané, vychádza z plne decentralizovaného modelu programu. Pobočka si teda na základe centrálne nastavenej bezpečnostnej politiky a očakávaní z vedenia sama implementuje vzdelávací program a zabezpečí vzdelávací materiál, pričom centrálnemu vedeniu musí reportovať priebeh. Sama sa rozhoduje aj o konkrétnom spôsobe odovzdávania vzdelávacích materiálov zamestnancom, pričom možným návrhom sú nasledujúce spôsoby:

- Spôsob šírenia materiálov pre budovanie povedomia je možné navrhnút rôznymi formami. Odporúčam spoločnosti vyhnúť sa hneď na začiatku tradičnej forme školení a zvoliť úvodom napríklad výrazný hromadný e-mail informujúci o veľkej plánovanej zmene. Súčasťou by mohlo byť inšpiratívne informačné video o konkrétnych výhodách plánovaného cloudového riešenia, no zároveň zvýraznenie nových potenciálnych hrozieb, ktoré môžu vzniknúť. Program môže byť následne priebežne posilňovaný informačnými plagátmi, webovými konferenciami atď…

- Spôsob šírenia tréningových materiálov môže byť riešený kombinovanou formou interných, lektorom vedených školení, v kombinácii s webovými, či newebovými konferenciami alebo interaktívneho video tréningu.

5.5.2.5 Postimplementácia

Program vzdelávania nie je implementáciou ešte zďaleka ukončený. Veľmi významnou fázou je zabezpečenie spätnej väzby, či už od účastníkov, lektorov, alebo aj formou návratnosti investície do programu SAE. V tejto postimplementačnej fáze sa zvykne program ohodnocovať postupne z hľadiska 4 odlišných levelov:

- **Level 1** – Ohodnotenie zo strany uchádzačov a ich spokojnosti s tréningom, ukáže, či bola v programe vhodne zvolená forma, model a tréningové materiály.

- **Level 2** – Meranie efektívnosti tréningu, zisťovaním, aké množstvo znalostí bolo uchádzačom poskytnuté. Pre začiatočníkov je vhodné aplikovať pred-test a po-test a porovnať úroveň znalostí pred a po tréningu. Stredne pokročilým uchádzačom je možné zadať tematickú prípadovú štúdiu na vypracovanie a skupine pokročilých účastníkov sa môže dať napísať krátka esej skúmajúca pochopenie potrebných konceptov. V tomto leveli sa zhodnocuje objektívnejšou formou, čo si uchádzači odniesli zo školenia v porovnaní s pôvodne nastavenými cieľmi. Vďaka ohodnoteniu programu na druhom leveli je možné často zistiť potrebu opakovania kurzu, prípadne úpravu formy alebo materiálov.

- **Level 3** – Hodnotenie zvyšovania pracovnej výkonnosti z dôvodu uskutočneného tréningu, dotazovaním vedúcich pracovníkov alebo priamym dlhodobejším pozorovaním uchádzačov, možnosťou sú aj náhodné testy formou social engineering o dodržovaní bezpečnostných zásad.

- **Level 4** – Vyhodnotenie vzniknutých benefitov pre organizáciu, resp. efektivita tréningového programu. Finančne vyhodnotiť návratnosť z investície do vzdelávania a budovania povedomia je pomerne náročné. Ušetrenie nákladov by totiž vzniklo v prípade bezpečnostného incidentu, ktorému by sa vďaka školeniam predišlo. Je teda možné istým spôsobom vyhodnocovať, či sa zmenšujú počty bezpečnostných incidentov alebo napadnutí alebo sa vďaka vyškoleným užívateľom znížia náklady na udržiavanie bezpečnosti v pobočke. Pre pobočku je každopádne výhodné evidovať podobné štatistiky a vyhodnocovať, či sa jej viac oplatí investovať peniaze do zaučenia všetkých užívateľov k tomu, ako sa brániť bezpečnostným hrozbám, alebo je výhodnejšie investovať do kvalitnejšieho vzdelania pre užší okruh špecialistov, ktorí dokážu systém lepšie zabezpečiť.

Kvalitné ohodnotenie musí mať priamu väzbu na stanovené ciele a preto sa uvedené 4 hodnotiace levely porovnávajú s pôvodne nastavenými očakávaniami jednotlivých typov tréningov. Indikátormi úspechu sú pritom pozitívne odpovede na nasledujúce otázky :

Tabuľka 24 - Spôsoby ohodnotenia nastavených očakávaní zo vzdelávacieho programu, Zdroj: Vlastné spracovanie

	Ohodnotenie nastavených očakávaní			
Level hodnotenia→ Typ tréningu↓	**L1** **Spokojnosť študentov**	**L2** **Efektívnosť učenia**	**L3** **Efektívnisť realizácie**	**L4** **Efektívnosť programu**
Awareness	Ako dobre vstrebali účastníci nové informácie?Ako veľmi sú s plánovanou zmenou spokojní?	Ako dopadol po-test v porovnaní s pred-testom?	Ako dobre využívajú účastníci získané informácie v dennej pracovnej činnosti?	Znížila sa kritickosť a počet bezpečnostných incidentov? Zrýchlila sa obsluha zákazníkov vďaka Sharepointu?
Training	Ako dobre naplnil tréningový program očakávania účastníkov?	Dokázal tréning dostatočné a preukázateľné zvýšenie rozsahu znalostí účastníkov?	Ako dobre aplikujú účastníci nadobudnuté znalosti pri pracovných požiadavkách?	Znížila sa kritickosť a počet bezpečnostných incidentov? Zrýchlila sa obsluha zákazníkov vďaka Sharepointu?
Education/PD	Zabezpečilo vzdelávanie profesný rozvoj a zvýšenie kvalifikácie v odbore účastníkov?	Dokázal účastník adekvátne aplikovať nadobudnuté vzdelanie v reálnych prípadoch v praxi?	Ako dobre využíva účastník nadobudnuté vzdelanie pre napĺňanie celopodnikových cieľov a zámerov?	Znížila sa kritickosť a počet bezpečnostných incidentov? Zrýchlila sa obsluha zákazníkov vďaka Sharepointu?

V prípade, že ohodnotenie programu spĺňa počiatočné požiadavky v dostatočnej miere, môže sa vzdelávací program rozvíjať ďalej v rovnakom duchu poďla plánu. V opačnom prípade sa na problémové miesta programu aplikujú potrebné zmeny a úpravy. Celý uvedený proces vzdelávacieho programu sa musí rovnakým spôsobom, ako v prípade plánu obnovy, aplikovať do pobočky formou podnikovej smernice, dodržaním stanovenej štruktúry v prílohe C.

5.5.3 Viac-faktorová autentifikácia pre Sharepoint Online

Zabezpečenie dôvernosti dokumentov v DMS systéme Sharepoint Online je pre pobočku, hneď po dostupnosti, druhou významnou prioritou. V podnikovej smernici Zebry je jasne definovaná požiadavka na dvojfaktorovú autentifikáciu všetkých užívateľov, ktorí sa prihlasujú do firemnej siete externe, bez firmou zabezpečenej VPN. Sharepoint Online je ideálnym príkladom takého užívateľského prístupu. Cloudové riešenie totiž so sebou prináša

až príliš jednoduchý prístup užívateľov do podnikového systému, z akéhokoľvek miesta a zariadenia s prístupom na internet. Užívateľovi pritom stačí užívateľské meno a heslo, ktoré si v prípade tých lenivejších užívateľov jenoducho zapamätajú webové prehliadače aj automaticky. Čo sa zdá byť užívateľsky veľmi praktické, prinesie však pobočke nové bezpečnostné hrozby v podobe neautorizovaných prístupov k interným dátam a následné narušenie integrity dát, teda neautorizovanú modifikáciu, odcudzenie alebo stratu.

Keďže pobočka v rámci migrácie dokumentových úložisk do Sharepointu presunie veľké množstvo dôležitých dokumentov, ktorých neoprávnené odcudzenie by spôsobilo obrovské škody, mala by vytvoriť bezpečenejší prístupový mechanizmus jednotlivých užívateľov do systému. V prípade riešeného DMS systému navrhujem preto pobočke využiť bezpečnostnú funkcionalitu systému Sharepoint navrhnutú priamo spoločnosťou Microsoft. Dvojfaktorová autentifikácia užívateľov je v cloudovom riešení Sharepointu navrhnutá veľmi intuitívne, takže jej zavedenie zabezpečí hlavný administrátor jednoduchým nastavením. Postup nastavenia a priebeh dvojúrovňovej autentifikácie je znázornený v prílohe D.

Veľkou výhodou tohto riešenia je skutočnosť, že jeho jednoduchá implementácia je užívateľom SharePointu umožnená bez dodatočných nákladov, pričom sa očakáva dostatočný bezpečnostný účinok pre prípadné pokusy o neautorizovaný prístup do Sharepointu.

5.5.4 Návrh managementu prístupových oprávnení k dokumentom

K zabezpečeniu ďalšej priority - integrity dokumentov, existuje obdobne, ako v predchádzajucom návrhu, riešenie od spoločnosti Microsoft aplikovateľné špeciálne pre prostredie cloudovej verzie SharePointu. Systém Microsoft Azure Rights Management je pobočke navrhovaný z dôvodu všetkých nasledujúcich uvedených výhod, ktoré jej môže priniesť:

Tabuľka 25 - Výhody softwaru Microsoft Azure Rights management, Zdroj: Vlastné spracovanie podľa (14)

Využiteľné výhody systému Microsoft Azure Rights Management	
+	**Zabezpečenie všetkých typov dokumentov, úzke prepojenie s MS Office**
+	**Zabezpečenie súboru bez ohľadu na jeho neskoršie fyzické presuny či kópie**
+	**Možnosť auditovania a monitorovania zaobchádzania so zabezpečeným dokumentom**
+	**Podpora od rôznych operačných systémov a zariadení**
+	**Intuitívna a rýchla aplikácia systému**
+	**Podpora cloudového riešenia**
+	**Podpora flexibilných zmien množstva dokumentov**
+	**Možnosť rýchlo nastaviteľnej flexibilnej prístupovej politiky pre administrátorov aj užívateľov, tvorba prednastavených šablón prístupových oprávnení pre užívateľské skupiny**
+	**Defaultná možnosť prístupu k dokumentom autorizovaným osobám(admin) uľahčuje správu v prípade fluktuácie správcov obsahu**
+	**Auditovací systém formou sledovania užívateľských logov umožňuje sledovať pokusy o neoprávnené prístupy k dokumentom**
+	**Možná synchronizácia s Active Directory**
+	**Po zrušení služby MS Azure Rights Management sa nestratia prístupy k pôvodne zabezpečenému obsahu**

Aktivácia tejto technológie je pre oprávneného administrátora rovnako jednoduchá, ako v predchádzajúcom príklade, aktivuje sa jedným tlačítkom. Celý postup je uvedený v prílohe E. Aktiváciu musí mať na starosti hlavný administrátor, pričom môže prideliť odlišné oprávnenia k využívaniu tejto služby. Možnosťou je umožniť zamykať dokumenty a prideľovať na ne oprávnenia len manažérom, teamleaderom a vlastníkom obsahu, ktorí pracujú s najkritickejšími dokumentami. Ostatným užívateľom sa môžu prideliť len prístupové oprávnenia k čítaniu a editovaniu dokumentov, ku ktorým sú oprávnení.

Táto technológia je opäť doporučená hlavne vďaka svojmu výhodnému pomeru "pridaná hodnota/náklady vynaložené na jej získanie". Pobočka bude implementovať verziu Sharepoint Online – Office 365, Enterprise E3, ktorá systém Microsoft Azure RMS obsahuje automaticky a službu stačí len aktivovať bez ďalších doplnkových poplatkov.

5.5.5 Microsoft cloud app Security (SECaaS)

V časti návrhu by som rada spomenula ešte jednu možnosť využitia ďalšej služby od spoločnosti Microsoft, Microsoft cloud app Security, ktorá predstavuje novovznikajúci trend v oblasti servisných modelov - SECaaS (Security as a service- Bezpečnosť ako služba). Táto služba by pobočke zabezpečila komplexný kontrolný mechanizmus všetkých cloudových aplikácií a ich rozšírenú ochranu formou bezpečnostných upozornení či štatistík systémovej prevádzky.

Obrázok 29 - Užívateľské rozhranie Cloud App Security aplikácie, Zdroj: (15)

Bezpečnost cloudových aplikácii od Microsoftu je paušálne platenou službou, s cenou odvíjajúcou sa od počtu užívateľských licencií, 5 $/užívateľ/1 mesiac. Licenciu by mal mať pridelenú každý užívateľ, ktorého činnosť chceme v cloudovom prostredí monitorovať.

Bez ohľadu na cenu a na skutočnosť, že táto technológia nie je pre pobočku aktuálne bezpečnostne nevyhnutná, je brnenskej pobočke odporúčaná. Zahŕňa v sebe okrem potrebného zabezpečenia centralizovaný systém nastavenia politiky a bezpečnostných smerníc užívateľského správania sa v cloudovom prostredí, teda v SharePointe. Ponúka navyše automatizovaný auditný mechanizmus a teda možnosť priebežného zefektívňovania. Perspektívnou výhodou uvedenej služby je aj možnosť podpory všetkých aplikácií v cloudovom prostredí, nie len tých od spoločnosti Microsoft. To môže byť do budúcna pre pobočku veľkou výhodou, či už ekonomickou alebo aj konkurenčnou. Cloudové riešenia sa

budú totiž bezpochýb rozrastať aj v iných typoch podnikových aplikácii a mať možnosť kvalitnej a centralizovanej bezpečnostnej správy a politiky by bolo nenahraditeľné.

V prípade, že by sa pobočka chcela vyhnúť paušálnym poplatkom za túto službu, stále by jej zostala potreba vytvoriť vlastné smernice, politiky a jednoznačne definovať akceptovateľné správanie sa užívateľov v systéme Sharepoint. Rovnako by ju čakal aj návrh auditného systému, ktorý by musel byť riešený pravidelne pomocou externých auditorských organizácií.

5.5.6 Legislatívne nezrovnalosti

Činnosť poskytovateľa systému SharePoint, spoločnosti Microsoft so svojím sídlom v USA a dátovými centrami rozmiestnenými po celom svete, podlieha odlišnej legislatíve než servisná pobočka Zebry, sídliaca v Českej republike. Nedostatočné informácie o fyzickom umiestnení svojich dát môžu priniesť pobočke problémy s plnením národných zákonných požiadaviek, či s naplňovaním zmluvných podmienok so zákazníkmi a dodávateľmi. Jedná sa napríklad o právne riziká v súvislosti s medzinárodným presunom osobných a citlivých údajov, na ktorých zabezpečenie je potreba vhodných zmluvných ochranných opatrení.

Nakoľko nie je v priamej kompetencii servisnej pobočky vyjednávať zmluvné podmienky s Microsoftom, minimum, ktoré by mala pre zmiernenie nežiadúcich legislatívnych rizík urobiť, je informovať sa. Pre pobočku je skutočne dôležité vedieť, aké má práva a povinnosti vo vzťahu k poskytovateľovi a naopak.

Novinkou v tejto oblasti, ktorej naplňovanie by mala pobočka bezpochýb sledovať, je od februára 2016 vzniknutá dohoda *EU-U.S. Privacy Shield* (pre viac informácií viď. (24) (25)). Jej cieľom je stanoviť pravidlá pre ochranu európskych osobných a citlivých dát uložených v amerických spoločnostiach. Pre európske spoločnosti to znamená vyššiu transparentnosť zaobchádzania s ich dátami, vyššie zabezpečenie a garantované rýchle riešenie ich sťažností a námietok. Pre americké spoločnosti to znamená vysoké sankcie, v prípade nesplnenia pravidiel. Zaviazali sa totiž, že budú na základe pravidelnej kooperácie s európskymi inšitúciami v oblasti ochrany dát monitorovať a naplňovať európske bezpečnostné požiadavky. Microsoft sa k uvedenej medzinárodnej dohode vyjadril pozitívne a prisľúbil svoju participáciu na zvyšovaní zabezpečenia.

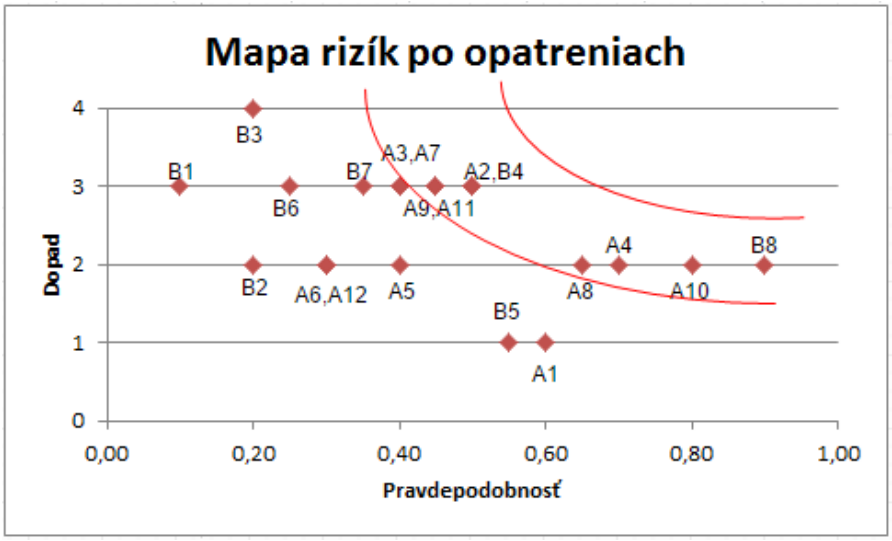
5.6 Analýza rizík po zavedení opatrení

Opatrenia voči zisteným rizikám z analýzy boli navrhnuté s cieľom znížiť pravdepodobnosť výskytu rizík, prípadne znížiť ich negatívny dopad na pobočku. V rámci zanalyzovania efektov navrhovaných opatrení na pobočku je vykonaná analýza rizík ešte raz, s prepočítanou hodnotou rizík po implementovaní všetkých navrhovaných bezpečnostných riešení. Výsledky sú graficky znázornené aj v mape rizík.

Tabuľka 26- Analýza rázik po implentovaní navrhnutých opatrení, Zdroj: Vlastné spracovanie

Analýza rizík súvisiacich s implementáciou DMS								
Číslo	**Scenár**	**Pravd.**	**Dopad**	**Hodnota rizika**	**Opatrenie**	**Nová pravd**	**Nový dopad**	**Nová hodnota rizika**
A	**Funkčné hrozby**							
A.1	Nevyužítý potenciál a funkcionalita DMS	0,90	1	0,90	Budovanie povedomia, Kontinuálny vzdelávací program, Zdôrazňovanie výhod centralizácie	0,60	1	0,60
A.2	Neustála decentralizovaná manipulácia s dokumentami	0,75	3	2,25		0,50	3	1,50
A.3	Neefektívny workflow v novom prostredí	0,70	3	2,10		0,40	3	1,20
A.4	Nesystematická a príliš rozvetvená štruktúra	0,70	2	1,40		0,70	2	1,40
A.5	Neefektívna spolupráca / workflow	0,40	2	0,80		0,40	2	0,80
A.6	Nutnosť využívať iné úložiská dokumentov	0,30	2	0,60		0,30	2	0,60
A.7	Časové náklady a spomalené podnikové procesy	0,40	3	1,20		0,40	3	1,20
A.8	Dlhá doba trvania implementácie	0,65	2	1,30		0,65	2	1,30
A.9	Strata nadväznosti a neefektívny prenos kompetencií	0,45	3	1,35		0,45	3	1,35
A.10	Nevyužívané stránky zaberajúce priestor	0,80	2	1,60		0,80	2	1,60
A.11	Nedostatočný dohľad, správa sa vymkne z rúk, ohrozená správna funkcionalita	0,85	3	2,55	Politika, Manažment prístupových oprávnení k dokumentom (RMS)	0,45	3	1,35
A.12	Strata niektorých dokumentov	0,60	4	2,40	BCM + Paralelné prechádzanie na nový systém DMS	0,30	2	0,60
B	**Bezpečnostné hrozby**							
B.1	Modifikácia, zničenie, strata dokumentov	0,40	4	1,60	Manažment prístupových oprávnení k dokumentom(RMS), Zálohovací systém	0,10	3	0,30
B.2	Nedostupnosť SharePointu	0,20	4	0,80	BCM plán	0,20	2	0,40
B.3	Prístup neoprávnených subjektov	0,70	4	2,80	Viacfaktorová autentifikácia, SECaaS	0,20	4	0,80
B.4	Nesystematické prideľovanie prístupových oprávnení	0,80	3	2,40	Politika, smernice, SAE, vzdelávací program	0,50	3	1,50
B.5	Nedostupnosť dokumentov v požadovaných lehotách	0,55	4	2,20	Zálohovací systém, BCM plán	0,55	1	0,55
B.6	Exponenciálny nárast chýb a exponenciálny pokles efektívnosti práce s DMS	0,75	3	2,25	Microsoft cloud app security-SECaaS, smernice, RMS	0,25	3	0,75
B.7	Nežiaduci a bezpečnostne nevyhovujúci obsah	0,80	3	2,40	SECaaS, SAE, Smernice,	0,35	3	1,05
B.8	Nedostupnosť, narušená integrita, dôveryhodnosť, náklady, pokuty,...	0,90	3	2,70	Proaktívne informovanie sa	0,90	2	1,80
Σ				**35,60**				**20,65**

Z analýzy vyplynulo, že aplikovaním navrhnutých opatrení by pobočka výrazne znížila hodnotu všetkých kritických bezpečnostných hrozieb.



Obrázok 30 - Mapa rizík po implementácií navrhovaných opatrení, Zdroj: Vlastné spracovanie

5.7 Ekonomická analýza

Praktická časť diplomovej práce prezentovala návrh proaktívnej eliminácie rizík plynúcich z cloudovej verzie DMS systému Sharepoint, do ktorého pobočka Zebry plánuje zmigrovať všetku podnikovú dokumentáciu. Keďže hodnotové podnikové aktívum, o ktoré sa tu predovšetkým jedná, sú podnikové dokumenty, návrhy predstavujú investície do IT zabezpečovacích riešení, ktoré zabránia narušeniu dostupnosti, dôvernosti a integrity týchto dokumentov v cloudovom prostredí.Investície do navrhovaných bezpečnostných opatrení predstavujú pre pobočku dodatočné náklady, ktoré bude firma ochotná vynaložiť len v prípade, že si bude istá pozitívnou návratnosťou tejto investície (ukazovateľ ROI- Return on Investment). To sa bude snažiť dokázať nadchádzajúca ekonomická analýza.

5.7.1 Návratnosť investície do bezpečnostných opatrení

Informácie obsiahnuté v dokumentoch majú pre pobočku rôznu hodnotu v závislosti od ich kategorického rozdelenia, tak ako bolo uvedené v BIA analýze. Táto hodnota sa dá pochopiť, ako možný finančný prínos pre pobočku plynúci z ich užívania ale aj ako finančný náklad v prípade ich straty. Predpokladom pritom je, že tieto náklady budú natoľko významné

a pre pobočku neprijateľné, že sa jej oplatí preventívne investovať peniaze do bezpečnostných opatrení. Prínosy z opatrení je potom možné definovať ako ušetrené náklady za riziko.

5.7.1.1 Náklady na navrhované bezpečnostné opatrenia

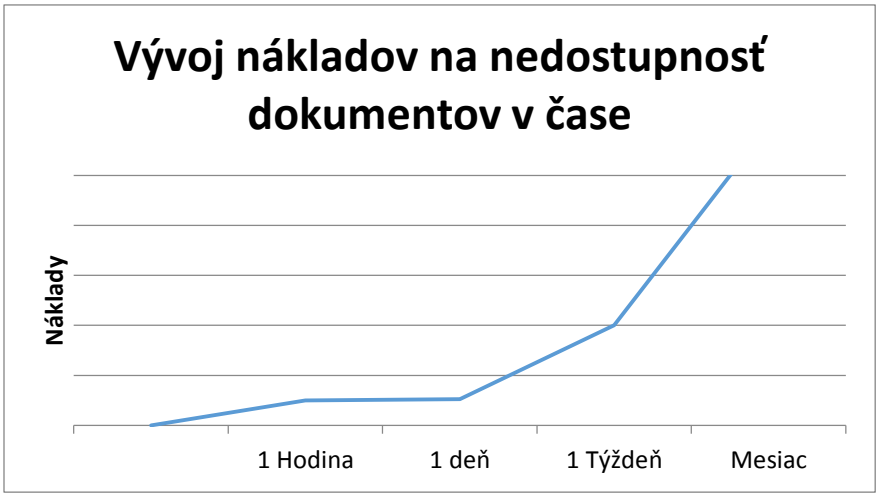
Navrhnuté opatrenia je možné približne finančne vyjadriť, pričom uvedené hodnoty predstavujú odhadované sumy získané za pomoci konzultácie so zodpovednými osobami z pobočky, na základe ich predošlých skúseností alebo predikcií. Personálne náklady berú do úvahy priemerné hodinové mzdové náklady na zamestnancov → 225 Kč, pričom ostatné operačné náklady na zamestnancov sú v tomto porovnaní zanedbané.

5.7.1.2 Náklady na potenciálne riziká

Vyčísliť presnú hodnotu nákladov na potenciálne riziká býva veľmi problematické. Jedná sa tu totiž o hypotetickú rovinu, o meranie niečoho, čo sa ešte nestalo a s čím pobočka nemá skúsenosť. Uvedená ekonomická analýza bude preto vyjadrovať hodnotu potenciálnych rizík nepriamo, formou nákladov ušlého zisku a ďalších finančných nákladov, ktoré by pobočke vznikli v prípade naplnenia scenárov hrozieb. Postup výpočtu nákladov rizík súvisiacich s jednotlivými hrozbami sa trochu líši:

- **Nedostupnosť dokumentov –** v prípade rizík zamedzenia dostupnosti dokumentov v Sharepointe, je potrebné rozlišovať nad časovým faktorom. V závislosti od rastúcej doby nedostupnosti sa totiž náklady exponenciálne zvyšujú, viď Obrázok 31:
  - **V prípade krátkodobej nedostupnosti (hodiny/max. 1 deň)** - Je potrebné uvažovať nad rizikom neschopnosti obsluhy prioritných zákazníkov, ktorí si za rýchly servis nadštandardne priplatili. Tí predstavujú síce len približne 30% podiel z celkového počtu zákazníkov (mesačne približne 5000), no ich percentuálny podiel na tržbách pobočky je väčšinový, približne 60% tržieb. Uvažujeme v takomto prípade teda o priemerných ušlých tržbách z prioritných zákazníkov, o odhadovaných nákladoch na penále za nesplnenie zmluvnej doby poskytnutia servisu a o nákladoch na pracovníkov helpdesku, ktorých čas je nevyužitý (približný počet zamestnancov je 150). Rovnako je potrebné ale uvažovať aj o ťažko vyčísliteľnom faktore straty dôvery prioritných zákazníkov, ktorý nie je možné vyčísliť.
  - **V prípade stredne dlhej doby nedostupnosti (týždeň)** – Keďže pevne stanovený termín obsluhy neprioritných zákazníkov sa pohybuje v intervale kratšom než je 1 týždeň, týždňový výpadok systému by k predchádzajúcim nákladom pridal náklady za príjmy zo servisu neprioritných zákazníkov, ako aj za stratu ich dôvery.
  - **V prípade úplnej straty dokumentov zo systému Sharepoint** – Náklady za úplnu stratu dokumentov v Sharepointe by pri úplnej strate nabrali nevyčísliteľný charakter. Hovoríme totiž o strate podnikových smerníc, definícii procesov, produktových špecifikácii, analýz a výsledkov interných auditov, informácií o zákazníkoch a

dodávateľoch, o strate knowledge management dokumentácie, plánovanej projektovej dokumentácie a teda aj nápadov, atď. Presné vyčíslenie v tomto prípade nie je možné, no strata takýchto dokumentov by mohla vyústiť k neschopnosti servisnej činnosti a obrovskej strate povesti firmy, zákazníkov či dodávateľov.



Obrázok 31- Náklady na nedostupnosť dokumentov v DMS systéme, Zdroj: Vlastné spracovanie

- **Užívateľská nespôsobilosť** - Neschopnosť užívateľov pracovať v novom systéme môže ústiť v predĺženej dobe obsluhy zákazníkov a teda hromadiacim sa požiadavkam zákazníkov a ich nespokojnosti, prípadne penálom za nedodržanie doby obsluhy. Užívatelia môžu zapríčiniť aj stratu dokumentov, prípadne v prípade nedodržiavania bezpečnostných smerníc aj bezpečnostné incidenty.
- **Narušenie dôvernosti systému –** Neautorizovanými prístupmi vznikajú pobočke náklady s únikom informácií a dát ku konkurencii alebo neoprávneným subjektom, s pokutami za zneužitie citlivých dát, za poškodenie systému, atď. Nezávislá štúdia spoločnosti IBM vykonávaná od roku 2013 preukazuje priemerné náklady na neuatorizovaný prístup a zneužitie podnikových dát na 90 mil CZK. (viď. (26)).
- **Narušenie integrity –** Náklady na činnosť bez odcudzených dát + náklady na ich znovuvytvorenie + náklady na náhrady škody zaintresovaným stranám. V Prípade odcudzenia je možné uvažovať nad výsledkami IBM štúdie, tak ako v predchádzajúcom príklade a teda škode minimálnej škode v hodnote 90 mil CZK
- **Absencia kontroly nad systémom –** V prípade neschopnosti systematickej a centralizovanej kontroly sa okrem rizík neefektívnej činnosti vystavuje pobočka dobrovoľne všetkým bezpečnostným rizikám v zvýšenej miere a teda zvyšuje pravdepodobnosť, že nastanú. Je v záujme samotnej pobočky robiť interný bezpečnostný audit, ktorý zaručí zákazníkom, že firma dbá na bezpečnostné opatrenia pri práci s dokumentami, ktoré často obsahujú informácie aj o nich. Zákazníci alebo právna zodpovednosť ho môžu v niektorých prípadoch striktne vyžadovať. Pobočka v Brne nemá aktuálne pracovnú kapacitu, ktorá by bola školená alebo oprávnená takýto audit vykonávať a spoločnosť by sa teda tak či tak musela obrátiť na externého poskytovateľa, ktorý by predstavoval náklad navyše.

- **Legislatívny nesúlad** – Náklady na neznalosť legislatívnych podmienok je možné vyjadriť v nevedomom porušovaní zákonných požiadaviek na zabezpečenie zaobchádzania s citlivými dátami alebo formou neschopnosti dostať sa k svojim dátam alebo k splneniu svojich bezpečnostných požiadaviek u poskytovateľa, v prípade krízovej situácie alebo havárie.

Nezanedbateľným prínosom zavedenia navrhovaných opatrení je aj zvýšenie zákazníckej dôvery a imagu firmy vďaka zvýšeniu dôrazu na zabezpečenie, spoľahlivosť a dostupnosť podnikových systémov. To môže byť v prípade skupiny zákazníkov, ktorí predstavujú často zložku kritickej infraštruktúry, nie len veľmi hodnotné ale aj požadované. Prínos je možné približne vyčísliť v očakávanom náraste počtu zákazníkov a teda aj ziskov firmy. Konkrétne hodnoty nákladov rizík (v CZK) v porovnaní s nákladmi na jednotlivé opatrenia voči nim sú uvedené v nasledujúcej Tabuľke:

Tabuľka 27- Finančné porovnanie nákladov rizík a navrhovaných opatrení, Zdroj: Vlastné spracovanie

Hrozba	Scenár rizika	Náklad na riziko	Opatrenie	SF náklady	HW náklady	Vstupné Personálne		Náklady spolu
						Počet osôb	Počet dní	
Nedostupnosť dokumentov	Výpadok DMS systému	↓	BCM spracovanie plánu obnovy	/	/	3	5	27 000
	Krátkodobý výpadok SharePointu	105 000	technológia One Drive	Zdarma súčasť Sharepointu,	/	2	3	10 800
	Dlhodobý výpadok Sharepointu/úplná strata dát	31 mil	lokálna disková záloha	v cene HW	3 mil	3	5	827 000
	Dlhodobý výpadok SharePointu/Lokálneho disku/úplná strata	>125 mil						
Užívateľská nespôsobilosť	Nesystematické, bezpečnostne nevyhovujúce zaobchádzanie so systémom	zvýšené časové náklady na servis → znížené príjmy, zvýšené penále	Vzdelávací program, SAE	zdarma interné + online dostupné zdroje, pokročilé vzdelávanie externým odborníkom neskôr v prípade potreby	/	3 + 350	5 + 2	1 287 000
Narušenie dôvernosti systému	Neautorizované prístupy do systému	>90000000	Viacfaktorová autentifikácia	Zdarma súčasť Sharepointu,	/	1	1	1 800
Narušenie integrity	Neautorizovaná zmena, zneužitie, odcudzenie, strata dokumentov	>90000000	Manažment prístupových oprávnení k dokumentom(RMS)	Zdarma súčasť Sharepointu,	/	3	10	54 000
Absencia kontroly nad systémom	Neexistujúci kontrolný mechanizmus a auditný systém	240000/rok + tvorba vlastných kontrolných mechanizmov	Microsoft cloud app security-SECaaS	5 $/užívateľ/1mesiac = 50 000 Kč	/	3	5	27 000 + 50 000 mes.
Legislatívny nesúlad	Právne nezrovnalosti, pokuty, neschopnosť hájiť svoje záujmy	Trestnoprávna zodpovednosť PO, prípadne konkrétnej FO	Informovanosť o EU-U.S. Privacy Shield	/	/	1	3	5 400
SPOLU								2 240 000 + 50 000 mes.

K uvedenému finančnému porovnaniu je nutné dodať, že sa v niektorých položkách jedná len o odhady približných hodnôt, keďže sa hlavne v rámci nákladov na riziká, pohybujeme v značne hypotetickej úrovni. Pri posudzovaní nákladov na riziká nedostupnosti dokumentov sa jedná o predpoklad, že by výpadok znemožnil servisné služby v celom rozsahu a teda sumy pozostávajú z ušlých tržieb prioritných a následne aj všetkých ostatných zákazníkov. V praxi by však dopad v závislostí od rôznych situácií a prvkov náhody nemusel dopadnúť až tak kriticky.

5.7.2 Zhodnotenie ekonomickej analýzy

Zložitosť vyjadrenie hodnoty bezpečnostných hrozieb je v uvedenom príklade umocnený ešte tým, že sa jedná o novo implementovaný cloudový systém, s ktorým nemá pobočka žiadne vlastné skúsenosti. Často totiž hrajú rolu faktory ako ohrozená povesť firmy, konkurencieschopnosť, dôvera u zákazníkov alebo strata duševného vlastníctva, čo nie sú presne finančne vyjadriteľné položky. Riziká môžu v takomto prípade nastať vo väčšom alebo menšom rozsahu oproti uvedenej tabuľke, no princíp výpočtu by ostal rovnaký.

Odhliadnúc od nejednoznačnosti niektorých nákladových položiek, cieľom tejto ekonomickej analýzy bolo dokázať, ako môže pobočka eliminovať všetky nájdené riziká s vynaložením minimálnych nákladov – Hodnota počiatočnej investície do všetkých navrhovaných opatrení zároveň by predstavovalo len čosi viac než 2,5 % priemerných mesačných čistých príjmov zo servisnej činnosti pobočky, priemerne sa pohybujúcich v hodnote 90 mil CZK. Pritom pravdepodobná hodnota nákladov na riziká, nadobúda mohonásobne vyššie hodnoty, aj keď ich naplnenie je sprevádzané prvkom nejednoznačnosti. O priamej návratnosti investícií by bolo možné hovoriť v prípade uskutočnenia nejakej z uvedených hrozieb a ich scenárov, kedy by vo väčšine prípadov boli náklady na opatrenia hneď navrátené.

Čo sa týka opatrenia aplikáciou Microsoft Cloud app security, tá by pobočke vytvorila navyše mesačnú paušálnu položku vo výške 50 000 CZK, no v porovnaní s objemom príjmov je to stále zanedbateľná suma. Táto technológia ostáva v rámci môjho návrhu pobočke odporúčaná napriek tomu, že nie je úplne nevyhnutná. Je to tak hlavne vďaka širokému spektru svojich výhod, ktoré môže pobočka do budúcna aplikovať širokospektrálne naprieč podnikom. O všetkých ostatných návrhoch osobne predpokladám, že sú pre pobočku vzhľadom k jej situácii nevyhnutné.

6 ZÁVER

Uvedená diplomová práca si stanovila za cieľ navrhnúť spôsob zavedenia DMS systému do vybranej organizačnej zložky spoločnosti. Rozhodla som sa pre servisnú pobočku nadnárodnej spoločnosti Zebra, sídliacu v Brne.Vplyvom organizačných a celoštruktúrnych zmien po uskutočnenej akvizícii sa dostala pobočka do príležitosti zefektívniť svoj aktuálne veľmi decentralizovaný systém správy dokumentov. Pod tlakom jednoznačných pokynov zo strany hlavného vedenia sa presadil ako systém riešenia služba spoločnosti Microsoft, SharePoint Online, využívajúci cloudovú technológiu.

Stavajúc na zanalyzovanej východiskovej situácii bolo v práci navrhnuté projektové riadenie plánovanej zmeny, prebiehajúce postupnosťou aplikovaného Lewinovho modelu. V rámci projektu bola vypracovaná aj analýza rizík, z ktorej vyplynuli ako najvýznamnejšie hrozby riziká súvisiace s presunom celopodnikovej dokumentácie do prostredia Cloud Computing. S cieľom eliminovať nájdené riziká v postupnosti, ktorá nasleduje priority pobočky kladúce na svoje dokumenty, sa navrhli možné bezpečnostné opatrenia. Medzi nimi systém BCM, vzdelávací program a SAE, dvoj-faktorová autentifikácia užívateľov, riadenie prístupových oprávnení k dokumentom, služba SECaaS a návrh zníženia negatívnych vplyvov legislatívnych nesúladov medzi poskytovateľom cloudového systému a servisnou pobočkou.

Ekonomickou analýzou v závere práce bola porovnaná finančná náročnosť implementácie jednotlivých opatrení s predpokladanou hodnotou nákladov, ktoré by priniesli príslušné riziká v prípade ich realizácie. Pomer prínosov a nákladov opatrení je pre pobočku aj vzhľadom k jej finančnej situácii určite prijateľný. Viacero z navrhnutých opatrení je navyše realizovateľných zdarma, s nákladmi len na ľudský faktor.Paušálne platené opatrenie formou služby SECaaS poskytovateľa nie je možno akuálne z bezpečnostného hľadiska pre pobočku nevyhnutné, no so svojím profilom dodávateľa do kritickej infraštruktúry budú na ňu pravdepodobne v blízkej budúcnosti kladené vyššie, zákonom dané bezpečnostné požiadavky. Vzhľadom k tomu je pobočke z mojej strany odporúčané venovať sa aktívne všetkým navrhovaným možnostiam opatrení, napriek zdanlivému komplexnému zabezpečeniu zo strany cloudového poskytovateľa.

Práca naplnila svoje pôvodne nastavené ciele a ponúkla pobočke vhodné alternatívy, ktoré jej umožnia plynulý prechod do nového DMS systému, minimalizujúc riziká a maximalizujúc jej úžitok. Verím, že práca bude v konečnom dôsledku praktickým prínosom nie len pre servisnú pobočku spoločnosti Zebra v Brne, ale aj iným subjektom zaoberajúcim sa podobnou problematikou.

7 ZOZNAM POUŽITEJ LITERATÚRY

(1) *Zebra*. [online]. [cit. 2016-04-16]. Dostupné na internete: <https://www.zebra.com/us/en.html>.

(2) KUNSTOVÁ,Renata.Efektivní správa dokumentu: Co nabízí Enterprise Content Management, Grada Publishing, a.s., 2009, 204 s. ISBN 978-80-247-3257-2

(3) *Znalostný manažment* [online]. [cit. 2016-04-16]. Dostupné na internete: < http://itlib.cvtisr.sk/archiv/2009/4/znalostny-manazment.html?page_id=1060>.

(4) GÁLA,Libor.POUR,Jan.TOMAN,Prokop.Podniková informatika, Grada Publishing, a.s., 2006,482 s. ISBN 80-247-1278-4

(5) *Manažment znalostí v praxi*. [online]. [cit. 2016-03-23]. Dostupné na internete: < http://www.riadenie.sk/manazment-znalosti-v-praxi-mladkova/>.

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

(7) ČSN EN 82045-1 (013740). Správa dokumentov- Časť 1: Zásady a metódy

(8) *Document management system* [online]. [cit. 2015-02-11]. Dostupné na internete: < http://www.docpath.com/art-document-management-system-project.aspx>.

(9) *Gartner magic quadrant enterprise content management 2015.* [online]. [cit. 2016-04-16].Dostupné na (10)interneternete<http://www.project-consult.de/ecm/news/2015/gartner_magic_quadrant_enterprise_content_management_2015>.

(10) *Enterprise content management 2015.* [online]. [cit. 2016-02-12]. Dostupné na internete: < https://www.g2crowd.com/categories/enterprise-content-management>.

(11) CURRY, Ben. Microsoft SharePoint 2010: kapesní rádce administrátora. Vyd.Brno: Computer Press, 2011, 647 s. ISBN 978-80-251-3401-6.

(12) *Microsoft OneDrive* [online]. [cit. 2016-05-03]. Dostupné na internete: < https://news.microsoft.com/presskits/onedrive/#sm.0001jpoqw71cxwdumwrd9583f36sq>

(13) *Multi factor authentificationf for Office 365* [online]. [cit. 2016-05-03]. Dostupné na internete: < https://blogs.office.com/2014/02/10/multi-factor-authentication-for-office-365/>

(14) *Set up Information Rights Management (IRM) in SharePoint admin center* [online]. [cit. 2016-05-04]. Dostupné na internete: < https://support.office.com/en-us/article/Set-up-Information-Rights-Management-IRM-in-SharePoint-admin-center-239ce6eb-4e81-42db-bf86-a01362fed65c>

(15) *Enterprise- grade security for your cloud apps* [online]. [cit. 2016-05-03]. Dostupné na internete: < https://www.microsoft.com/en-us/server-cloud/products/cloud-app-security/>

(16) *Sharepoint 2013 overview.* [online]. [cit. 2014-04-16]. Dostupné na internete: < https://products.office.com/en-us/sharepoint/sharepoint-2013-overview-collaboration-software-features>

(17) *NIST Special Publication 800-145*, The NIST Definition of Cloud Computing, U.S. Department of Commerce,2011

(18) *NIST Special Publication 800-34 Rev.1*, Contingency Planning Guide for Federeal Information Systems , U.S. Department of Commerce,2010

(19) *NIST Special Publication 800-50*, Building an Information Technology Security Awareness and Training Program, U.S. Department of Commerce,2003

(20) PITAŠ, Jaromír, 2012. Národní standard kompetencí projektového řízení verze 3.2: National standard competences of project management version 3.2. Vyd. 3., dopl. a aktualiz. Brno: Společnost pro projektové řízení, , 342 s. ISBN 978-80-260-2325-8

(21) RAIS,Karel.DOSKOČIL,Radek. Operační a systémová analýza 1. Vyd.Brno: CERM, 2011, 136 s. ISBN 978-80-247-4564- 0

(22) JEŽKOVÁ, Zuzana, 2013. Projektové řízení: jak zvládnout projekty. Kuřim: Akademické centrum studentských aktivit,. 381 s. ISBN 978-80-905297-1-7.

(23) RAIS,Karel.DOSKOČIL,Radek. Risk Management: Studijní text pro kombinovanou formu studia. Vyd.Brno: CERM, 2007, 152 s. ISBN 978-80-214-3510-0

(24) *EU-U.S. privacy Shield.* [online]. [cit. 2016-05-02]. Dostupné na internete: < http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf>

(25) *Microsoft comes support EU-U.S. Privacy Shield.* [online]. [cit. 2016-05-02]. Dostupné na internete: < https://www.petri.com/microsoft-comes-support-eu-u-s-privacy-shield>

(26) *IBM X-Force Research.* [online]. [cit. 2016-05-06]. Dostupné na internete: < http://www-03.ibm.com/security/data-breach/ >

(27) ADAM, Azad. Implementing Electronic Document and Record Management Systems. New York :Auerbach Publications, 2007. 270 s. ISBN 0-8493-8059-6

(28) STRNÁD, Ondřej. Systémový prístup k riadeniu informačnej bezpečnosti. Vyd. Tripsoft v Trnave, 2009. s. 233. ISBN 978-80-89291-20-5.

(29) MYŠÍK, Jiří. Hodnocení efektů při zavedení nebo inovaci informačního systému v podniku. Vyd. Ostrava: Key Publishing, 2010, 55 s. Monografie (Key Publishing). ISBN 978-80-7418-059-0.

8 ZOZNAM OBRÁZKOV

9 ZOZNAM TABULIEK

10 ZOZNAM PRÍLOH

Príloha A: SWOT Analýza (Zdroj: Vlastné spracovanie)

Príloha B: Diagram PERT (Zdroj: Vlastné spracovanie)

Príloha C: Predloha podnikovej smernice (Zdroj: Interné materiály)

Príloha D: Postup dvojfaktorovej autentifikácie v SharePointe (Zdroj: (13))

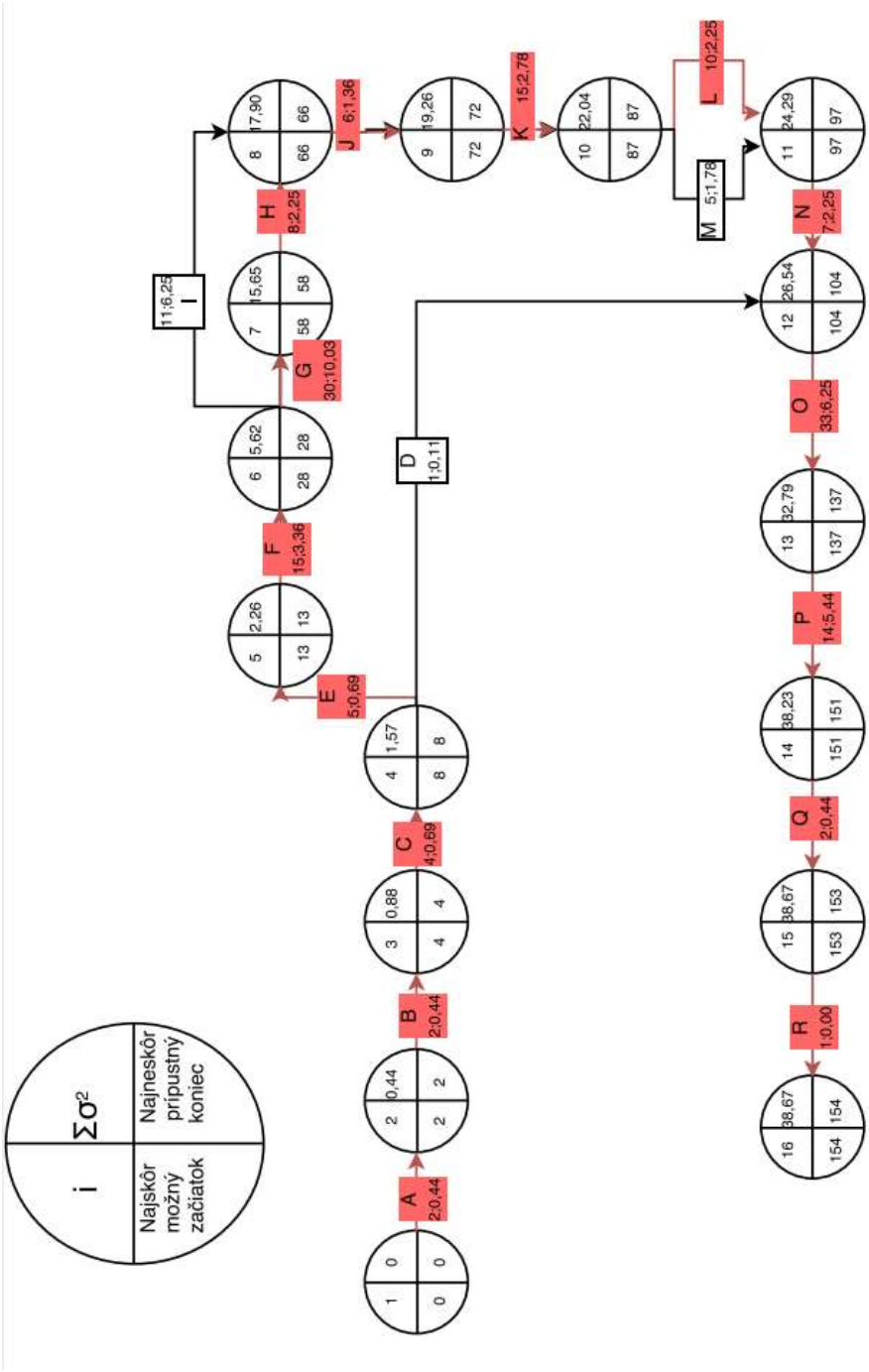
Príloha E: Manažment prístupových oprávnení (Zdroj: (14))

Príloha F: Časový diagram (Zdroj: Vlastné spracovanie)

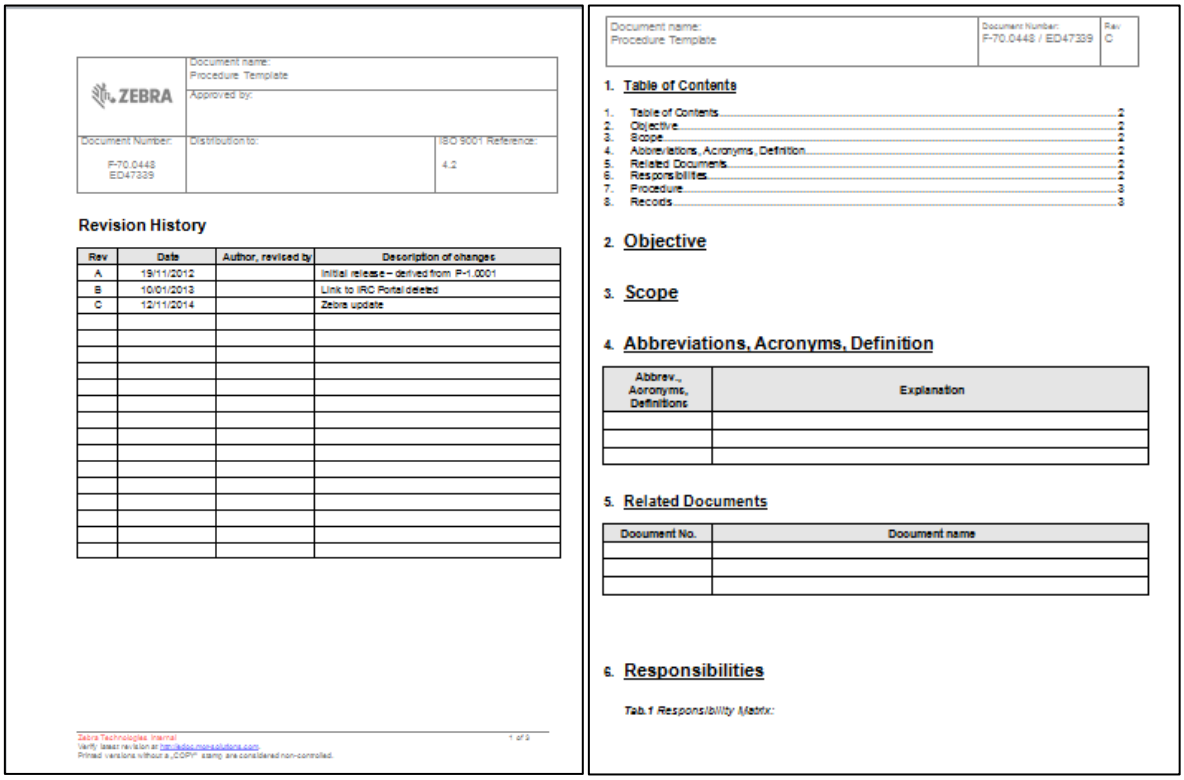
Príloha A: SWOT Analýza (Zdroj: Vlastné spracovanie)

SWOT analýza	
Silné stránky	**Slabé stránky**
+ Dlhoročné skúsenosti + Ponuka nadštandardného servisu s rýchlou dodávkou náhradného produktu + Globálna podpora zákazníkov + Certifikácia manažmentu kvality ISO 9000 + Komplexná podpora zákazníka vo väčšine svetových jazykov + Technologicky inovatívny líder v oblasti svojho pôsobenia	– Chaos po akvizícii – Neefektívne zaobchádzanie s podnikovou dokumentáciou – Vysoké ceny servisu – Decentralizovaný systém ukladania dokumentov – Závislosť od opravárenského centra – Neefektívna komunikácia a spolupráca so zákazníkmi
Príležitosti	**Hrozby**
+ Skvalitnenie komunikácie so zákazníkmi + Presun do nového DMS, efektívnejšieho + Technologické trendy, napr. Cloud Computing	– Vyjednávacia sila dodávateľského opravárenského centra – Výskyt konkurenčných servisných centier schopných poskytnúť servis zákazníkom Zebry – Ohrozenie RFID technológie vírusmi – Klesajúci počet technicky zameraných absolventov vysokých škôl – Nedostatočná bezpečnosť produktov a možnosť ich napadnutie najmä v prípade zákazníkov, ktorí sú súčasťou kritickej infraštruktúry

Príloha B: Diagram PERT (Zdroj: Vlastné spracovanie)



Príloha C: Predloha podnikovej smernice (Zdroj: Interné materiály)



ZEBRA	Document name: Procedure Template Approved by:	
Document Number: P-70.0448 ED47339	Distribution to:	ISO 9001 Reference: 4.2

Revision History

Rev	Date	Author, revised by	Description of changes
A	19/11/2012		Initial release – derived from P-1.0001
B	10/01/2013		Link to IRC Portal deleted
C	12/11/2014		Zebra update

Zebra Technologies Internal 1 of 3
Verify latest revision at http://sdoc.mes-solutions.com
Printed versions without a „COPY" stamp are considered non-controlled.

Document name: Procedure Template	Document Number: P-70.0448 / ED47339	Rev C

1. Table of Contents

2. Objective

3. Scope

4. Abbreviations, Acronyms, Definition

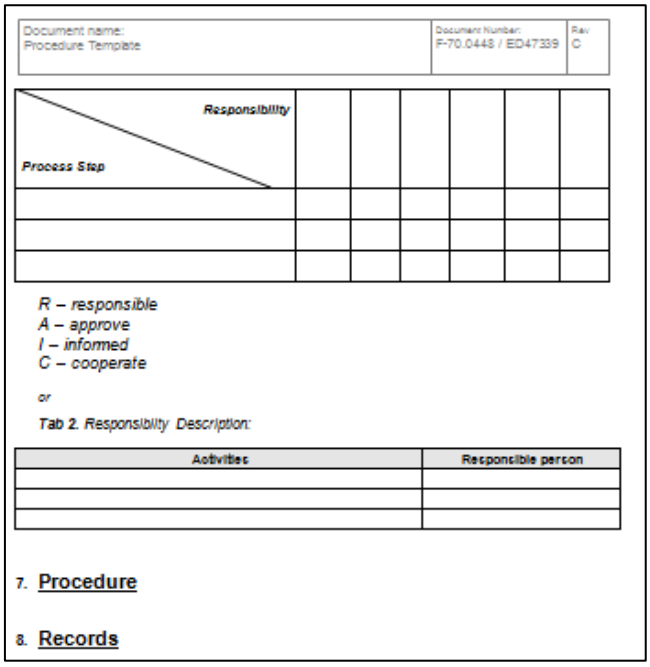
Abbrev., Acronyms, Definitions	Explanation

5. Related Documents

Document No.	Document name

6. Responsibilities

Tab.1 Responsibility Matrix:



Document name: Procedure Template	Document Number: F-70.0448 / ED47339	Rev C

Responsibility / *Process Step*						

R – responsible
A – approve
I – informed
C – cooperate

or

Tab 2. Responsibility Description:

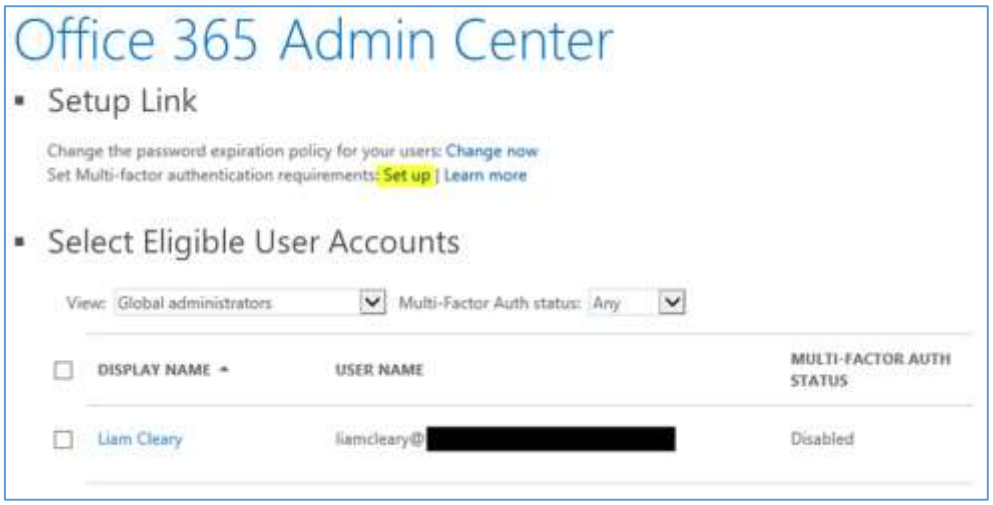
Activities	Responsible person

7. Procedure

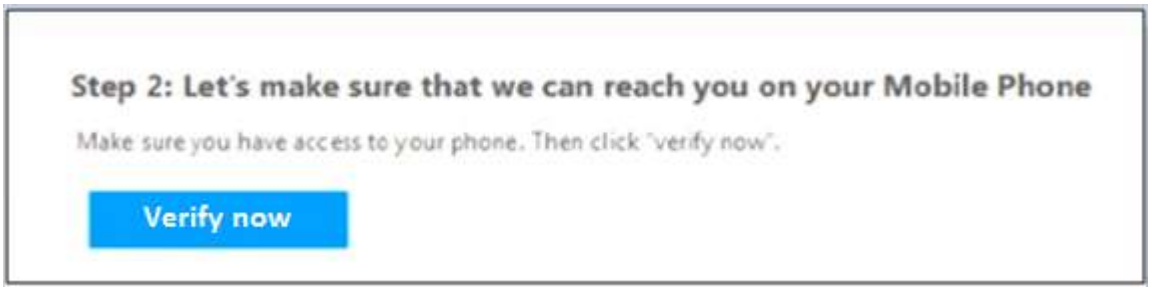
8. Records

Príloha D: Postup dvojfaktorovej autentifikácie v SharePointe (Zdroj: (13))

Užívateľ s hlavným administrátorským oprávnením v prvom kroku nastaví žiadúcej skupine užívateľov požiadavok na druhý faktor autentifikácie pred vstupom do systému.



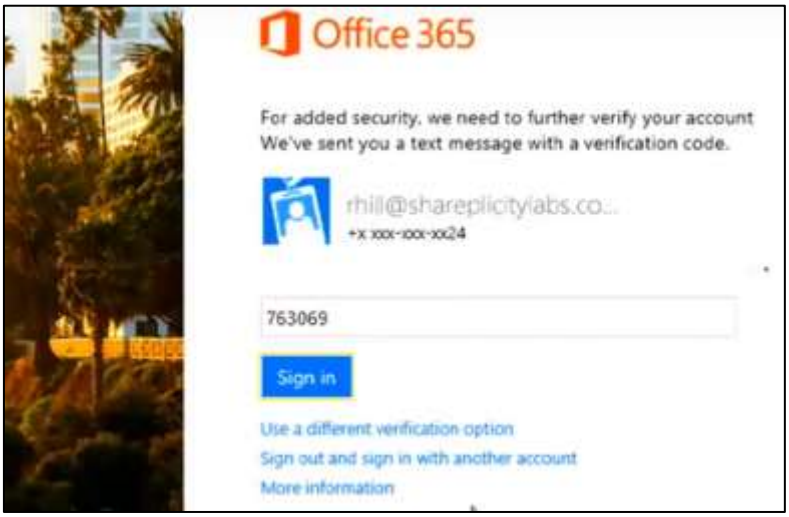
Po schválení požiadavku administrátora si v najbližšom prístupe musí užívateľ nastaviť, akým spôsobom sa bude verifikovať . Na výber ma mobilný telefón alebo kancelársky telefón, pri ktorých si volí možnosť telefonátu alebo textovej správy. Ďalšou možnosťou je zvoliť si namiesto telefónov mobilnú aplikáciu, ktorú je možné stiahnuť z app obchodu. Po vybraní sa musí overiť dostupnosť zvolenej technológie pomocou overovacieho hesla. Jednotlivé kroky sú znázornené postupne na nasledujúcich obrázkoch:



Každé ďalšie prihlásenie užívateľa do systému je sprevádzané vyžiadaním primárneho hesla, odoslaním overovacieho kódu na ním vybrané zariadenie a zadanie sekundárneho kódu do systému.

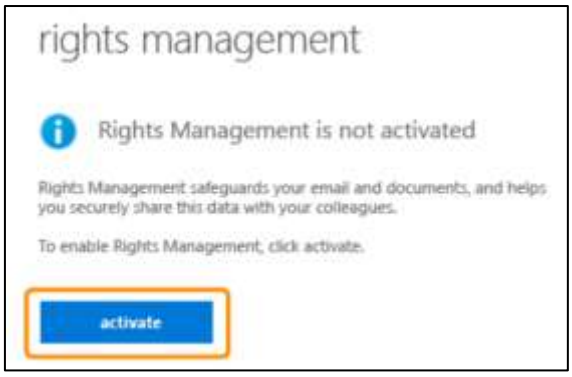

Office 365
Sign in with your organizational account
rhill@shareplicitylabs.co...
Keep me signed in
Sign in
Cancel
Can't access your account?

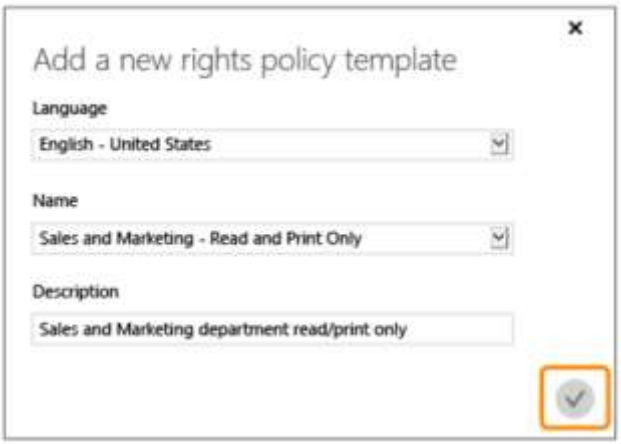

Office 365
How do you want us to verify your account?
rhill@shareplicitylabs.co...
+x xxx-xxx-xx24
Text me at +x xxx-xxx-xx24
Call me at +x xxx-xxx-xx24
Sign out and sign in with another account
More information

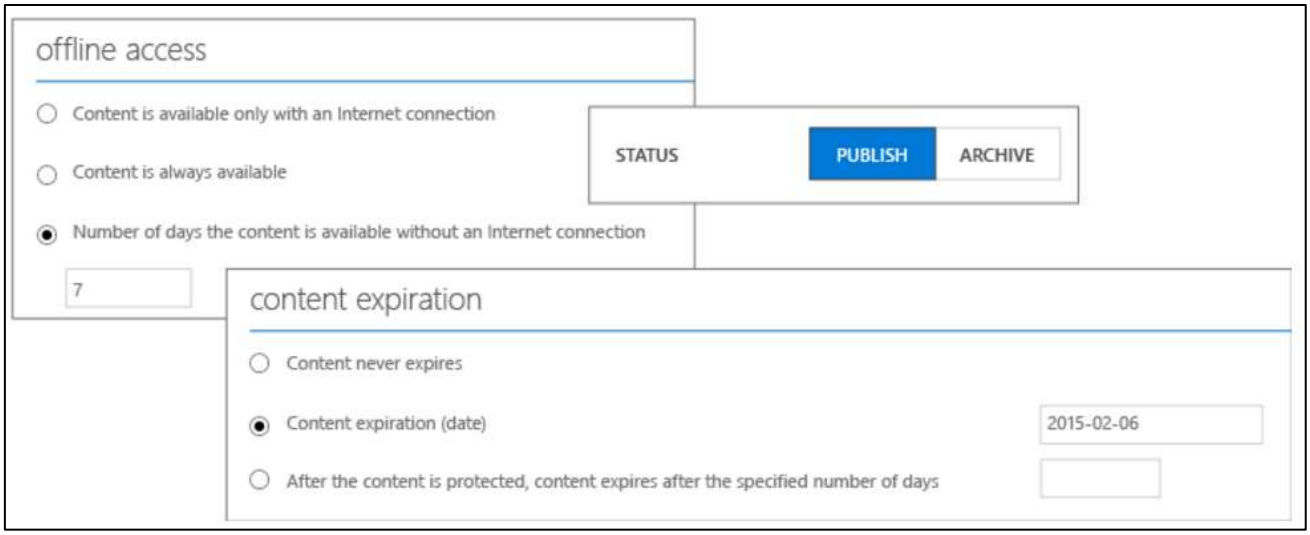

Office 365
For added security, we need to further verify your account
We've sent you a text message with a verification code.
rhill@shareplicitylabs.co...
+x xxx-xxx-xx24
763069
Sign in
Use a different verification option
Sign out and sign in with another account
More information

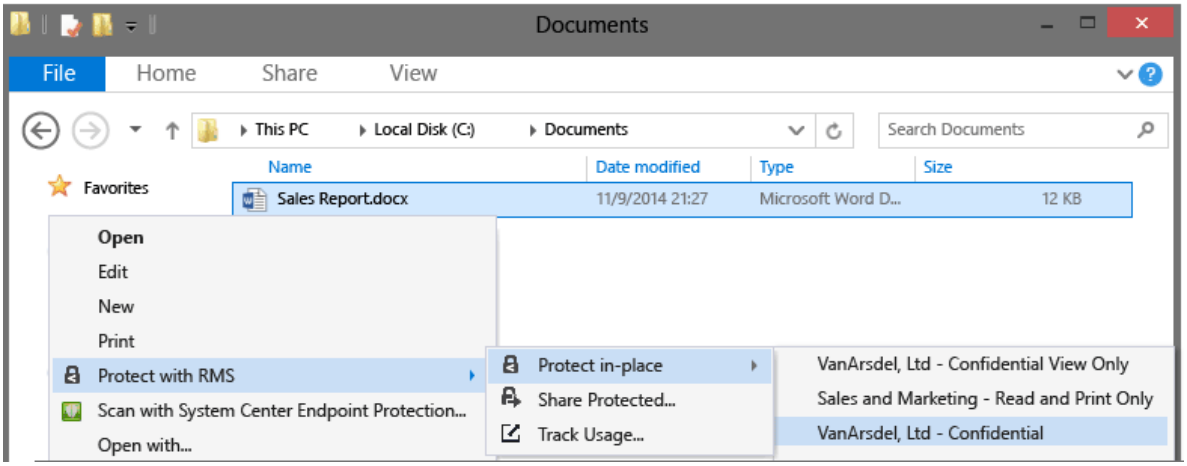
Príloha E: Manažment prístupových oprávnení (Zdroj: (14))

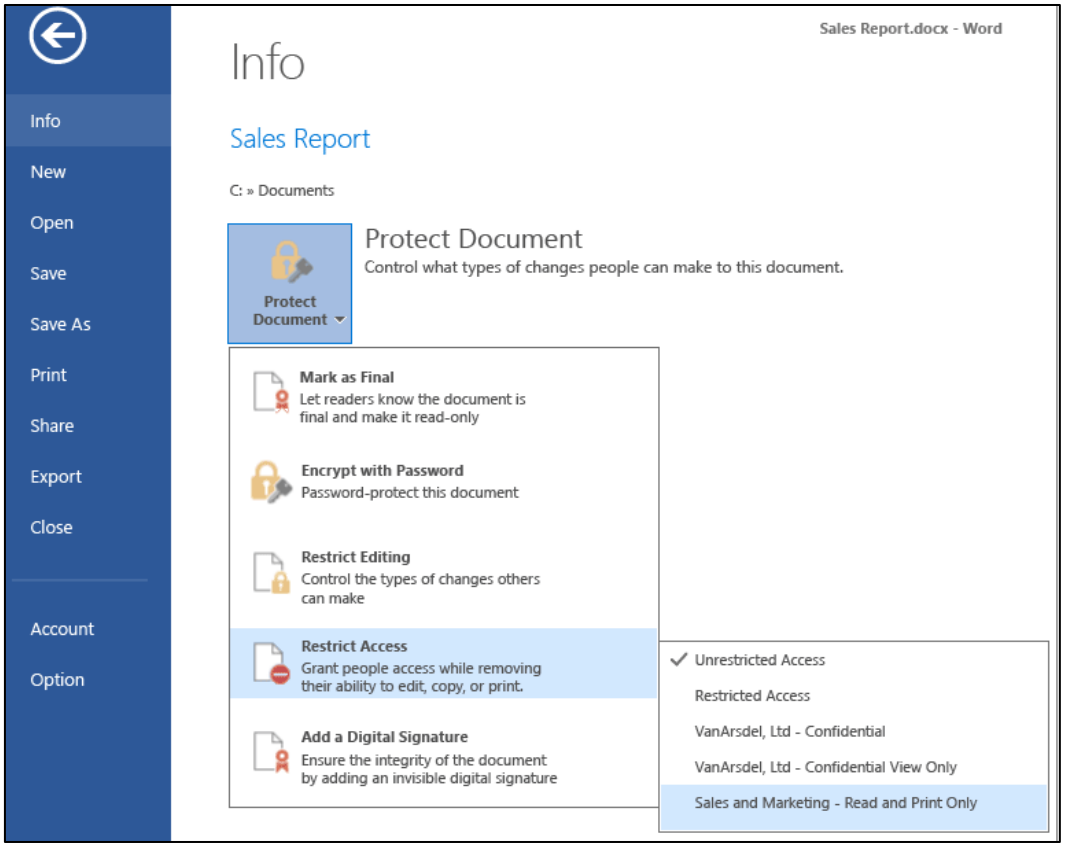
Oprávnený administrátor aktivuje túto službu jediným tlačítkom *Activate.* Následne je možné tvoriť šablónové skupiny oprávnení, pričom sa dá zvoliť doba expirácie dostupnosti dokumentu alebo počet dní offline dostupnosti dokumentu. Následne sa užívateľom pri spracovávaní dokumentov v Office formátoch ponúknu medzi možnosťami zabezpečení aj administrátorom prednastavené šablóny prístupových oprávnení. Na nasledujúcich obrázkoch je tento postup znázornený:






offline access
Content is available only with an Internet connection
Content is always available
Number of days the content is available without an Internet connection
7
STATUS
PUBLISH
ARCHIVE
content expiration
Content never expires
Content expiration (date)
2015-02-06
After the content is protected, content expires after the specified number of days


Documents
File
Home
Share
View
This PC
Local Disk (C:)
Documents
Search Documents
Favorites
Name
Date modified
Type
Size
Sales Report.docx
11/9/2014 21:27
Microsoft Word D...
12 KB
Open
Edit
New
Print
Protect with RMS
Scan with System Center Endpoint Protection...
Open with...
Protect in-place
Share Protected...
Track Usage...
VanArsdel, Ltd - Confidential View Only
Sales and Marketing - Read and Print Only
VanArsdel, Ltd - Confidential


Sales Report.docx - Word
Info
Sales Report
C: » Documents
Info
New
Open
Save
Save As
Print
Share
Export
Close
Account
Option
Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature
Unrestricted Access
Restricted Access
VanArsdel, Ltd - Confidential
VanArsdel, Ltd - Confidential View Only
Sales and Marketing - Read and Print Only

Príloha F: Časový diagram (Zdroj: Vlastné spracovanie)