KŐ Andrea – SZABÓ Zoltán

A TUDÁSMENEDZSMENT ÉS AZ IT-AUDIT KAPCSOLÓDÁSI PONTJAI – A TUDÁSMENEDZSMENT-RENDSZEREK AUDITJA

A cikkben a szerzők megvizsgálják a tudásmenedzsment komplex rendszerfejlesztési projektekben és az informatikai auditban játszott szerepét. Fő céljuk, hogy a tudásmenedzsment-rendszerek fejlesztéséhez kapcsolódó audit támogatására értékelési modellt készítsenek. Cikkükben megvizsgálják a tudásmenedzsmentnek az IT-auditban játszott általános szerepét, az auditban érintett tudásvagyon védelmének kérdését, a tudásmenedzsment-folyamatok szerepét a rendszerfejlesztésben (auditszempontból), a kontrollok implementálását, valamint a tudásmenedzsment és az IT-audittal kapcsolatos szabványok, módszertanok kapcsolatát. Az eredmények illusztrálására egy az Európai Unió 7. keretprogramjából finanszírozott nemzetközi projekt (GUIDE, IST–2003–507498) szolgál.

Kulcsszavak: **IT-audit, kockázat, kockázatelemzés, tudásmenedzsment-rendszerek**

A tudásmenedzsment- (TM) megoldások hatékonyan támogathatják az informatikai fejlesztéseket. Az egyik ígéretes, és kutatási szempontból számos kihívással bíró terület az ontológiák és az ontológiára épülő TM-rendszerek. Az ontológiaalapú alkalmazások fejlesztése napjainkban gyakran alkalmazott, népszerű megoldás, főleg az összetett és nagy, vállalati méretű alkalmazások, vagy nemzeti és nemzetközi szintű e-kormányzati megoldások esetében. Ezek nem „csak" IT-projektek, hanem összetett tudásmenedzsment-projektek speciális TM-vonatkozású jellemzőkkel és kockázatokkal. Az ilyen fejlesztések értékelése és auditja speciális megközelítést igényel. Tudásmenedzsment-rendszerek értékelésekor a TM-vonatkozású aspektusokat is vizsgálni kell, ami kiegészítő követelményeket ad az audithoz.

Az audit-módszertanok kockázatalapú megközelítésre épülnek, ezért az IT-auditornak az audit korai fázisaiban kockázatelemzéssel kell foglalkoznia. Ebben a cikkben is elsősorban az IT-auditra és annak tudásmenedzsment-aspektusaira koncentrálunk, de nem szabad megfeledkeznünk arról sem, hogy a tudás auditja is releváns koncepció. A problémakör feltárásához elsőként hadd mutassuk be a témához kapcsolódó legfontosabb definíciókat és kapcsolataikat!

A tudáshoz kapcsolódó auditokat a szakirodalom két csoportba osztja. „Az információs audit az a folyamat, amely eredményesen meghatározza a jelenlegi információs környezetet azáltal, hogy feltárja, milyen információ szükséges a szervezeti igények kielégítéséhez" (Henczel, 2000: 211. old.). E definíció szerint az információs audit olyan eszköz, amely a stratégiailag jelentős információs erőforrások azonosítására használható, és segít azonosítani azokat a feladatokat és tevékenységeket, melyek tudást hoznak létre, vagy a szervezet más területeiről induló tudástranszferen alapulnak (Henczel, 2000). Az információs audit a feltárt, dokumentált információs erőforrások tudástérképének kifejlesztésére koncentrál. Alkalmazható arra, hogy segítségével azonosítsuk a szervezetben előállított információt és annak értékét, a szakértelmet, a tudásvagyont, valamint az információs hiányosságokat. Felhasználható arra is, hogy megvizsgáljuk a külső és belső információforrások használatát, feltérképezzük az információáramlást, az információs folyamatokat és a bennük megjelenő szűk kapacitásokat.

A tudásaudit inkább a tacit tudásra és a szervezet tudására koncentrál, mint pl. a tudás és a szervezeti tudás viszonya, mindaz a tudás, információ, tapasztalat, szakértelem és vállalati know-how, ami a személyzet fejében van. A tudásaudit a szervezet tudásmenedzsment-területének „egészségességét" vizsgálja. Arra szolgál, hogy meghatározza a szervezet tudásvagyonának eredetét, a kialakítás módját és végeredményét. Tipikus esetben a tudásaudit két fő célt igyekszik elérni: meghatározni, mely problémák hatnak a tudásteremtésre, transzferre, megosztásra; valamint megvizsgálni, hogy milyen tudás összegyűjtésére van lehetőség, hol van rá szükség, és miként lehet azt újrahasznosítani. Foglalkozik azzal is, hogy milyen eredményes és hatékony módszerek állnak rendelkezésre a tudás tárolásához, eléréséhez és transzferéhez (Henczel, 2000). „Az átfogó és részletes tudásaudit a szervezet tudásmenedzsment-képességeinek, meglévő tudásvagyonának és tudásmenedzsment-tevékenységeinek a teljes körű vizsgálatát, szemlézését, értékelését jelenti.

A tudásaudit tényekre alapozott, elemző, magyarázó és az eredményeket közzétevő tevékenységsorozat, melynek része a szervezet információs és tudáspolitikájának, tudásfolyamatainak, valamint struktúrájának elemzése is. A szervezeti tudásvagyont teszi átláthatóvá (Hilton, 2002).

A tudásaudit a szervezeti tudásvagyon, a kapcsolódó TM rendszerek szisztematikus áttekintése, ezek megfelelőségének és integritásának ellenőrzése. Problémaorientált tevékenység, amely feltárja a rendelkezésre álló tudást, a hiányzó tudást, ezek lehetséges felhasználóit, valamint a szervezeti tudáshasznosítás javasolt módját (Liebowitz, 2000).

Az információrendszerek ellenőrzése, auditja az előzőekben felsoroltakkal szemben egy olyan folyamat, amely azért gyűjt és értékel bizonyítékokat, hogy

- meghatározza, vajon az információrendszer és a kapcsolódó erőforrások megfelelően védik-e az erőforrásokat,
- biztosítják-e az adatok és rendszerek integritását,
- eredményesen támogatják-e a szervezeti célok elérését releváns és megbízható információk szolgáltatásával,
- hatékony-e az erőforrás-felhasználásuk, és
- érvényben vannak-e megfelelő belső ellenőrzési és irányítási eljárások (kontrollok) az üzleti, üzemeltetési és biztonsági célkitűzések teljesítésének biztosítására, a nemkívánatos események megelőzésére, felismerésére és korrekciójára (ISACA 2005).

A tudásmenedzsment és az IT-audit kapcsolata számos aspektusból leírható, vizsgálatával rengeteg izgalmas problémára derülhet fény. A következő szakaszban az IT-audit szakterületre koncentrálunk, bemutatva a tudásvonatkozású problémaköröket.

A tudásmenedzsment és az IT-audit kapcsolata

A tudásmenedzsment és az IT-audit viszonyrendszere összetett. Nagyon leegyszerűsítve, a TM folyamatai és az IT-audit kölcsönösen támogathatják egymást. Az auditornak megfelelő ismeretekkel kell rendelkeznie az auditálandó rendszerről és annak környezetéről. Az audit végrehajtásához össze kell gyűjteni, és rendszerezni kell a releváns tudást, hogy képes legyen a vizsgálandó rendszer céljának, funkciójának, a hozzá kapcsolódó potenciális kockázatoknak a feltárására. Az auditornak az értékeléshez fel kell térképeznie és értékelnie kell a releváns tudáselemeket. Ezt a folyamatot jól kialakított TM-folyamatok támogatni képesek, és növelhetik az eredmény értékét. A nem megfelelő TM-folyamatok viszont rendkívül fáradtságossá teszik az auditot, és korlátozzák az eredmények hasznosíthatóságát. A TM-rendszerek értékes forrásai lehetnek az audithoz szükséges ismereteknek. Számos TM-megoldás segítheti az auditot, többek közt a következők:

- auditvonatkozású szakterületi ontológiák segíthetik a koncepcionális értelmezési zavarok elkerülését,
- dokumentummenedzsment-rendszerek és szövegbányászati megoldások támogathatják az auditjelentések további elemzését.

Az audit a fő forrása lehet az IT-rendszerekkel, folyamatokkal, a szervezettel, a kockázatokkal kapcsolatos tudásnak, a tacit tudás explicitté transzformálásával, vagy akár új tudás feltárásával (pl. hiányosságok felismerésével, melyek auditszempontból másfajta menedzsmentet, további kontrolleszközöket igényelnek).

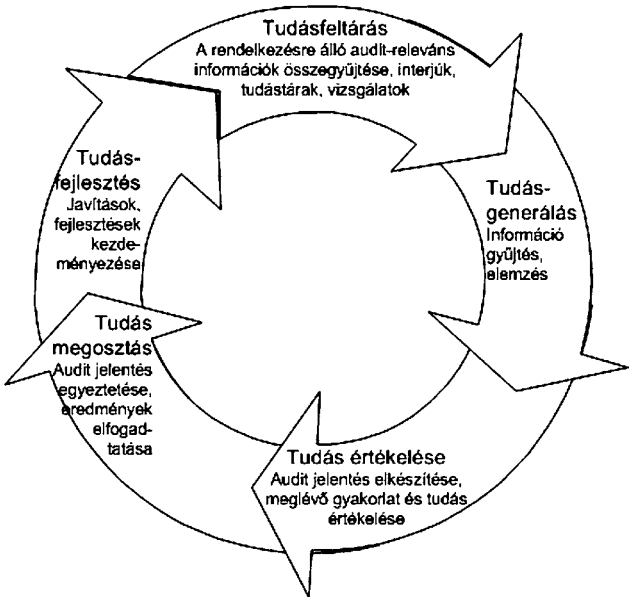
Egy másik fontos apektusa a kérdésnek, hogy az audit a tudásmenedzsmenttel és a TM-rendszerekkel kapcsolatos kockázatok feltárására is alkalmazható. Egy tipikus eset, amikor az audit eredményeként kiderül, hogy nem megfelelő az információs és a tudásvagyon védelme, pl. a TM-rendszerek tudásbázisának nem kielégítő jogosultsági és azonosítási rendszere miatt.

Másrészről az audit maga is TM-kockázatok forrása lehet. Magas a kockázata annak, hogy értékes tudásvagyon kerül illetéktelen kezekbe. Hogyan védheti egy szervezet az audit által érintett tudást? A tipikus IT-alapú védelmi megoldásokon túl (mint pl. a naplózás, a beléptetési rendszerek) a tudásmenedzsment további eszközöket kínál, mint amilyen a tudásmegosztási politikák alkalmazása.

Az IT-audit speciális alosztálya a TM-rendszerek auditálása, ahol az összes fentebb említett probléma releváns.

1. ábra

Az IT-audit tevékenységekhez kapcsolódó TM-folyamatok



A tudásmenedzsment életciklusa

Az 1. ábra bemutatja az IT-audit tevékenységekhez kapcsolódó TM-folyamatokat. A TM-életciklus alfolyamatai interpretálhatók auditaspektusból. Az auditornak információt és tudást kell gyűjtenie a vizsgálandó területről. Ismernie kell a korábbi évek audit eredményeit, a kontroll környezetet és eljárásokat (tudásfeltárás és generálás). Az összegyűjtött tudásra alapozva az auditornak értékelnie kell a helyzetet, és el kell készítenie az audittervet. Az auditfolyamat során az auditreleváns tudást alkalmazzák, miközben az auditált szervezettel való együttműködés is nélkülözhetetlen. Az auditfolyamat eredményeként létrejött jelentés megállapításait, javaslatait meg kell osztani a szervezeti vezetéssel, a következtetéseket pedig az érintett szervezeti egységnél fel kell használni a felmerült problémák megoldására, a gyakorlat fejlesztésére (tudásmegosztás és fejlesztés).

Az 1. táblázat összefoglalja a TM és az IT-audit kapcsolatát. Az IT-audit releváns tevékenységeket a TM-életciklus fázisai szerint mutatjuk be. Célunk a TM legfontosabb értéknövelő lehetőségeinek feltárása. Az értékelésben az auditfolyamat jellegzetes TM-vonatkozású kockázatai szintén fontos szerepet játszanak, ezért a táblázat ezeket is tartalmazza *(1. táblázat, lásd a 25. oldalon).*

Tudásmenedzsment – biztonsági szabványok

A következőkben a tudásmenedzsment és az IT-audit /IT-szolgáltatásmenedzsment/biztonsági szabványok kapcsolatával foglalkozunk. A szakirodalomban számos szabvány elérhető, mely tudásmenedzsment szempontból is hasznos lehet. Ebben a cikkben csak a legfontosabb, leggyakrabban hivatkozott szabványokkal foglalkozunk.

A kontrollok implementálása, a tudásmenedzsment és az IT audit/szolgáltatási/biztonsági szabványok kapcsolata – a releváns auditszabványok: COBIT, ITIL

Az IT-menedzsment és biztonsági szabványok, módszertanok számos szervezet szakembereinek szakmai közösségei által a legjobb gyakorlatokból, konszenzusos, kompromisszumos alapon kristályosodtak ki. Az IT-szolgáltatások menedzselését támogató szabványok (pl. COBIT és ITIL), a biztonsági szabványok (pl. Common Criteria, ISO 15408), a rendszerfejlesztés (Bootstrap, ISO 12207 stb.), rendszerbevezetés, projektmenedzsment (PMBOK, PRINCE2), a minőségbiztosítás (ISO 9001) és a kockázatmenedzsment (COSO) szabványai mind kiforrott, gyakorlatban is sikeres módszerekből erednek (best practice). A legtöbb kormányzati szabályozásnak (mint pl. a Sarbanes-Oxley Act) való megfelelés megköveteli a szabványok alkalmazását. A szervezetek rendszerint de facto szabványokat alkalmaznak (mivel egy belső szabványfejlesztés a költségessége mellett hiányosságokat is tartalmazhat, míg a hivatalos szabványok elfogadottan biztosítják a törvényi elvárások teljesítését). A nagyobb szervezetek már megtanulták, hogy saját biztonsági politikák, szabványok kialakítása nemcsak drágább, de rendszerint kevésbé sikeres is, mint a hivatalos szabványokra (pl. az ISO 17799) való támaszkodás (Oud, 2005).

A tudásmenedzsment áthatja a legtöbb (ha éppen nem az összes) szervezeti tevékenységet, főleg az IT területén. A fent említett szabványoknak is számos tudásorientált aspektusa van. A szabványok tipikusan fontos eszközök az informatikai rendszerek bevezetéséhez és használatához szükséges közös nyelv kialakításához. Az adaptáció folyamatában a szervezeti tanulásnak meghatározó szerepe van. A legjobb gyakorlatra épülő szabványok és módszertanok nagy hangsúlyt fektetnek a tudás externalizációjára, tudástárak, átfogó dokumentáció és a releváns tacit tudás explicitté tétele révén. A tudásmegosztás standard mintáit is gyakran maguk a szabványok nyújtják (pl. a PRINCE2 dokumentációs sablonokat biztosít). Az ITIL folyamatai és a CobIT kontrollcéljai közül számos fokozottan tudásorientált:

Az ITIL központi funkciója a konfigurációmenedzsment, mely a szervezet IT-infrastruktúrájának

1. táblázat

A tudásmenedzsment és az IT-audit kapcsolata

TM-életciklus fázis	*IT-audit releváns tevékenységek*	*A TM értéknövelő lehetőségei*	*TM-vonatkozású kockázatok az auditfolyamatban*
Tudásmenedzsment vízió és célok definiálása (értékelési-fázis)	Az IT-audit céljainak és hatókörének definiálása	Közös nyelv, szakmai alap biztosítása (pl. szakterületi ontológiákkal), egységes megközelítés a TM és az IT-audit stratégia terén	Az audit nem illeszkedik a stratégiához Értelmezési problémákból eredő nem világos célok és vízió Az audit hatóköre nem optimális A piaci ismeretek hiánya irreleváns beavatkozásokhoz vezethet
A rendelkezésre álló tudás feltérképezése (feltárás, generálás fázisa)	Rendelkezésre álló információs erőforrások előzetes felbecslése	Technikai tudás rendelkezésre állása – pl. tudástérkép	Nagy mennyiségű releváns tudás rejtve marad Az előkészítés hosszabb és erőforrás-igényesebb Nem megtervezett a tudásvagyon védelme
A tudás megszerzése: szakértelem begyűjtése (pl. strukturált/ strukturálatlan interjúk, megfigyelések) Kérdőívek stb.(feltárás, generálás fázisa)	Adatgyűjtés, megfigyelés, interjúk, dokumentumelemzés az auditfolyamat támogatására	Közös nyelv (pl. ontológia) biztosítja a tudásmegosztást a résztvevők közt, segíti a tacit tudás feltárását, a tudástárak dokumentálják az explicit tudást	Félreértésekből fakadó potenciális konfliktusok Szükségtelenül nagy erőfeszítések az adatgyűjtésben A feltárt tények nem megfelelő értelmezése A kontrollálatlan tudáserőforrások védelme megoldatlan
Új tudás fejlesztése (fejlesztés és generálás fázisa)	Az audithoz szükséges tudás meghatározása és kifejlesztése	Külső és belső tudástárak segítik az értékelést és a javaslatok elkészítését	A feltárt információk rossz értelmezése A szükséges tudás hiánya korlátozza a relevanciát A szervezeti célok és igények félreértése irreleváns eredményekhez vezet
A tudás megosztása	Az audittal kapcsolatos és az auditált alkalmazottak számára releváns tudás megosztása, az auditfolyamat eredményeinek elfogadtatása, megbeszélése	TM-kultúra és mechanizmusok biztosíthatják a tudás megosztását és intézményesítését	A tudásmegosztás számos kockázattal bír, ilyenek az eltérő szakmai háttér, kultúra, a bizalom hiánya stb.)
A tudás hasznosítása	Javító célú beavatkozások, fejlesztési tervek készítése	A magasabb szintű tanulási potenciál segíti az új ismeretek, gyakorlatok, módszerek elsajátítását.	Az új tudás (eredmények) nem intézményesíthető, az irreleváns javaslatokat elszabotálják
Értékelés	Megvalósítás utáni szemle, visszacsatolások	Tudástárak, szakértő rendszerek és ontológiák segíthetik az összehasonlítást és értékelést A tudásvagyon kontrollja a teljes folyamatra kiterjeszthető	A tudásvagyon feletti kontroll elvesztését nem észlelik, az eredmények nem használhatók visszacsatolásként

(nemcsak a hardver, szoftver és hálózati eszközök, hanem szolgáltatások, eljárások, eseményfeljegyzések stb.) komplex modell formájában való reprezentációja érdekében elosztott, akár tacit tudás összegyűjtését is igényli. A probléma itt kevésbé a nyilvántartások összeállításán és vezetésén van, hanem inkább a nagyszámú elem közti összetett, és gyakran rejtett összefüggések feltárásán.

A változtatáskezelés az infrastrukturális változások fölötti kontrollt biztosítja. Ez megköveteli az infrastruktúráról karbantartott részletes ismeretek meglétét, és formalizált, nyomon követhető tudásmegosztást a folyamat során.

Az eseménykezelés és a problémamenedzsment népszerű és széles körben alkalmazott ITIL-funkciók. Az eseménykezelés felelős az IT-szolgáltatások zökke-

nőmentes fenntartásáért azáltal, hogy technikai zavarok esetén gyorsan helyreállítja a szolgáltatást. A problémamenedzsment már proaktív jellegű, az események újbóli előfordulásának megakadályozásáért felelős. Mindkét terület megköveteli a tudásmegosztást, a naprakész ismereteket az infrastruktúráról, és igényel egy átfogó tudásbázist (pl. az események kezelési megoldásairól). Több TM-alkalmazást is felhasználhatnak, mint a szakértő rendszereket, adatbányászati megoldásokat.

Az ontológiák, tudástárak, tudásbázisok és egyéb TM-alkalmazások nagyon jól hasznosíthatóak a fenti szabványok szervezeti megvalósításában. Ezek nélkül az ITIL funkciók és az egyéb szabványok, módszertanok implementációja csaknem lehetetlen, de mindenképpen nagyon kockázatos volna.

A COBIT esetében hasonló helyzetet figyelhetünk meg. Ha csak néhány magas szintű kontrollcélt vizsgálunk is (a COBIT 3-ból), mint a kockázatértékelés (PO9), a külső szolgáltatók kezelése (DS2), a folyamatos szolgáltatás biztosítása (DS4), vagy az eljárások fejlesztése és karbantartása (A14), megfigyelhetjük, hogy az eljárásokban és formális rendszerekben, technikai megoldásokban (mint pl. a tudásmegosztás, ontológiák) megtestesülő tudás előfeltétele az egyes kontrollcélok megvalósításának.

A fenti példákból látható, hogy a tudásmenedzsment eszközei és megoldásai szükséges és nélkülözhetetlen elemei az IT-szabványok implementációjának, mivel jelentősen csökkenthetik a kockázatot és elősegíthetik az adaptációt. A tudásmenedzsment kulcstényező az IT-szolgáltatásmenedzsment és biztonsági szabványok hasznosításában. A következőkben a probléma másik oldalát is vizsgáljuk: hogyan lehet a kockázatkezeléssel és az IT-szabványokkal a tudásmenedzsmentet támogatni?

Kockázatok a TM-rendszerek fejlesztésében

Az IT-rendszerek fejlesztésének kockázatos jellege a sikertelen kezdeményezések nagy számával jól demonstrálható. Módszertanok és szabványok segíthetik ennek a problémának a kezelését. A rendszerfejlesztés nehézségei mellett a sikeresen megvalósított rendszerekkel kapcsolatos operatív kockázatok menedzselése is elvárható, ebben a megfelelő IT-szolgáltatásmenedzsment és biztonsági szabványok játszhatnak szerepet. A fentebb említett audit és szolgáltatásmenedzsment-vonatkozású szabványok többsége éppen erre az operációs aspektusra koncentrál.

Komplex természetüknél fogva magas szintű kockázatok köthetők a tudásmenedzsment-rendszerek fejlesztéséhez is. A TM-alkalmazások bukási arányát 50 és 70% közé becsülik (Ambrosio, 2000). Ez a kockázatos jelleg az üzemeltetésre is igaz. Vizsgáljuk meg közelebbről elsőként a tudásmenedzsment-rendszerek fejlesztésének problémakörét!

Egyes tudásmenedzsment-alkalmazásokban (pl. szakértő rendszerek) a beépített tudás megköveteli a szakértelmet mind az IT, mind a tudásmenedzsment területén. E rendszerek megvalósítás utáni szemlélése rendkívül nehézkes lehet. A rendszerekbe ágyazott tudáselemek karbantartásának hiányosságai és a beépítendő új tudáselemek validációjának elmaradása a rendszerek mellőzéséhez vezethetnek.

A szervezeti igények, illetve tudásmenedzsment-rendszerekkel szemben támasztott követelmények nem világos definiálása.

A nem konszolidált, egységesített, nem világos terminológia sikertelen rendszerekhez vagy inkonzisztens tudásbázishoz vezethet. Egy másik hasonló probléma a tudásstruktúra hiánya. Emiatt a tudásmenedzsment-rendszerek, leginkább az ontológiák, nagyon fontos szerepet játszhatnak a rendszerek fejlesztésében. Ez különösen igaz nemzetközi fejlesztések vagy nagyobb, különböző háttérrel rendelkező projekttagok esetén.

A jogi, szabályozási, etikai követelmények kezelése további kockázati forrást jelent.

Másrészről a tudásmenedzsment-alkalmazások maguk komoly operatív kockázatok forrásai.

A tudásvagyon kontrollálatlan elérése a szervezeteket a biztonsági követelmények fokozott figyelembevételére ösztönzi.

A tudásvagyon sérülése károkat okozhat a szervezetekben, pl. tudáslopás. A tudásvagyon nem megfelelő változtatása nem megfelelő minőséget és csökkent hasznosíthatóságot okozhat. Mivel a nem IT-szakértők (pl. szakterületi szakértők) szerepe nagyon fontossá vált a tudásmenedzsment-rendszerek üzemeltetésében és karbantartásában, e tevékenységek ellenőrzése alapvető igény a szervezetekben. A komplexitás eredményeként a tudásmenedzsment-rendszerek változtatáskezelése rendkívül összetett és időigényes lehet.

A tudásmenedzsment-alkalmazások esemény- és problémakezelése speciális szakértelmet kíván, és a dokumentációt kiemelten fontossá teszi.

Bár a tudásmenedzsment-rendszerekkel szembeni rendelkezésre állási követelmények nem olyan magasak, mint az alapvető tranzakciófeldolgozó-rendszerek esetében, az ilyen rendszerek kiesése így is nagyon komoly károkat okozhat.

A fent említett valamennyi probléma még összetettebbé válhat, ha a tudásmenedzsment-alkalmazást egy külső szolgáltató biztosítja. Az SLA meghatározása összetett feladat. Mivel e rendszerek és szolgáltatások értéke hamar erodálódhat az üzleti és versenykörnye-

zetben bekövetkezett dinamikus átrendeződések miatt, a karbantartás egy problematikus, de fontos témakör.

A tudásmenedzsment-rendszerek fejlesztésének auditálási nehézségei a TM-projektek sajátos jellegzetességeiből erednek. Ezek a projektek egyrészt kapcsolódnak az IT-területhez (az összes IT-projektmenedzsment problémakör releváns) másrészt a tudásmenedzsmenthez is, mivel a TM-vonatkozású kockázatokat is számba kell venni. Az audit jó lebonyolítása érdekében az auditornak alaposan ismernie kell több várhatóan elkülönült területet (mint pl. az ontológiafejlesztő eszközök, a tudásmenedzsment-eszközök, a TM-környezet, az alkalmazott szabványok, a feldolgozandó tudásterület). Számos szerepkörnek kell zökkenőmentesen kooperálni az audit folyamán (pl. a területkör szakértői és az IT szakértői). Emiatt a TM-alkalmazások fejlesztésének értékelése összetett feladat, melynek több összekapcsolódó dimenziója van. A következő részben az ilyen auditok támogatására szolgáló modellt mutatunk be.

Értékelési keretrendszer tudásmenedzsment-rendszerek fejlesztési projektjeihez

Ahogyan az a tudásmenedzsment-szakirodalomból ismert, minden tudásmenedzsment-kezdeményezés egyben változás is a szervezetben. A vállalatoknak a folyamatos változás kihívásával kell szembenézniük, és ez természetesen hat a tudásmenedzsment-rendszerek fejlesztési projektjeire is. Gondoljunk pl. a szakterületi tudás változására, vagy azokra a környezeti változásokra (pl. változások a szabályozási környezetben), amelyek befolyásolják a szakterületi tudás. A változáskezelésnek nagy szerepe van abban, hogy a rendszer a változások következtében előálló új követelményeknek megfeleljen. A tudásmenedzsment-rendszerek ugyanakkor segíthetik a tudásmenedzsment-folyamatok felülvizsgálatát, szükség szerinti átalakítását és a szervezeti kultúra, rutinok módosítását.

A tudásmenedzsment-rendszerek fejlesztése során számos kockázattal kell szembenéznünk. Az egyes projektekben meg kell határozni a kockázatviselés szintjét, amely függ a szervezeti kultúrától, az ellenőrzési tevékenységek hatékonyságától, az alkalmazott szabványoktól. A kockázatkezelésnek kitüntetett szerepe van napjainkban, többek között a változásmenedzsment megnövekedett súlyának köszönhetően.

A tudásmenedzsment-projektek sikere, hasonlóan egyéb projektekéhez, megtérülésükkel kapcsolatos. Ezen a területen ugyanolyan nehézségekkel kell szembenéznünk, mint egyéb rendszerfejlesztési projektekben. A hasznok egy része nem vagy nehezen számszerűsíthető, pl. „hatékonyabb ügyintézés, vagy elégedettebb ügyfelek", ezért a nem megfogható eredmények kimutatására is alkalmas mutatószámrendszert kell felhasználni. Ugyanakkor a megtérülés igazolása alapvető elvárás a menedzsment részéről. Másfelől a tudásmenedzsment-rendszerek fejlesztése erőforrás- és költségigényes, elsősorban a felhasználásra kerülő humán szakértelem miatt. A fejlesztés során számos kockázatot kell kezelni, pl. a szervezeti változásokat, a fluktuációt. A tudásmenedzsment-rendszerek fejlesztése során legalább háromféle kockázattal kell számolnunk: az informatikai kockázatokkal, a projektmenedzsment-kockázatokkal és a tudásmenedzsment-kockázatokkal. Az általunk javasolt kiértékelési keretrendszer kockázatalapú megközelítést követ. Az alkalmazott kockázati kategóriák a következők:

- a felhasznált informatikai eljárások, módszertanok, pl. a CommonKADS az ontológiafejlesztés területén,
- az alkalmazott szabványok, pl. COBIT, ITIL,
- dokumentáció és kezelése (van-e dokumentációs szabvány, támogató IT-megoldás),
- a szabályozási környezetnek való megfelelés,
- a tudásmenedzsment-követelményeknek való megfelelés,
- a beépített tudás minősége,
- a tudásmenedzsment-folyamat minősége, eszközei (pl. a tudásmegosztás módja, értékelése),
- a változáskezelés módja,
- a projektszervezet, pl. vannak-e a projektszervezetben definiált tudásmenedzsment-szerepkörök.

A kockázatkezelés első lépése a tudásmenedzsment-rendszerek fejlesztése során fellépő kockázatok összegyűjtése a felsorolt dimenziók mentén. A következő lépés a kockázatok hatásainak feltárása *(2. táblázat)*, vagyis az egyes dimenziókhoz tartozó kockázatok egyfajta szubjektív értékelése, az ellenőr előzetes tapasztalatai alapján. Az értékelés során valamennyi kockázati dimenzióhoz egy numerikus értéket rendelünk egy és öt között. Az öt a nem megfelelő, az egy a legjobb, ajánlható kategória *(3. táblázat)*. A súlyozott auditátlag az egyes numerikus értékek átlaga (a példában 2,84). Ha a súlyozott auditátlag három alatti, akkor a vizsgált tudásmenedzsmentrendszer-fejlesztési projekt fontossági szintje alacsony, ha három, akkor a fontossági szint közepes, ha három feletti, akkor a fontossági szint magas. A vizsgált tudásmenedzsment-rendszer fejlesztési projekt kockázataihoz rendelt bekövetkezési valószínűség egy szubjektív érték, amely háromféle lehet, magas, alacsony és közepes. A fontossági szint és a bekövetkezési valószínűség határozza meg a kockázati kategóriát a kockázati mátrixnak megfelelően *(4. táblázat)*.

2. táblázat

A kockázatok kiértékelése

Kockázati területek	Súlyozott audit-átlag	Fontossági szint	Valószínűség	Kockázati kategória
Informatikai eljárások, módszertanok	1	alacsony	magas	közepes
Alkalmazott szabványok	3			
Dokumentáció és kezelése	3			
Szabályozási környezetnek való megfelelés	5			
Tudásmenedzsment követelményeknek való megfelelés	3			
Projektszervezet	2			
Súlyozott audit átlag	2,84			

Ha a kockázati kategória magas, alapvető hiányosságok vannak a tudásmenedzsment-rendszer fejlesztése során, a projektmenedzsment nem volt megfelelő, a tudásmenedzsment-szempontokat nem vették figyelembe. Ha a kockázati kategória közepes, vannak nem megfelelő területek a tudásmenedzsment-rendszer fejlesztése során, találtak kontrollokra vonatkozó hiányosságokat, de nem az összes szempont vonatkozásában. Ha a kockázati kategória alacsony, a tudásmenedzsment-rendszer fejlesztése megfelelően történt.

3. táblázat

Auditosztályok

Kategória	Leírás
5 Nem kielégítő	Az ellenőrzött dimenzió/tevékenység nem felel meg az előírásoknak, eljárásoknak, a szabványoknak.
4 További javítás, fejlesztés szükséges	Az ellenőrzött dimenzió/tevékenység nem minden esetben felel meg az előírásoknak, eljárásoknak, a szabványoknak.
3 Átlagos	Az ellenőrzött dimenzió/tevékenység általában megfelel az előírásoknak, eljárásoknak, a szabványoknak.
2 Jó	Az ellenőrzött dimenzió/tevékenység megfelel az előírásoknak, eljárásoknak, a szabványoknak. Vannak audithiányosságok, de ezek következményeként nem alakulnak ki magas kockázati kategóriák.
1 Kiváló, példaértékű	Az ellenőrzött dimenzió/tevékenység megfelel az előírásoknak, eljárásoknak, a szabványoknak. Nincsenek lényeges kontrollhiányosságok.

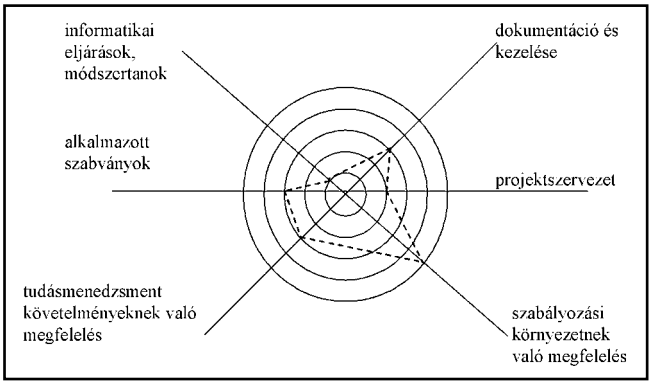
4. táblázat

Kockázati mátrix

Fontossági szint	Valószínűség	Kockázati kategória
Magas	Magas	Magas
Magas	Közepes	Magas
Közepes	Magas	Magas
Magas	Alacsony	Közepes
Alacsony	Magas	Közepes
Közepes	Közepes	Közepes
Alacsony	Közepes	Alacsony
Közepes	Alacsony	Alacsony
Alacsony	Alacsony	Alacsony

2. ábra

Értékelési keretrendszer a tudásmenedzsment-rendszerek fejlesztéséhez



Az értékelési keretrendszer alkalmazása a Guide ontológiafejlesztési projektre

A 2. ábrán bemutatott értékelési keretrendszert a Guide projektben kifejlesztett tudásmenedzsment-megoldáson keresztül demonstráljuk. Az ismertetett tudásmenedzsment-rendszer egy a személyazonosítás és hitelesítés területre kialakított informális ontológia (ebben a kontextusban egy szakterület formális leírása) prototípusa. A fejlesztés sajátosságait a következő rész tartalmazza.

A Guide projektben kialakított ontológia fejlesztésének sajátosságai

A személyazonosítás és hitelesítés terület fogalmi leírása, modellezése napjaink aktuális, ugyanakkor kihívásokkal bíró feladata, többek között a következő okok miatt:

- az elektronikus szolgáltatások terjedése (és így a személyazonosítás és hitelesítés iránti megnövekedett igény),
- a technológiai fejlődés felgyorsulása,

- a személyazonosítási és hitelesítési megoldások életciklusának rövidülése (pl. a biometrikus azonosítókkal ellátott intelligens kártyaprogramok Európa több országában),
- a törvényi és szabályozási környezet és annak változásai (pl. a nemzeti adatvédelmi törvények),
- a biztonsággal kapcsolatos követelmények.

A szakterületi tudás leírásának és rendszerezésének hatékony eszközei a szakterületi ontológiák. A szakirodalomban egy gyakran hivatkozott ontológiameghatározás Gruber nevéhez fűződik:

„Az ontológia a fogalmi modell (fogalomalkotás) világos és részletes leírása" (Gruber, 1993: 199. o.), ahol a fogalmi modell, illetve a fogalomalkotás egy adott szakterület gondolkodásmódját tükrözi.

Egy ontológia különböző formákban jelenhet meg, de mindenképpen tartalmaznia kell a tárgyterület szakkifejezéseit, terminológiáját és a jelentésük leírását (szemantika). Az ontológia gyakorlatilag mindig egy szakterület közös értelmezésének megjelenése, amely elősegíti a különböző érdekelt felek közötti kommunikációt. Egy ilyen közös alap hozzájárul a pontos és eredményes információcseréhez, amely lehetőséget nyújt az újrafelhasználhatóságra, a közös használatra és a közös üzemeltetésre.

Az ontológia fentiekben tárgyalt előnyeit vettük figyelembe a Guide projektben is. A projekt (IST-2003-507498 6th Framework Programme) célja egy az elektronikus kormányzatot támogató személyazonosítási és hitelesítési architektúra kialakítása. A projektben több mint húsz partner vett és vesz részt különböző európai országokból. Az összetett, különböző hátterű partnereket tömörítő projektszervezet igényli a közös szakmai alap létrehozását. A személyazonosítási és hitelesítési ontológia jól támogatja ezt a törekvést.

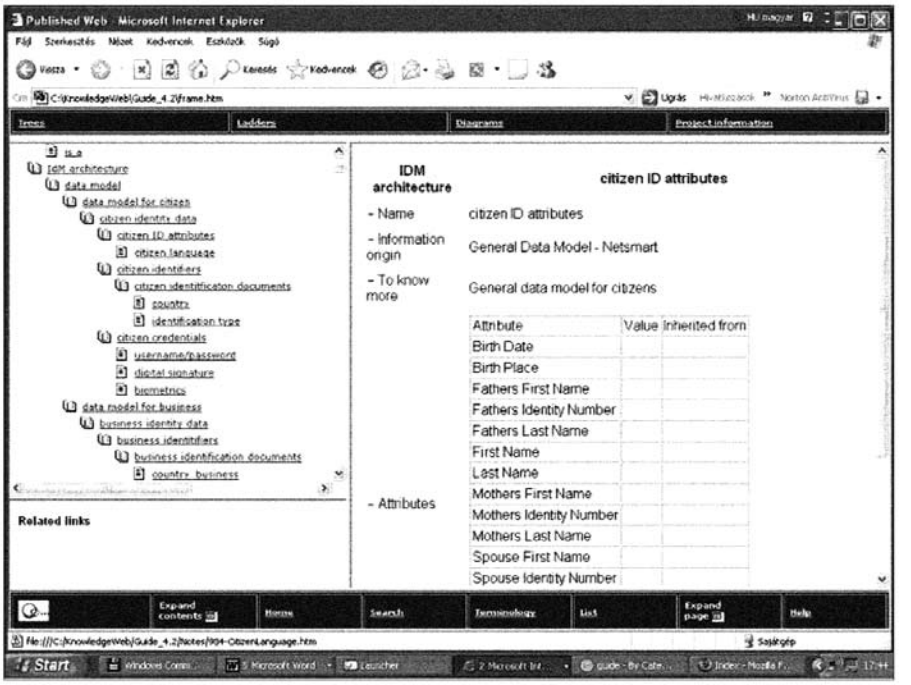
Az ontológia fejlesztését az alkalmazott módszertan alapvetően befolyásolja. A szakirodalomból számos fejlesztési módszertan ismert, így a leggyakrabban hivatkozottak a következők: TOVE, Menthology, Plinius, Enterprise Model Approach, CommonKADS (Schreiber, 1999) és a Sure-Studer módszertan (Fensel, 2003). Az ontológia fejlesztése során egy az előzőekben felsorolt módszertanokra támaszkodó, de elsődlegesen a Sure-Studer módszertant követő saját megközelítést alakítottunk ki.

Az ontológiafejlesztő környezetek vonatkozásában is számos megoldás közül választhatunk. A kiválasztott fejlesztőeszköz a PcPack4 lett. A kiválasztást a fejlesztési feladat elméleti hátterének és a PcPack4–nek a hasonlósága indokolta. Különösen fontos és előnyös volt a PcPack4 hatékony tudásmodellezési támogatása a tudásszerzés kezdeti fázisaiban.

A rendszer hasznosságai közül ki kell emelnünk a tudásmenedzsmenthez kapcsolódó előnyöket, a tudásmegosztás hatékonyabbá tételét az ontológia web-es változatának segítségével *(3. ábra)*. Az egységes terminológia támogatja a „közös szakmai nyelv" megalapozását. Az együttműködést a PcPack4 elősegíti, így a közös fejlesztés megvalósítható.

3. ábra

Az ontológia html verzója, az ojektum fa egy részlete és az állampolgári azonosító attribútumainak annotációja



Az értékelési keretrendszer alkalmazása a Guide ontológia prototípus-fejlesztési projektre

Ebben a részben bemutatjuk a Guide ontológia prototípus kifejlesztésére alkalmazott értékelési keretrendszert. Ez a projekt egyszerre IT- és tudásmenedzsment-projekt is. A kockázati területek felmérése alapján jutottunk az 5. táblázatban összefoglalt értékekhez.

Az informatikai eljárások, módszertanok dimenzióhoz 2-t rendeltünk, mivel a fejlesztés nem ad-hoc módon történt, hanem igazodtunk a meghatározó módszerta-

nokhoz. A tudásbázis html-verziója publikus, az ontológia biztonsági szempontból megfelelően védett. Az alkalmazott szabványok dimenzióhoz szintén 2-t rendeltünk, szabványos ontológianyelvet használtunk (RDF), és figyelembe vettük a COBIT auditmódszertan ajánlásait a fejlesztés során. A dokumentáció és kezelése is 2 értéket kapott, az alkalmazott dokumentummenedzsment-rendszer és az együttműködést támogató környezet használata (Docushare) miatt. A szabályozási környezetnek való megfeleléshez 3-at rendeltünk (a szabályozási környezet igen összetett, pl. a nemzeti adatvédelmi törvények és az európai adatvédelmi törvény egyaránt része). A tudásmenedzsment-követelményeknek való megfelelés dimenzióhoz 3-at rendeltünk, a tudásmenedzsment-folyamatok, különösen a tudásmegosztás minőségét a rendszer javította. Ennek ellenére a partnerek egy része idegenkedett a számukra szokatlan IT-megoldástól. A tudáselemekhez tulajdonosokat rendeltünk, akik azok karbantartásáért felelnek. A változáskezelést a PcPack4 verzió kezelése és a „discussion forum" biztosítja. A projektszervezet is 3-at kapott, mivel nem sikerült megvalósítani a feladatkörök teljes körű szétválasztását, maradtak átfedő szerepkörök *(4. ábra).*

5. táblázat

A kockázatok kiértékelése

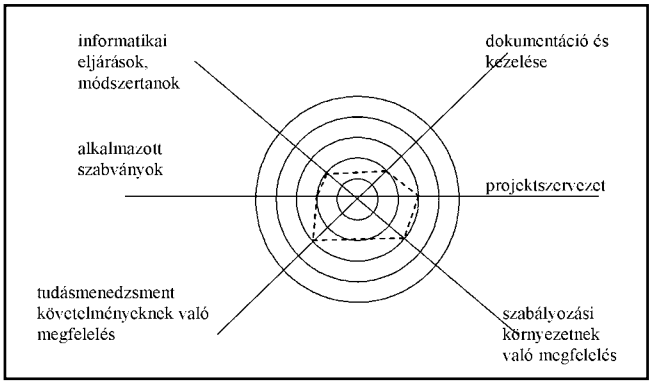
Kockázati területek	Súlyozott audit átlag	Fontossági szint	Valószínűség	Kockázati kategória
Informatikai eljárások, módszertanok	2	alacsony	közepes	alacsony
Alkalmazott szabványok	2			
Dokumentáció és kezelése	2			
Szabályozási környezetnek való megfelelés	3			
Tudásmenedzsment követelményeknek való megfelelés	3			
Projektszervezet	3			
Súlyozott audit átlag	2,5			

Konklúzió, további kutatási kérdések

A tudásmenedzsment és az IT- audit is napjaink aktuális, fontos témakörei, amelyek hatékonyan alkalmazhatják egymás eljárásait, megoldásait. Egyre több tudásmenedzsment-rendszert használnak mindennapi feladatokra is, ezért a tudásmenedzsment-rendszerek fejlesztési projektjeinek kiértékelése alapvető, különösen a fejlesztési költségek igazolásának szempontjából.

4. ábra

Az értékelési keretrendszer alkalmazása a Guide ontológia prototípus-fejlesztési projektre



Az általunk használt keretrendszerben az értékelés alapjául a fejlesztés során felmerülő kockázatok összessége szolgál. Mind a tudásmenedzsment, mind az IT-kockázatok számbavétele alapvető az értékelés során.

A kutatás következő szakasza a keretrendszer finomítását, javítását célozza meg, a kockázati kategóriák aktualizálásán keresztül. További cél több teszteset kipróbálása, és egyúttal a tudásmenedzsment-rendszerű fejlesztési projektek sajátosságainak elemzése.

Felhasznált irodalom

Ambrosio, J. (2000): Knowledge Management Mistakes, (online), http: //www.computerworld.com/industrytopics/energy/story/0,10801,46693,00.html

Fensel, D. – van Harmelen, F. – Davies, J. (2003): Towards the Semantic Web – Ontology driven knowledge management, John Wiley & Sons Ltd., West Sussex

Fensel D. (2001): Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce, Springer-Verlag, Berlin

Hylton, A. (2002b): A knowledge audit must be people-centered and people focused, (online), http://www.knowledgeboard.com/library/people_centered_knowledge_audit.pdf

ISACA (2005): CISA Review Manual, Inc, Illionois, USA

Liebowitz, Jay et al. (2000): The knowledge audit. Knowledge and Process Management. Volume 7 Issue 1, pp 3–10.

Oud, E. J. (2005): The Value to IT of using International Standards. Information Systems Control Journal, V3, pp 35–39.

Schreiber, A. Th. et al. (1999): Knowledge Engineering and Management: The CommonKADS Methodology Version 1.1, University of Amsterdam

Cikk beérkezett: 2006. 12. hó
Lektori vélemény alapján átdolgozva: 2007. 3. hó