

Souhrnné stanovisko Řídicího orgánu Rámce podpory Společenství
ke

Zprávě o posouzení souladu s předpisy k 29.10.2004
Zahajovacího auditu souladu s předpisy a auditu systémů implementačních struktur SF
a FS – EUROPAID/114848/D/SV/CZ

(A.1)

ad 2.1 "Zjištění" str. 6:

ŘO RPS připravil **projekt (hrazený z prostředků technické pomoci pro RPS - odd. 323) "Analýza lidských zdrojů ORPS ve vztahu k současným a předpokládaným činnostem v průběhu programovacího období 2004 - 2006"**. Tento projekt odpovídá doporučení auditora stran zpracování a pravidelné aktualizace (analýzy) potřeb lidských zdrojů.

ad 6.1. kap. A2 str. 19

vyjádření za odd. 324: Personální stav oddělení pro informace, publicitu a vzdělávání je naplněn, tvoří jej pět zaměstnanců (včetně vedoucího oddělení).

ad str. 22 kap. B poslední odstavec, poslední věta:

"pracovní skupina se schází dle potřeby, zpravidla jednou měsíčně."

Na str. 23: bod **Průběžné monitorování RPS** a jednotlivých OP, zpracování zpráv o realizaci RPS je chybně v druhém bodu uvedeno "Zpracování podkladové dokumentace pro pravidelné monitorovací schůzky s ŘO a PJ". Jde o schůzky s řídicími orgány a **platebním orgánem (PO)**, tj. zástupcem Ministerstva financí. V dalším zjištění zprávy odpovídají skutečnému stavu.

Kap. E Řídicí výbor RPS – správný název je Poradní výbor Řídicí výbor (Steering Committee v originále CSF) je pro svoji čistě poradní roli v českém překladu RPS a běžné terminologii označován jako Poradní výbor Rámce podpory Společenství. (Poradní výbor Rámce podpory Společenství byl ustaven Rozhodnutím ministra pro místní rozvoj č. 170/2003 ze dne 19. prosince 2003. V příloze č. 1 tohoto rozhodnutí byl vydán Statut Poradního výboru Rámce podpory Společenství.)

K bodu **vyjasnění právní kompetentnosti (E.1)** lze uvést, že je třeba vycházet z relevantní evropské legislativy upravující poskytování pomoci ze strukturálních fondů s přihlédnutím ke konkrétnímu nastavení podmínek pro ČR. Zejména je možné uvést, že v obecném nařízení o strukturálních fondech č.1260/1999 je zakotven v čl. 10 princip koordinace, vykonávaný prostřednictvím Rámců podpory Společenství, operačních programů a ostatních nástrojů, v návaznosti na čl. 17 téhož nařízení pak Rámec podpory společenství má koordinovat veškerou strukturální pomoc Společenství v dotčených regionech. V souladu se základními principy evropského práva jsou platná nařízení bezprostředně závazná v členských státech EU a v případě nesouladu mají přednost před národní legislativou.

Na základě výše zmíněného nařízení byl vyjednáán a schválen Rámec podpory Společenství pro Českou republiku na roky 2004-2006, v němž je specifikována role ŘO RPS a ŘO OP. Zachycení právní kompetence je tak rozděleno mezi nařízení č.1260/1999 a zmíněný dokument. Nařízení sice ponechává konkrétní pověření výkonem funkcí jak ŘO RPS, tak ŘO OP na rozhodnutí členských států, trvá však na zajištění efektivního řízení pomoci ze

strukturálních fondů, jehož je koordinace vůdčím principem. Rámec podpory Společenství jako dokument je pak mezinárodní dohodou sui generis mezi členským státem EU a Evropskou Komisí a je proto pro každý členský stát závazný. V jeho kapitole 6 Implementing provisions se uvádí, že „ŘO RPS, který nese celkovou odpovědnost za účinnost, správnost řízení a provádění pomoci poskytované ze strukturálních fondů České republiky, je Ministerstvo pro místní rozvoj. Řídicí orgán RPS je zodpovědný za koordinaci implementace RPS...“ zcela v souladu s nařízením 1260/1999. Přitom se jedná o zajištění koordinace prostřednictvím série konkrétních nástrojů, které jsou ostatně běžné také v ostatních členských státech (monitorovací výbor RPS, Poradní výbor, pracovní skupiny, pokyny aj.) a které zajišťují standardní úroveň koordinace, požadovanou také a zejména Evropskou Komisí.

Klíčové je přitom pravidlo, že aniž by obecné nařízení a dokument RPS rušily či měnily vnitrostátní předpisy (zákon o ministerstvech aj.), mohou v zájmu koordinace upravit právní kompetenci v oblasti strukturálních fondů bez dalšího ve prospěch ŘO RPS, tak jak je to vedle řady jiných zemí také příznačné pro ČR. Lze tedy uzavřít, že výše uvedené články nařízení 1260/1999 ve spojení s kapitolou 6 Rámce podpory Společenství je třeba interpretovat jako závazné ustanovení právní kompetence ŘO RPS, pokud jde o systém implementace strukturálních fondů v ČR. Tento systém je přesně vymezen jako systém orgánů určených příslušnými rozhodnutími vlády ČR.

Kap. E Pracovní skupiny - Činnosti pracovních skupin je popsána v Operačním manuálu RPS, nicméně vzhledem ke skutečnosti že bude často docházet ke změně PS, např. vzniknou na základě potřeby nové pracovní skupiny PV RPS a některé z existujících svou činností utlumí, příp. dokonce zaniknou, nelze detailně popsat činnost PS.

F. Monitorovací systém strukturálních fondů (IS MSSF)

Odbor monitorování programů (#33) byl na základě Rozhodnutí ministra k 31.7.2004 začleněn do sekce Rámce podpory Společenství a Fondu soudržnosti.

F1. Struktura monitorovacího systému

1) Centrální úroveň – MSSF CENTRAL

MMR vytvořilo a provozuje centrální monitorovací systém strukturálních fondů – IS MSSF CENTRAL. Informační systém je určen pro pracovníky Řídicích orgánů, platebních jednotek, Platebního orgánu a bude poskytovat souhrnné informace o přípravě a stavu realizace operačních programů SF/FS. Bezpečný přístup externích uživatelů k IS MSSF CENTRAL je zajištěn přes meziresortní síť GOVBONE, GOVNET.

Nížší úrovně jsou: informační systémy MONIT, ISOP a SAP.

SW nástroj pro Konečného příjemce (žadatele) je Elza, Benefil, Benefit

2) Výkonná úroveň – administrace a správa projektů – IS MONIT, ISOP, SAP

IS SAP pro OP Rozvoj venkova a multifunkční zemědělství

IS MONIT pro ostatní OP.

Tyto IS slouží pro administraci a hodnocení projektů.

CRR je zřízeno MMR.

Mezi ŘO (kromě OP PP, OP R VaMZ) byla uzavřena s firmou TESCO SW Servisní smlouva pro IS MONIT.

3) Softwarová podpora žadatelů

Sběr projektových žádostí konečných příjemců těchto OP, které využívají IS MONIT, je zajišťován pomocí následujících SW nástrojů: ELZA, BENEFIT, BENEFIL. Projektová žádost a Žádost o platbu vyhotovená v těchto SW nástrojích je importována přímo do IS MONIT v elektronické podobě.

F2. MSSF CENTRAL

MMR uzavřelo smlouvu s firmou S&T Services (dříve Fujitsu Services, ICL) na vytvoření Monitorovacího systému strukturálních fondů.

Vývoj aplikace byl ukončen v srpnu 2003.

Následně byla Rozhodnutím ministra č.114/2003 jmenována Malá hodnotitelská komise a Velká hodnotitelská komise, jejichž členy byli zástupci ŘO, RPS, PO, odboru IT MMR a Českého statistického úřadu.

V září 2003 auditorská firma GiST zpracovala Plán posuzování akceptačních kritérií základní verze Monitorovacího systému strukturálních fondů, který stanovil 12 Akceptačních kritérií.

Provoz MSSF CENTRAL

Servisní smlouva na údržbu a další rozvoj IS MSSF CENTRAL (mezi MMR a S&T) byla uzavřena 31. ledna 2004.

Školení MSSF CENTRAL

V období od srpna 2003 do dubna 2004 bylo proškoleno celkem 206 uživatelů.

Zabezpečení MSSF CENTRAL

Práva uživatelského přístupu

Postupy jsou formalizovány. Přístupy vč. rolí jsou zřizovány na základě požadavků ŘO.

Plán obnovy systému po havárii, záložní kopie

Je upraveno novou Bezpečnostní politikou informačních systémů MMR (Rozhodnutí č.168/2004 s účinností od 13.9. 2004).

Zjištění (F.1 – F.4)	Stanovisko OMP
<p>Byly zjištěny tyto nedostatky týkající se vývoje a údržby IS MSSF CENTRAL:</p> <ul style="list-style-type: none"> • Kromě formálního převímacího protokolu není k dispozici žádný doklad o testování významných změn systému • V procesu testování významných změn systému není patrné zapojení uživatelů (ŘO) 	<p>Zápisy z jednání Pracovní skupiny obsahují požadavky na změnu, návrh řešení a souhlas s řešením</p> <p>Bylo napraveno: Vytvořen dokument Pokyny pro uživatele IS MSSF CENTRAL (platí od 1.11.2004) – definuje postupy řešení vad, úprav aplikace, evidence testování uživateli. Vytvořen dokument Metodika provozování aplikace MSSF CENTRAL, která definuje postupy zpracování změn mezi uživateli, dodavatelem a MMR. Zřízena Evidenční databáze změn. (od 1.11.2004) pro evidenci a sledování postupu řešení všech požadavků.</p>

<ul style="list-style-type: none"> • Programátoři dodavatele (TESCO) mají plný, vzdálený přístup k živé aplikaci a datům MSSF CENTRAL • V systému MSSF CENTRAL je prováděno několik desítek drobných změn měsíčně. Tyto změny nerespektují žádné formální postupy řízení změn a jsou implementovány přímo do živého systému. Dodavatel poskytuje na konci měsíce statistické údaje. • Přestože rozhraní systému MSSF Central – Viola bylo testováno v červenci, rozhraní bylo upraveno a jeho úprava nadále probíhá. Pro umožnění přenosů rozhraní je nezbytné aktivní zapojení programátorů Viola a MSSF CENTRAL 	<p>Přístup je dočasný, bude ukončen.</p> <p>Bylo napraveno: Vytvořen dokument Pokyny pro uživatele IS MSSF CENTRAL (platí od 1.11.2004) – definuje postupy řešení vad, úprav aplikace, evidence testování uživateli. Vytvořen dokument Metodika provozování aplikace MSSF CENTRAL, která definuje postupy zpracování změn mezi uživateli, dodavatelem a MMR. Zřízena Evidenční databáze změn. (od 1.11.2004) pro evidenci a sledování postupu řešení všech požadavků.</p> <p>Od 12.7.2004 se rozsah předávaných informací (datových polí) mezi IS MSSF-CENTRAL a Viola zásadně nemění. Přístup programátorů je dočasný, bude ukončen. Bude obousměrný automatický přenos.</p>
<ul style="list-style-type: none"> • Postup správy (administrace) práv uživatelského přístupu není formalizovaný 	<p>Postupy jsou formalizovány. Přístupy vč. rolí jsou zřizovány na základě požadavků ŘO.</p>
<ul style="list-style-type: none"> • Neexistuje plán obnovy systému po havárii pro MSSF 	<p>Bylo napraveno: Bezpečnostní politika informačních systémů MMR (Rozhodnutí č.168/2004 s účinností od 13.9. 2004)</p>

G2 Proces IT a zabezpečení počítačů

Organizační schéma OI neodpovídá současnému stavu. OI má, na základě Rozhodnutí ministra č. 197/2004 ze dne 25.10.2004, již pouze dvě operační oddělení:

231 - Oddělení podpory uživatelů a správy aplikací

232 - Oddělení koncepce, vedení projektů a správy serverů

Činnosti zabezpečované oddělením 932 - Správy a evidence HW a SW (údržba a nákup HW, evidence SW a HW, řízení dodavatelských smluv) byly rozděleny mezi stávající oddělení tak, že na Oddělení podpory uživatelů a správy aplikací (231) zajišťuje evidenci HW a ostatní činnosti přešly na Oddělení koncepce, vedení projektů a správy serverů (232).

OI má dále na základě systemizace MMR (Rozhodnutí ministra č. 198/2004 ze dne 27.10.2004) pouze 14 kmenových zaměstnanců (včetně ředitele odboru a sekretářky), dále 3 externí pracovníky.

V části **Celková činnost IT** jsou tyto nesrovnalosti:

- Na serverech s operačním systémem Unix jsou mimo jiné provozovány webové aplikace, spisová služba (evidence písemností), personální informační systém a poštovní služby MMR.
- Pracovní stanice nejsou a ani nikdy nebyly založeny na operačním systému Windows 2000, používal se operační systém Windows NT 4.0 Workstation a v současné době se přechází na Windows XP (přechod bude završen do konce roku 2004).
- Servery s operačním systémem Windows slouží zejména pro sdílené adresáře, síťové tiskárny, antivirové programy, MS Exchange, MSSF, DIS, CEDR a jiné systémy. Servery s operačním systémem Windows nikdy nebyly využívány pro firewallovou ochranu MMR!

V části **Celkové zabezpečení** jsou následující nesrovnalosti:

- Vytvoření bezpečnostní politiky pro oblast informačního systému MMR vyplynulo nejenom z připravované Informační strategie, ale a to zejména, z Bezpečnostní strategie MMR, která byla přijata Rozhodnutím ministra č. 56/2001 ze dne 13.12.2001. Toto rozhodnutí ukládá přípravu jednotlivých bezpečnostních politik do poloviny roku 2002.
- Klasifikace informačních aktiv na MMR **již existuje** a byla provedena nově jmenovaným bezpečnostním manažerem. V souvislosti s organizačními změnami na MMR k 1.11.2004 - změna organizační struktury MMR a systemizace probíhá v současné době aktualizace klasifikace informačních aktiv tak, jak je to vyžadováno Bezpečnostní politikou informačního systému MMR.
- Interní audit probíhá v OI od prosince 2002 a do současné doby není neuzavřený, byl zaměřen pouze na kontrolu účetních dokladů, objednávek a faktur. Vůbec neřešil personální otázku a ani rozsah činností zajišťovaných OI.
- Opatření ředitele úřadu č. 1/2000 zůstává v platnosti do přípravy bezpečnostní dokumentace navazující na Bezpečnostní politiku informačního systému MMR. Předpokládaný termín přípravy navazujících směrnic je do konce roku 2004.

K části **Uživatelská přístupová práva** OI připravuje formalizaci pokynů a postupů upravujících uživatelská práva v souladu se zaváděním Bezpečnostní politiky informačního systému MMR, navazující dokumentace a metodologie ITIL. Předpokládaný termín ukončení současného stavu a nasazení formalizovaného postupu je konec roku 2004.

OI započalo ve spolupráci s externí firmou specializující se na konzultace v oblasti bezpečnosti IS (zaměstnanci této firmy jsou držiteli certifikátu CISA) práce na tzv. studii „Business Continuity Plan“, která je podkladem pro přípravu **Plánů obnovy systému po havárii**, jak je požadováno v odpovídající kapitole Zprávy z auditu PWC. Tato studie bude dodána do konce roku 2004, zároveň s touto studií jsou započaty přípravy na vybudování záložního pracoviště MMR. Předpokládaný termín přípravy kompletních Plánů obnovy systému po havárii je do konce měsíce března 2005.

Situace popsaná v části **Antivirová ochrana** neodpovídá stavu na MMR (ani současnému a ani stavu platnému k 29.10.2004).

- E-mailová komunikace do/z MMR je kontrolována dvoustupňově – v 1. kroku jsou všechny e-maily testovány antivirovým programem NOD32, než jsou přijaty ke zpracování na Exchange serveru a v 2. kroku jsou kontrolovány na pracovních stanicích programem AVG.
- Na MMR je, nad rámec antivirové ochrany e-mailové komunikace, implementováno i antispamové řešení, chránící před nevyžádanou poštou.
- OI zakoupilo systém na antivirovou ochranu HTTP provozu od společnosti Symantec (Symantec Web Security). V současné době probíhají implementační práce a nasazení tohoto systému do rutinního provozu je plánováno do konce roku 2004.

V části **Zálohování dat** uvádí PWC ve své Zprávě nepřesnosti týkající se evidence úspěšnosti zálohovacího procesu. Je sice pravda, že neexistuje (není zavedena) písemná forma protokolu o výsledku zálohování, nicméně díky centrálnímu zálohovacímu systému Veritas NetBackup je prováděn auditní záznam o výsledku zálohy (jak denní přírůstkové, tak i kompletní týdenní) každého serveru zařazeného do systému centrálního zálohování. Tento záznam je uložen na disku Backup serveru (server, který řídí centrální zálohování) a dále je o výsledku zálohy následující den e-mailem informován i správce zálohování.

Kapitola **Serverová místnost** obsahuje následující nepřesnosti:

- Místnosti sousedící se serverovou jsou využívány jako operativní sklad HW. HW zde není uskladněn trvale, ale pouze po přechodnou, nezbytně dlouhou dobu.
- Není pravda, že serverovna není vybavena hasicím přístrojem. Hasicí přístroj v serverově byl i v době prováděného auditu. Jedná se příruční hasicí přístroj CO₂ o hmotnosti 5 kg.
- Skla v oknech jsou vybavena průhlednou bezpečnostní folií bránící jejich rozbití. Tato informace byla poskytnuta i p. Halouzkoovi ze společnosti PWC na schůzce dne 13.9.2004.

Vyjádření ke **Zjištěním a doporučením týkajícím se IT systémů a zabezpečení MMR:**

- Přijatý bezpečnostní manažer byl formálně jmenován do funkce Rozhodnutím ministra č. 168/2004 ze dne 13.9.2004. Stejným rozhodnutím byla vydána i Bezpečnostní politika informačního systému MMR jako dokument závazný pro všechny zaměstnance. O této skutečnosti byl informován p. Halouzka z PWC při schůzce dne 13.9.2004.
- Bezpečnostní manažer provedl klasifikaci informačních aktiv. Stávající klasifikace je platná ke dni 15.10.2004. V současné době probíhá nová klasifikace informačních aktiv v důsledku výrazných organizačních změn na MMR.
- Požadovaná dokumentace standardů zabezpečení IT je v současné době v procesu vytváření. Dokončení této dokumentace je předpokládáno do konce roku 2004, resp. u dokumentace týkající se Krizových situací a obnovy systému po haváriích do konce měsíce března 2005.