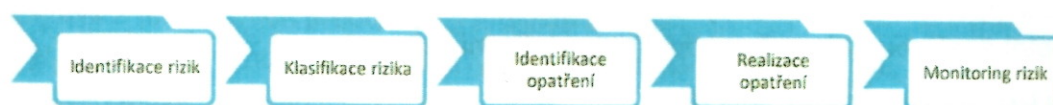


Analýza rizik projektu

Každý projekt je v průběhu celého svého životního cyklu doprovázen riziky. Projekt i projektový tým musí být na zvládnutí rizik připraven. Základem zvládnutí rizik je jejich průběžná analýza, vyhodnocování a návrh vhodných opatření k jejich řízení. Řízení rizik zahrnuje opatření k jejich zamezení nebo snižování dopadu, dále přenos vhodných rizik na třetí strany i akceptaci rizik, která není možné eliminovat, nebo přenést. K řízení rizika patří také vytváření podmínek pro efektivní operativní zvládnutí rizik.

Metodika analýzy rizik

Metodika analýzy rizik užívaná v projektech společnosti SOFO Group a.s. vychází z principů využívaných v systémových normách (např. ČSN EN ISO 9001, ČSN ISO/IEC 27001, ČSN ISO 31000, ITIL), v mezinárodně respektované metodice řízení projektů PRINCE2®, dle níž jsou naši projektoví manažeři certifikováni (viz kapitolu 11 PROJEKTOVÝ TÝM), i z tzv. postřehů dobré praxe (best practices) získaných při předchozích realizovaných projektech.



Obrázek 1 – Schéma analýzy rizik

Prvním krokem je identifikace jednotlivých rizik. Míru každého rizika je možné vyjádřit číselně pomocí následujícího vzorce:

$$MR = PV \times DP,$$

kde Míra rizika (MR) je dána součinem pravděpodobnosti realizace rizika (PV) a dopadu v případě realizování rizika (DP). V tomto případě může nabývat Míra rizika hodnot <1;25>.

Tabulka 1 – Hodnocení pravděpodobnosti rizika

Pravděpodobnost výskytu (PV)	Body	Častost výskytu ²
<i>nepravděpodobná</i>	1	≤ 1 z 20 projektů (5 % a méně)
<i>velmi malá</i>	2	≤ 1 z 10 projektů (10 % a méně)
<i>malá</i>	3	≤ 1 z 5 projektů (20 % a méně)
<i>mírná</i>	4	≤ 1 ze 2 projektů (50 % a méně)
<i>vysoká</i>	5	> 1 ze 2 projektů (více než 50 %)

² Je vztažena ke srovnatelným projektům.

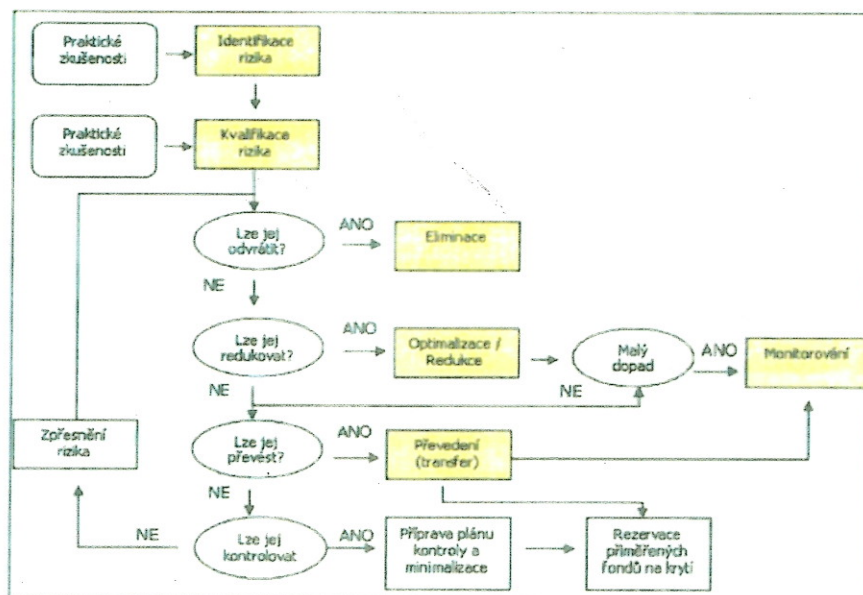
Tabulka 2 – Hodnocení dopadu rizika

Dopad (DP)			body
termín	finance ³	kvalita ⁴	
<i>zpoždění dílčích prací</i>	<i>zanedbatelné ztráty (do 1 %)</i>	<i>možná vada kategorie C</i>	1
<i>zpoždění etapy</i>	<i>nízké ztráty (do 2 %)</i>	<i>více vad kategorie C</i>	2
<i>zpoždění více etap</i>	<i>střední ztráty (do 5 %)</i>	<i>možná vada kategorie B</i>	3
<i>zpoždění celého projektu</i>	<i>vysoké ztráty (do 10 %)</i>	<i>více vad kategorie B</i>	4
<i>zastavení projektu</i>	<i>velmi vysoké ztráty (10 % a více)</i>	<i>možná vada kategorie A</i>	5

Pro všechna rizika, která dosáhnou předem stanované hodnoty MR, je potřeba identifikovat možná opatření. Pro každé z těchto opatření projektový tým určí náklady na realizaci opatření a vyhodnotí jeho dopad na rizika projektu. Toto předběžné vyhodnocení je nezbytné k určení opatření, která budou realizována. Následuje komplexní zhodnocení aktuálních rizik včetně výpočtu aktuálních hodnot MR, nákladů na vybraná opatření a jejich celkového dopadu. Až na základě tohoto komplexního zhodnocení přistoupí projektový tým k realizaci opatření k řízení rizik.

Nevhodná opatření mohou do systému vnést nová rizika. Proto je potřeba vždy pracovat s kompletní analýzou rizik a všemi opatřeními k řízení rizik.

Graficky lze celý proces znázornit takto:

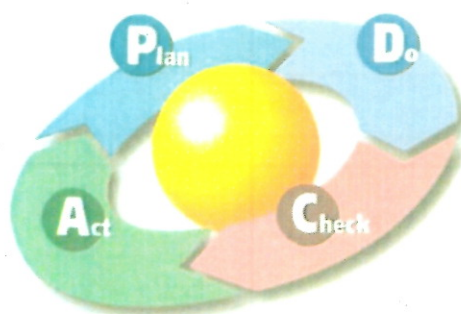


Obrázek 2 – Schéma analýzy rizik

³ Procentuální vyjádření finanční ztráty je vztaženo k celkovým nákladům projektu.

⁴ Kategorie vad A, B a C odpovídají vadám dle článku 4.9. Smlouvy v kapitole 4.

Proces analýzy rizik probíhá po celou dobu přípravy a realizace projektu podle Demingova cyklu. Demingův cyklus, známý také jako Plan – Do – Check – Act (Plán – Výkon – Kontrola – Náprava), zahrnuje plánování, realizaci, průběžný monitoring a aktualizaci analýzy rizik i nápravných opatření.



Obrázek 3 – Schéma Demingova cyklu

V rámci procesu analýzy rizik byly pro identifikaci rizik využity tyto metody:

- analýza dostupných dat,
- poučení z relevantních předchozích projektů a aktivit,
- brainstorming v rámci projektového týmu a zaměstnanců společnosti,
- metoda Delphi („co když...?“).

V následující tabulce jsou semikvantitativní metodou popsána možná rizika, která mohou ohrozit projekt během celého životního cyklu. Ke každému riziku je uveden dopad rizika (DP), pravděpodobnost (PV) a opatření k jeho řízení:

Popis rizika	Míra dopadu (DP)	Pravděpodobnost výskytu rizika (PV)	Míra rizika (MR)	Návrh na eliminaci vzniku rizik
FÁZE PŘÍPRAVNÁ				
Organizační/Technická rizika				
Nesprávné nastavení priorit realizace plánovaného projektu	4	1	4	Pro realizaci všech plánovaných aktivit byl sestaven koordinovaný a zkušený projektový tým. Byla provedena důkladná analýza možností, nároků a předpokladů udržitelnosti. Priority byly stanoveny na základě této analýzy a strategie rozvoje společnosti + finančních možností (výhled, vč. ostatních plánovaných projektů).

Nedostatečná personální kapacita pro přípravu projektu	4	1	4	Členové projektového týmu mají zkušenosti s tvorbou a návrhem portálových řešení a webových aplikací obecně. Projektový tým tvoří zkušení zaměstnanci se znalostmi z oboru. Analytici a vývojáři v týmu mají přímou zkušenost s tvorbou e-learningových systémů a systémů pro testování.
Výběr vhodné infrastruktury pro úspěšnou realizaci projektu a řádné zdokumentování (promyšlenost kritérií, zohlednění rizik).	5	1	5	Pečlivé definování požadavků na funkcionalitu; poměr cena/výkon. Zpracování BIA ⁵ analýzy. Průzkum zkušenosti mezi členy projektového týmu (rizika, předpoklady). Fyzické oddělení vývojového, testovacího a produkčního prostředí (bezpečnostní požadavek). Konzultace s právníkem a ekonomem společnosti s důrazem na zabezpečení provozu a dlouhodobé udržitelnosti.
Nedostatečné informace pro přípravu projektu, projevující se ve špatné interpretaci požadavků zadavatele	4	1	4	Důraz na předkládání výstupů z pracovních jednání. Příprava průběžných dokumentů a realizace pravidelných projektových porad. Projektové vedení dle metodiky PRINCE2®. Seznámení s veškerými požadavky na systém v rámci setkání projektového týmu. Shromažďování požadavků, jejich analýzu a řešení otevřených záležitostí – je použit nástroj MS Team Foundation Server, který usnadňuje týmovou kooperaci a minimalizuje možnost zanesení chyby vlivem nepochopení požadavku.

⁵ Business Impact Analysis, analýza dopadů na projekt a jeho výstupy.

Nesprávné definování požadavků.	4	1	4	Příprava systému bude odpovídat požadavkům zadávací dokumentace. Analytici dodavatele budou konzultovat zadání vzhledem k technickým možnostem a co nejlepší výsledné uživatelské zkušenosti.
Finanční rizika				
Růst cen/vstupů v průběhu realizace projektu (oproti plánu v přípravné fázi)	3	2	6	V rozpočtu projektu jsou zohledněny nákladové ceny i tvorba přiměřeného zisku s ohledem na časový harmonogram projektu.
FÁZE REALIZAČNÍ				
Organizační/Technická rizika				
Nedodržení základních postupů projektového managementu.	4	1	4	Vedení projektu dle PRINCE2® metody, pravidelné projektové schůzky, eskalace problémů a odchylek. Evidence a správa požadavků v systému MS Team Foundation Server.
Pozdní odhalení případných chyb v aplikaci.	4	2	8	Během vývoje bude zvolen iterativní přístup, aplikace bude tvořena po menších funkčních modulech, z nichž každý bude podroben samostatnému testování a akceptaci. Projektový tým obsahuje skupinu testerů, kteří minimalizují počet funkčních chyb již při vývoji.
Nedostatečný návrh architektury systému.	3	1	3	Systém bude vytvořen a spravován v robustní technologii MS .NET, čímž bude zaručena aktuálnost technologie a snadná rozšiřitelnost a udržitelnost projektu v budoucnu.
Změnové požadavky během práce na projektu.	5	4	20	Dle ZD bude vyčleněna potřebná kapacita na analýzu a implementaci případných změnových požadavků. Veškeré změny budou podléhat řízení změnových požadavků. V první fázi projektu proběhne akceptace specifikace, tudíž případné změnové požadavky ze strany zadavatele budou minimalizovány.

Nedostatečná součinnost ze strany zadavatele	4	3	12	Za dodavatele bude jmenován projektový manažer, který bude koordinovat veškerou komunikaci mezi zadavatelem a dodavatelem. Budou definovány role v projektovém týmu a zastupitelnost klíčových pozic v případě neočekávaných událostí. Případné nedostatky v komunikaci budou řádně eskalovány.
Zcizení know-how a dat v rámci vývoje.	3	1	3	Zabezpečovací opatření (firewall). Oddělení vývojového, testovacího a produkčního prostředí. Monitoring činnosti zaměstnanců na svěřené infrastruktuře. Dodavatel provozuje certifikovaný systém ochrany dat a informací dle normy ISO/IEC 27001:2005 a řídí vývoj aplikací dle metodiky SCRUM a projekt dle PRINCE2®.
Grafická podoba aplikace neodpovídá představám zadavatele	2	1	2	Grafická podoba uživatelského prostředí bude navržena buď přímo zadavatelem, nebo dodavatelem a poté schválena zadavatelem. Návrh grafického prostředí a ergonomie aplikace proběhne podle zažitých zvyklostí vedoucí k co nejvyšší míře uživatelské spokojenosti. Důraz bude kladen na jednoduchost ovládání. Konečná ergonomie bude schválena sadou UAT testů ze strany zadavatele
Funkční zpracování jednotlivých modulů neodpovídá představám zadavatele	3	1	3	V rámci realizační fáze budou probíhat schůzky se zástupci dodavatele, na nichž bude potvrzena požadovaná funkčnost modulů v jednotlivých iteracích.
Nízká motivace zaměstnanců – neochota zaměstnanců participovat na projektu, přinášet nápady, neproaktivní přístup k uloženým úkolům.	4	1	4	Zapojení zaměstnanců – realizace „kick-off“ projektu (informace o projektu, důvody pro realizaci, požadavky, cíle), vtáhnutí do procesu přípravy a realizace projektu, pravidelné informování (interní mailing), zjišťování zpětné vazby (ocenění nápadů). Systém odměn vázaný na plnění termínů, nové nápady (inovace v plánu projektu), realizace „teambuildingových“ aktivit.

Problémy s nasazením aplikace v datovém centru zadavatele	3	2	6	Aplikace bude vyvíjena na kompatibilních technologiích a testována na virtualizovaných prostředích s operačním systémem MS Windows Server a databázovým prostředím MS SQL Server. Projektový tým má s těmito technologiemi bohaté zkušenosti
Finanční rizika				
Nedostatečné finanční zdroje při realizaci projektu.	4	1	4	Dodavatel vyčlenil na realizaci projektu dostatečné prostředky. Projekt je etapizován. Vytvořeny dostatečné rezervy pro překonání testovací fáze projektu. Finanční zdraví a síla společnosti.
Objektivní rizika: ohrožení projektu přírodními katastrofami, vloupáním, vandalismem, zcizením know-how atp. (objektivní příčiny).	5	2	10	Riziko přeneseno formou pojištění. Prostory jsou dostatečně zabezpečeny (technicky i elektronicky vč. napojení na pult ochrany). Přístup k citlivým datům má jen omezený počet osob (management a pověřeni pracovníci – písemné pověření, prověrky v souladu se systémem řízení informací ve firmě dle ISO/IEC 27001).
FÁZE PROVOZNÍ (UDRŽITELNOST)				
Organizační/Technická rizika				
Aplikace vykazuje nestabilitu při vysokém zatížení	3	1	3	Pro akceptaci projde aplikace zátěžovými testy tak, aby splnila požadavky zadávací dokumentace. Při dlouhodobě zvýšeném zatížení v počtu uživatelů je vzhledem k navržené infrastruktuře možno posílit virtuální prvky datacentra, příp. rozložit zátěž mezi více prvků.
Nestabilita, poruchovost zvolené infrastruktury	4	1	4	Produkční prostředí bude realizováno na virtuálních prvcích datového centra MPSV.

Ztráta dat nasazené aplikace	5	1	5	U aplikace bude nastaveno pravidelné zálohování jak formou rozdílové na denní bázi, tak formou pravidelné plné zálohy aplikace i datových struktur. Nasazením aplikace v datovém centru MPSV se zároveň minimalizuje riziko ztráty primárních dat.
Uživatelské rozhraní aplikace je špatně přijato ze strany uživatelů	3	2	6	Během vývoje bude kladen důraz na ergonomii a jednoduchost, která bude podpořena akceptačními UAT testy. V rámci školení se administrátoři systému seznámí s celkovou funkcí prostředí. K systému bude existovat podrobná uživatelská příručka.
Zastaralost systému během životního cyklu	4	2	8	Zvolená technologie Microsoft .NET zaručuje vysokou míru pravděpodobnosti budoucí kompatibility a udržitelnosti systému. Případné úpravy webové aplikace budou vzhledem k modulárnímu systému jednoduché a umožní reakci na potřeby zadavatele v oblasti nových technologií. Díky využití webové technologie bude nasazování nových verzí aplikace probíhat výhradně na straně serveru, čímž dojde k minimalizaci dopadů těchto kroků na uživatele.
Špatná uživatelská zkušenost na mobilních zařízeních	3	1	3	Při vývoji bude kladen důraz i na zobrazení obsahu uživatelům mobilních zařízení: techniky „Responsive Design“, tedy přizpůsobení vzhledu aplikace podle velikosti displeje.
Aplikace bude během provozu vystavena útoku hackerů	3	2	6	Aplikace bude vyvíjena s ohledem na vysokou bezpečnost. Klíčové funkce použitého řešení pomocí technologie MS MVC zajišťují ochranu proti útokům typu Cross-Site Scripting, XSS útokům a Cross-Site Request Forgery útokům a SQL injection. Veškeré požadavky budou validovány na straně serveru tak, aby nemohlo dojít k podvrhnutí dat.

Finanční rizika

Rostoucí náklady na provoz aplikace	4	2	8	Vzhledem k nasazení aplikace v datovém centru MPSV budou náklady pouze v rámci licencí na prostředí VMWare, Windows Server a SQL Server.
-------------------------------------	---	---	---	--