Az információbiztonság kérdése az agilis projektmenedzsmentben

Dr. Beinschróth József – Dombora Sándor
Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar

1084. Budapest, Tavaszmező u. 17.
beinschroth.jozsef@kvk.uni-obuda.hu
dombora.sandor@kvk.uni-obuda.hu

***Összefoglalás* –A klasszikus projekmenedzsment gyakorlatokkal szemben egyre inkább terjed az agilis módszertan. Ennek rugalmassága, dinamizmusa, hatékonysága kétségkívül jelentős előnyöket adhat, azonban mindezek számos információbiztonsági kockázatot is felvetnek. A cikk ezek felmérését, értékelését, jelentőségét, kezelhetőségét tárgyalja.**

I. Bevezetés

Egyre általánosabbá válik, hogy az egyes szervezetek tisztában vannak azzal, hogy működési folyamataikat különböző kockázatok fenyegetik, és ennek következtében előfordulhat, hogy kritikus folyamataik megszakadhatnak, bizalmasság sérülések következhetnek be. Egyre általánosabb az is, hogy a szervezetek védelmi intézkedésekkel előre felkészülnek az ilyen helyzetek kiküszöbölésére és a védelmi intézkedések részeként informatikai katasztrófa terveket készítenek. A védelmi intézkedések azonban – ahogyan a szervezetek működését meghatározó szabályzatok (pl. Szervezeti Működési Szabályzat, SZMSZ), folyamatleírások, munkaköri leírások, stb. – tipikusan a szervezetek mindennapi, rutinszerű tevékenységeihez kapcsolódó folyamatokra vonatkoznak.

Ugyanakkor a szervezetek mindennapi, rutinszerű tevékenységeik közé nem besorolható tevékenységeket is végeznek. Számos feladat projekt keretek között kerül megvalósításra, a projektszerű működés egyre inkább előtérbe kerül. Ennek fő oka az, hogy a tapasztalatok szerint a rutinszerű, csak a tevékenység (termék) minőségének javítására, illetve a hatékonyság növelésére koncentráló szervezet hosszabb távon elveszíti versenyképességét. A versenyképesség megőrzésének, a versenyelőny realizálásának feltételét többnyire a folyamatos innováció jelentheti.

Ismert tény, hogy az informatikai projektek jelentős hányada nem úgy valósul meg, ahogy a megrendelő megálmodta. Gyakran tovább tart vagy drágább a tervezettnél, esetleg a végeredmény nem kielégítő.

A projektszerű működés során számos kockázat léphet fel mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás területén. [1] Az egyes kockázatok jelentősége a projekt előrehaladása során változhat.

II. Projektek IT biztonsági kockázatai

A hagyományos projektek módszertana fix mérföldkövekhez kapcsolódó, a külső kockázatok kezelésére kevésbé alkalmas módszertan. A követelmények meghatározását követi a tervezés, a megvalósítás, az ellenőrzés, a végén pedig az üzemeltetés – az egyes lépések tipikusan egymásra épülnek, egymás folytatásai [4,5].

A hagyományos módszertan alapja, hogy az eredmény-termékkel szemben támasztott elvárásokat a projekt elején meghatározzuk, készítünk egy tervet és e tervet követve implementáljuk a rendszert. Elvileg ez egy tökéletesen működő rendszer, hiszen ha a terv jó és a projekt során folyamatosan követtük, akkor biztosan az előre meghatározott eredmény-terméket kapjuk.

Minden projekt során bekövetkeznek azonban változások (új információ kerül napvilágra vagy új, esetleg módosult igény) lépnek fel. Ez az jelenti, hogy a projekt elején hiába egyeztetünk le mindent, a munka során szinte mindig el kell térni a megbeszéltektől: a fejlesztés közben derülhetnek ki olyan információk, amik felboríthatják az előzetes terveket és új, megváltozott igényeket eredményezhetnek megrendelői oldalról. Nem lehet elmenni az új információk, a változáskezelési igények mellett pusztán azért, mert azok nem szerepelnek az előzetes tervekben. Ha pedig figyelembe vesszük ezeket, akkor az a határidőre és a költségekre is jelentős hatással lehet.

A projektek sikerét a projekt folyamán elsősorban az esetlegesen bekövetkező kiesések, leállások veszélyeztetik. Egy konkrét projekt akkor tekinthető sikeresnek, ha az elvárt eredmény a tervezett határidőn belül, a számára rendelkezésre bocsátott erőforrás kereteket nem átlépve jön létre. A sikertelen projekt mindenképpen számottevő

(nemcsak közvetlen anyagi, hanem például presztízs) veszteséget okoz. Az egyedi (egyszeri) jelleg jelentős mértékben megnöveli a projekt sikertelenségének kockázatát, hiszen az egyszeri végrehajtás miatt a begyakorolt módszerek, a bevált gyakorlat pontos, készségszintű alkalmazása – legalábbis a projekt egészére vonatkozóan – ez esetben szóba sem kerülhet. A mindennapi, rutinjellegű tevékenységek a projektszerűen végrehajtott tevékenységektől sok szempontból különböznek.

A rutinjellegű tevékenységek alapvető jellemzői, hogy általános, a szervezeti alaprendeltetéshez kapcsolódó célok megvalósítására, vagy ezek feltételeinek biztosítására irányulnak, továbbá időben folyamatosan, ismétlődően kerülnek végrehajtásra. Jellemző rájuk ezen kívül, hogy végrehajtásuk rendjét szervezeti és működési szabályzatok határozzák meg, valamint, hogy az adott feladat folyamatos végrehajtására létrehozott szervezeti munkakörök, a statikus szervezeti hierarchiában elhelyezkedő szervezeti egységek valósítják meg.

Ezzel szemben a projekt meghatározott egyedi cél elérésére irányuló, egységes elgondolás alapján végrehajtott tevékenységek összessége, amely jól definiált költségkerettel, kezdő és befejezési időponttal rendelkezik, jellemzője az egyszeri végbemenetel, továbbá, hogy működésnek feltételeit kifejezetten erre a célra készített dokumentumok (Projekt terjedelem meghatározás, Projekt Definíciós Dokumentum, stb.) határozzák meg.

A normál, rutinjellegű, mindennapi folyamatokat számos kockázat fenyegeti. Általánosan kijelenthető, hogy mindazon kockázatok a projekt keretek közötti működést is veszélyeztethetik, amelyek a mindennapi, folyamatos működés esetén előfordulhatnak. Ezen kockázatok szokásos csoportosítása a következő:

- fizikai veszélyforrások;
- logikai kockázatok;
- szervezeti és működési kockázatok;
- életciklushoz kapcsolódó kockázatok.

A mindennapi, rutin tevékenységek és a projektszerű működés között a fizikai és logikai kockázatok tekintetében alapvető különbségek nem állapíthatók meg: minkét esetben ugyanazon kockázatok tekinthetők relevánsnak (a projekt tevékenység eltérő – pl. nem helyhez kötött – volta miatt kisebb jelentőségű eltérések azonban jelentkeznek). Lényeges különbség van azonban a kétféle működés között a szervezeti és működési kockázatok tekintetében. Projekt keretek között történő működés esetén nem az általános, a szervezeti és működési szabályzatok határozzák meg a működést, hanem kifejezetten az adott projekt működési feltételeit meghatározó szabályzatok (melyek vagy folyamatosan léteznek vagy ideiglenesen – pl. utasítások formájában – jönnek létre jellemzően nem eléggé alaposan átgondolva). Ezekre vonatkozóan nyilvánvaló elvárás, hogy nem mondhatnak ellent az érvényes szervezeti és működési szabályzatoknak. Komoly, gyakran nehezen áthidalható problémát jelentenek a projekt végrehajtásában részt vevő különböző szervezetek (sok esetben több jogi személy) belső szabályzatainak ellentmondásai. A tervezett határidő betartását veszélyeztetheti, ha az ellentmondások feloldása elhúzódik, emiatt a működési feltételeket meghatározó szabályok kidolgozása nem történik meg időben.

Ugyancsak kockázatot jelent a nem megfelelő, nem mindenre kiterjedő, hibás vagy nem megfelelő szinten elfogadott szabályzat is. Projektszerű működés esetén kritikus lehet, ha a különböző változások nem megfelelőképpen vannak kezelve. Ennélfogva a jól definiált változáskezelési mechanizmus hiánya, illetve nem hatékony működése ugyancsak kockázatként értékelhető. (A változáskezelési mechanizmusnak megfelelő működés a mindennapi, rutin tevékenységek esetén is fontos, de a gyorsan fellépő változtatási igények, valamint a betartandó határidők miatt projekt keretek közötti működés esetén ez a tényező lényegesen nagyobb jelentőséggel rendelkezik. Minél nagyobb a változás, annál kevésbé lehetséges a szabályozás, ugyanakkor annál inkább szükség van rá.) Léteznek olyan kockázatok is, amelyek a projektszerű működés életciklusához kapcsolódnak. Ezen a területen megjelennek olyan kockázatok is, amelyek a normál, mindennapi működés során gyakorlatilag nem lépnek fel. A projektszerű működés egy meghatározott életciklus követését, azaz a következő egymás utáni lépések végrehajtását jelenti (1. A projekt definiálása; 2. A projekt végrehajtásának tervezése; 3. A projekt végrehajtása; 4. A projekt lezárása, az eredményátadása; 5. A projekt értékelése). Ezen lépések közül nyilvánvalóan az első négyhez kapcsolódhatnak kockázatok.

A projektszerű működést veszélyeztetheti a projekt (azaz a cél és a feladat, valamint a terjedelem) nem pontos definiálása. Előfordulhat, hogy a kitűzött cél ugyan teljesül, az előírt feladat az előírt határidőn belül, a tervezett erőforrások felhasználásával elvégzésre kerül, ugyanakkor a végső probléma mégsem oldódik meg (a célkitűzés volt hibás), vagy hogy a cél csak úgy érhető el, ha a tervezett területeken kívül mást is megváltoztatunk (a terjedelmet rosszul határoztuk meg).

Projekt keretek közötti működési környezetben, az eddigiekben felsorolt kockázat kategóriákon (fizikai, logikai, szervezeti és működési valamint az életciklushoz köthető kockázatok) túlmenően megjelennek újabb kockázat kategóriák is. A kifejezetten a projektszerű működés esetén fellépő kockázatok a következő kategóriákba sorolhatók:

- jogi jellegű kockázatok;
- kulturális jellegű kockázatok;
- komplexitásból eredő kockázatok;
- ismeretlen jellegű kockázatok.

Jogi jellegű kockázatként vehető figyelembe, hogy a projekt keretek közötti működés helyszínén esetlegesen speciális jogszabályi feltételek létezhetnek, illetve, hogy a működés során a vonatkozó jogszabályok megváltozhatnak. Kulturális jellegű kockázatként értékelhetjük, hogy a projekt keretek között megvalósuló tevékenységnek olyan különböző szervezetek, esetleg országok közötti együttműködésként kell megvalósulnia, amelyek egymástól eltérő kultúrával (társadalmi, technológiai, informatikai, biztonsági stb.) rendelkeznek. Ide sorolhatjuk az együttműködő partnerek közötti nyelvi nehézségeket is. Komplexitásból eredő kockázatok alatt azokat értjük, melyek abból erednek, hogy egy nagy komplex és egyedi feladatot egyszerre (idő-, költség- és egyéb erőforráskorláttal egy irányítás alatt, koordinálva) akarunk kezelni. Ez szemben áll a normál működéssel, ahol a feladatok dekomponálva, szakterületenként vagy más logikával külön irányítással, felelősség szerint is szétbontva, fokozatosan kidolgozott/fejlesztett módszerekkel folyamatosan oldunk meg. A projektszerű működés során számítani lehet olyan kockázatokra is, amelyek a korábbiakban nem fordultak elő, így ismeretlennek kell tekintenünk őket. Bár ismeretlen kockázatok a mindennapi, normál működés esetén is megjelenhetnek, fellépésükre projektek esetén fokozottan kell számítani. Ennek oka, hogy projektszerű működés esetén nem rutinszerű, az adott környezetben ismétlődő, sokszor kipróbált tevékenységekről van szó, így a tevékenység és a környezet egymásra hatása előre nem látható kockázatok fellépését okozhatja. Az előzőeken túlmenően létezhetnek pénzügyi jellegű kockázatok is. Ezek nem újabb kategóriát jelentenek, a felsorolt kategóriákat átfedhetik, de az eddigiektől különböző megközelítéssel vehetők figyelembe. A pénzügyi jellegű kockázatok az anyagi erőforrások (általában) korlátozott volta miatt jelennek meg. Leginkább azért következhetnek be, mert az adott feladathoz rendelt költségvetés nem tartalmaz megfelelő tartalékokat és a projekt során az esetlegesen fellépő, előre nem várt költségek leginkább az informatikai biztonság biztosításra fordított anyagi erőforrásokat emésztik fel.

III. Az agilis módszertan

Az agilis módszertant többnyire a kevésbé kiszámítható projektek esetén szokás alkalmazni [6], ugyanis ez a megközelítés a projekt megvalósítása során felmerült kockázatok azonnali és hatékony kezelésére alkalmas. Használata IT fejlesztési projektek esetén tipikus. Periódusokra (ciklusok) épül, ezek végrehajtása során minden esetben meghatározásra kerül egy aktuális priorizált feladatlista, ezután egy előre meghatározott időtartam (általában 2 hét) alatt megtörténik a feladatok végrehajtása (tipikusan elemzés, fejlesztés, tesztelés, integráció). Minden periódus végén megtörténik a visszacsatolás (sprint kiértékelés), melynek következtében jobb minőség érhető el: bemutatják az elkészült terméket, kiértékelik a megoldott feladatokat és megvizsgálják, hogy a felhasználói igényeknek megfelel-e a végeredmény. Így nemcsak egyszer, a projekt végén történik ellenőrzés, hanem a folyamat során többször is.

A periódus végén értesítik az érintetteket, lezárják a periódust és összegyűjtik a következő periódus feladatlistáját. Fontos, hogy az agilis módszertan esetén sem marad el a tervezés, de ha változás történik a projektben, nem hagyják azt figyelmen kívül csak azért, mert az az eredeti tervekben nem szerepelt. Ez esetben a terveknek az új információknak megfelelően azonnal módosulniuk kell.

Az agilis projekt menedzsment előnye a szinte azonnali adaptálhatóság, hátránya pedig az, hogy komplexebb feladatok (amelyek nem bonthatóak le rövid ciklusokra) kezelésére nem alkalmas.

Az agilis szemlélet a módszertan helyett a működőképes termékre, a motivált és a cél érdekében együttműködő projekttagokra helyezi a hangsúlyt. A csapat feladata az, hogy a megrendelő által felvázolt üzleti problémára hathatós megoldást találjon úgy, hogy az a rögzített költség- és időkeretbe beleférjen.

Az agilis módszertan gyökerei az 1990-es évekre nyúlnak vissza, mikor is az alkalmazásfejlesztőkre jellemző laza, rugalmas magatartást szerették volna viszontlátni a projektmenedzsment terén is.

Az agilis irányzatok hívei 2001-ben lefektették a legfőbb alapelveket, ez az un. Agile Manifesto, vagyis az Agilis Kiáltvány. A kiáltvány kimondja, hogy:

- az egyének és a köztük lévő interakciók, vagyis a személyes kommunikáció előnyt kell, hogy élvezzen a folyamatokkal és eszközökkel szemben,
- a működő szoftver fontosabb, mint az azzal kapcsolatos részletes, átfogó dokumentáció,
- az ügyféllel történő együttműködés értékelendőbb a szerződéses tárgyalással szemben,
- a változásokra történő reagálást előnyben részesítjük a tervek követésével szemben [2].

Az agilis módszertan nem egyértelműen fejlettebb vagy jobb, mint a hagyományos. A hagyományoshoz képest egy alternatívát nyújt, amelyet akkor célszerű választani, ha

- a környezet gyorsan változik, ahol a megrendelő igényei gyakran módosulnak;
- projekt csapat tapasztalt, megbízható, önszerveződő, elkötelezett projekttagokból áll;
- a projekt kicsi vagy közepes méretű.

Kerülni kell az agilis módszertant, ha

- a környezet főképpen szabályokra, parancsokra épül és változásoktól mentes;
- a szereplők nem vállalják fel a döntéseket, problémás a felelősség vállalása és az egyének nem hajlandóak azonosulni a szervezet céljaival;
- a projekt nagyméretű.

IV. Az agilis módszertan szerint végrehajtott projektek sajátosságai

Az agilis módszertan sokak szerint nem is igazi módszertan, hanem inkább egy sajátos hozzáállás a projektek során felmerülő feladatok és problémák megoldásához.

Fő jellemzői a rugalmasság, dinamizmus, gyorsaság, hatékonyság, emberközpontúság. A jó minőségű, gyors végrehajtásra koncentrál úgy, hogy a projekt sikeressége ne sérüljön. Nyilvánvaló korlátai a méret: bizonyos projektméret fölött szóba sem jöhet; és a bizalom: az együttműködő feleknek gyakorlatilag korlátlanul kell bízniuk egymásban, ezzel összefüggésben kiváló csapatmunkára van szükség. Ezek egyúttal kockázatokat is jelentenek: a túlzottan nagy méretű és nem a maximális bizalomra épülő agilis projekt nagy valószínűséggel nem lesz sikeres.

Bármilyen projekt esetén igaz, hogy a cél a működő termék és nem a dokumentáció, ugyanakkor az is egyértelmű, hogy tervezés és dokumentáció nélkül nem lehet projektet végrehajtani. Biztos azonban, hogy a projekt során történő folyamatos dokumentálás az agilis projektekben kisebb jelentőségű. A tervezés, követés és dokumentálás kisebb súlya nyilvánvalóan ellentmond bizonyos információbiztonsági szempontoknak.

Az agilis megközelítésnél a költségek és a határidők rögzítettek, ezekből indulunk ki, míg a hagyományos módszertan esetében ezeket csak becsülhetők. A gyakorlatban ez azt jelenti, hogy az agilis módszertan alkalmazása esetén a fő kérdés, hogy „Ennyi pénzből, ennyi idő alatt mi fér bele?” (A tradicionális modell módszertan esetén ez a kérdés úgy hangzik, hogy: „Mennyi idő alatt és mekkora költségből lehet mindezt megvalósítani?”)

V. Az agilis módszertan IT biztonsági kockázatai

Kétségkívüli tény az, hogy a kiválasztott projektmenedzsment módszertantól függetlenül vannak projekt kockázatok. Ezeket a klasszikus projektmenedzsment módszertanok projekt kockázatok kezelése címén felmérik, elemzik és ellenintézkedéseket foganatosítanak annak érdekében, hogy ne következzenek be, de ha valamilyen oknál fogva mégis megjelennek, csökkentsék az általuk kifejtett hatást. Ezek között jelentős mennyiségben jelennek meg az információbiztonságot érintő kockázatok. [3]

Mint tudjuk, az információbiztonság három alappillére a sértetlenség, bizalmasság és rendelkezésre állás, amelyeket veszélyforrások fenyegetnek. Ezek a kockázatok a projektek végrehajtása és az eredménytermék felhasználása során fejtik ki hatásukat. Összegyűjtöttük és bemutatjuk mindazokat a kockázatokat, amelyek az agilis módszertan alkalmazása során a leginkább relevánsak. A kockázatokat két nagy csoportra bontottuk: projektmenedzsment során fellépő kockázatok és eredménytermékben megjelenő kockázatok.

1. Projektmenedzsment kockázatok

Projektmenedzsment kockázatok kategóriába soroltuk mindazon kockázatokat, amelyek a projekt végrehajtása során jelentkeznek, hatásukat a projektszervezetben és a projektfeladatok végrehajtása során fejtik ki. Ezek a kockázatok inkább a projekt működését érintik, és direkt módon kevésbé befolyásolják a projekt során elkészült eredménytermékeket. Ezek közül az információbiztonsági kockázatok azok, amelyekre fókuszálunk, annak három alappillére mentén.

a. Bizalmasság

Az agilis fejlesztési módszertan kevésbé zárja formális keretek közé a projekt végrehajtását, mint a hagyományos módszertanok. Az agilis módszertan az eredményre teszi a hangsúlyt, és kevésbé tartja fontosnak a projekt végrehajtásának módját, feltételeit. Ennek következtében a projektszervezet rugalmas, gyorsan változhat az igényeknek megfelelően, ami egy pozitív jelenség, ugyanakkor erősen épít a projektben részt vevő projekttagok szakmai és helyi ismereteire, amelyek a projektszervezet változásával együtt változhatnak. Mivel a projektek során sok kis, átlátható, úgynevezett sprintekben megvalósított feladat végrehajtása történik, a projekttagok a projekten belül gyakran változhatnak. Mivel az agilis módszertan a projekt eredménytermék megvalósítását előbbre helyezi a dokumentáció elkészítésénél, az elkészült eredménytermékek dokumentációja gyakran vázlatos, hiányos, vagy egyszerűen elmarad az elkészítése. A változó humán erőforrással megvalósított sok kis feladat különböző fejlesztői képességeket igényel, így előfordulhat, hogy az egymásra épülő feladatokat más-más szakemberek valósítják meg, ahogyan azt a hatékonyság megköveteli. Ugyanakkor előfordulhat, hogy nem létező vagy hiányos dokumentáció következtében a fejlesztők informális módon keresik meg egymást, hogy megismerjék azokat a megoldásokat, amelyeket a korábbi feladatok mentén kollegáik kialakítottak. Az ilyen informális találkozókról általában nem készül emlékeztető vagy jegyzőkönyv, a projektmenedzsment szempontjából nézve ez nem releváns. A megbeszélések során elhangozhatnak üzleti titkok, amelyek megismeréséről a résztvevőket nem nyilatkoztatják, továbbá előfordulhat az is, hogy az általános titoktartásról sem nyilatkoztak a részvevők. A kötetlenebb projekt-adminisztráció miatt a projekttagok gyakran nem tudják egymásról, hogy van-e érvényes titoktartási megállapodásuk, csak azt, hogy az adott személyt a projektgazdák delegálták a projektre. Az előrehaladás érdekében az új projekttagok delegálásakor a formalitások későbbre halasztódhatnak vagy elmaradhatnak, a projektvezetés megbízik a projektre delegált munkatársakban. A projektkommunikáció során nem történik jogosultság ellenőrzés az üzleti titkok megismerésére vonatkozóan, a projektet delegált munkatársak megismerhetik a projekt végrehajtásához szükséges információkat. Az esetek többségében a munkatársak megbízhatók, de előfordulhatnak rendkívüli esetek, amikor távoznak a szervezetből, vagy másik projektre irányítják át őket, még a formaságok megszületése előtt. Azok a személyek, akik ilyen módon jutnak üzleti titkok birtokába és nem köti őket titoktartási megállapodás, potenciális információszivárgási forrásokká válhatnak, és ezáltal komoly üzleti kockázatot hordoznak.

Ha az agilis módszertan filozófiájának megfelelően nemdokumentált kommunikációs csatornák mentén történik a projektkommunikáció, követhetetlenné válik a projekttagok közötti információáramlás. Nem lehet tudni, hogy a projekttagok birtokában milyen információ van és mikor, milyen körülmények között jutott a tudomásukra. Ez egyben azt is jelenti, hogy egy esetleges információszivárgás esetén nem lehet kideríteni, ki, mikor és milyen körülmények között adott ki információt és nem akadályozható meg az esemény megismétlődése.

Amennyiben a konkurencia jut információhoz, jelentős piaci előnyhöz juthat, ennek következtében bizalomvesztés következhet be a projektben réészt vevő szervezetek között ami a felek közötti kapcsolat megromlásához vezethet. Több résztvevős projektek esetében elindulhat az egymásra mutogatás, amelynek következtében felbomolhat a partnerség, gyakorlatilag ellehetetlenülhet és akár meg is hiúsulhat a projekt végrehajtása. A nem létező, vázaltos, vagy hiányos dokumentáció megnehezíti új projektrésztvevők belépését, ugyanakkor új belépőknek gyanúsok lehetnek a projektkörülmények és nehéz lehet pótolni a kieső erőforrásokat. Amennyiben sikerül új projektrésztvevőt találni, hiányos, vázlatos vagy nem létező dokumentáció esetén a projekt folytatása az információrendelkezésre állása esetén lehetséges. Az is előfordulhat, hogy az információhiány jelentős többletráfordítást eredményez.

b. Sértetlenség

Agilis módszertan alkalmazása esetén a projekt résztvevői leginkább informális módon kommunikálnak egymással. Ennek következtében sok esetben feladatok definiálása is informális, azok végrehajtásához nem szükséges a megrendelő írásos jóváhagyása. Az informális kommunikáció következtében a projekttagok az általunk megértett követelmények mentén hagyják végre feladatainkat. A feladatok méretétől függően ezek akár két hét munkavégzést is jelenthetnek. Az így elvégzett munka mennyisége jelentős költséget képviselhet a projekt végrehajtása során.

Ha a megrendelő és a szállító között folytatott projektkommunikáció informális keretek között zajlik, továbbá a szállító projektmegbeszélései is informálisak az átadott információ torzulhat, a felek más-és mást érthetnek ugyanazokon a kifejezéseken a lokális kontextusnak megfelelőn, ami értelmezési problémákhoz, félreértésekhez vezethet. Mivel nincs visszacsatolás arra vonatkozóan, hogy pontosan mit szeretett volna az ügyfél, a munkatársak által elvégzett feladatok végrehajtása félreértésen alapul, ennek következtében az elkészült funkciók részben, akár nagymértékben is eltérhetnek ügyfél által megfogalmazott igényektől. Az, hogy az ügyféllel folytatott kommunikáció során legalább két munkatárs vesz részt a megbeszéléseken, biztosít valamilyen szintű minőségbiztosítást. Mivel nincs megkövetelve az ügyféltől kapott információk visszacsatolása és az elkészült termék fontosabb, mint annak a dokumentációja, ezért a megbeszélések során történt esetleges

félreértések csak akkor derülnek ki, amikor egy-egy funkció bemutatásra kerül. Ha az információ pontatlansága gyakran fordul elő egy projekt során, a feladatokra fordított túlmunka mennyisége jelentős mértékben befolyásolhatja a munkavégzés hatékonyságát, ami jelentős többletköltséget eredményezhet.

Előfordulhat, hogy a bemutatás során az ügyfél nem veszi észre az eltérést, csak akkor, amikor pl. jelentős adatmennyiséget rögzítettek a rendszerben és jelentős adatsérülés következik be. Amennyiben ez utóbbi eset többször is megismétlődik, az adatok javítása jelentős túlmunkát jelenthet az ügyfél számára. Bizalomvesztés következhet be a megrendelő részéről, amely megnehezíti a kommunikációt a felek között, és ellehetetlenítheti a projekt végrehajtását.

Az informális kommunikáció, a dokumentálás hiánya vagy vázlatossága nagymértékben befolyásolhatja az elkészült funkciók minőségét. A hiányosan rögzített követelmények és a követelmények dokumentálásának elmaradása megnehezíti a tesztforgatókönyvek összeállítását. Ugyanakkor a projektek végrehajtása sprintekben, azaz rövid feladatok formájában történik, amelyek keretében funkciók készülnek el, kerülnek átadásra. Az elkészült funkciókat tesztelik, amelyeket verziókiadás és élesítés követ. A gyakori verziókiadás rendkívül nagy mennyiségű tesztelést von maga után, hiszen nem elég az elkészült funkciók tesztelése, hanem a teljes rendszert újra kell tesztelni. A regressziós tesztelés ebben a környezetben jelentős erőforrást igényel, amely sok esetben nem áll rendelkezésre, és nem is végzik el. A nem megfelelő mértékű tesztelés hibás termékhez, a funkciók hiányosságaihoz vagy rendszerhibákhoz vezethet. Ez befolyásolja felek egymáshoz való viszonyát.

A feladatok részletes követelményei csak a feladat elvégzésének elkezdése előtt fogalmazódnak meg. Ennek következtében az igények változása viszonylag egyszerűen beépíthető a projekt során megvalósított termékbe. Ugyanakkor a projektek definiálásakor vázlatosan megfogalmazott eredménytermékek, biztonsági követelmények és a változások dokumentálásának hiányosságai megnehezítik a termékek átadás-átvételét, hiszen nincsenek pontosan definiált követelmények, amelyhez eredménytermékeket viszonyítani lehet.

c. Rendelkezésre állás

A módszertan hangsúlyozza, hogy a projektben minden feladatot legalább két embernek kell mélységében ismernie, de a gyakorlatban ez elmaradhat vagy csak informális módon jelenik meg, ami megnehezíti a minőségbiztosítást a projekt végrehajtása során. Előfordulhatnak olyan esetek, amikor megtervezik a megbeszéléseket, meghívják a résztvevőket, de ők valamilyen oknál fogva mégsem tudnak részt venni. Ezek oka lehet megbetegedés, túlterhelés, amikor az adott erőforrás több projektben is részt vesz és ütközés állhat elő más projektek feladataival. A megbeszélések dokumentálásának hiányosságai és a résztvevők távolmaradása ellehetetlenítheti a feladatok és méreteik pontos méretének meghatározását. Ez befolyásolhatja a munkatársakra kiosztott feladatok elvégzését és mennyiségét. Ez ellehetetleníti a feladatok kontrollját.

Előfordul, hogy az egyes feladatok végrehajtása során további erőforrások bevonására van szükség. Ez mind emberi erőforrás mind pedig eszközök esetében is megnyilvánulhat, hiszen sok esetben az erőforráshoz tervezik a projektet és időközben újabb projektek indulnak el. Amennyiben nem áll rendelkezésre megfelelő mennyiségű emberi erőforrás vagy a szükséges erőforrások csak bizonyos késleltetéssel állnak rendelkezésre, nehézkes vagy elhúzódik a beszerzés, jelentős csúszással kerülnek a végrehajtásra a projektfeladatok.

Az erőforrások rendelkezésre állását befolyásolhatja, hogy a kezdetben elvégzett nagyvonalú becslések hiányosan definiált funkciók megvalósításához tervezett feladatokon alapulnak. Ez olyan, mint a házépítés: a tervezett feladatok rendszerint alultervezettek és az építkezés során derül ki csak, hogy mennyivel kellett volna több erőforrást tervezni. A megvalósítás során megtörténik a feladatok pontosítása, amelyek megvalósítása jelentős többleterőforrás bevonásával hajthatók végre. A jelentős túlmunka eredményeképpen a projektre tervezett erőforrások elfogynak, miközben a tervezett rendszer funkcionalitása csak részben valósul meg. Az is előfordulhat, hogy a projekt végrehajtója egy olyan feladat spirálba bonyolódik bele, amely jelentős mennyiségű túlmunkához vezet, amit adott esetben nem fogad el a megrendelő és ez által jelentős veszteséget jelenthet számára.

A projekt kezdetén végrehajtott nagyvonalú feladatfelmérés hiányosságai nem biztos, hogy kiderülnek a projekt végrehajtása során, azok jelentkezhetnek a rendszer átadásakor, pl. biztonsági hiányosságok formájában. A biztonsági hiányosságok pótlása rendkívül költségigényes feladat, sok esetben a rendszer teljes egészére kiterjed.

Jellemző hiba a projektkockázatok felmérésének elmulasztása. Ez pótolható a projekt végrehajtása során, a sprintekbe rendezett feladatok végrehajtásával, amelyek rugalmassága lehetőséget nyújt a kockázatok kezelésére, de ez nem helyettesíti a kockázatok teljes körű felmérését és kezelését.

2. Eredménytermék kockázatai

A projektek végrehajtásának sikeressége és az eredménytermékek minősége nagymértékben függ a projektfeladatok végrehajtásának módjától, a feladatok és eredménytermékek egymásra épülésének tervezésétől, a projekt során megvalósítandó eredménytermékek tervezésének módjától. Az informatikai projektekben rendszeresek a változások, amelyeknek beépítését nagymértékben támogatja az agilis módszertan, ugyanakkor a megvalósítás során gyakran elmarad a dokumentálás, hiányos vagy elavult az elkészült termék dokumentációja.

a. Bizalmasság

Az informális úton folyatatott kommunikáció funkcionális és nem funkcionális hiányosságokhoz vezethet, amelyek befolyásolják az eredménytermék minőségét, az eredménytermék információbiztonsági megfelelését a helyi és jogszabályi előírásoknak. A háromrétegű webes szoftverarchitektúrák megjelenésével a kliens –szerver architektúrához képest további biztonsági kérdések merülnek fel.

A leggyakoribb problémák közé sorolható a biztonsági tervezés hiánya. A jogosultsági kérdést gyakran a termék előállításához felhasznált keretrendszer beépített funkciójával oldják meg. Előfordul, hogy az alkalmazott keretrendszer még fejlesztési fázisban van, és komoly hiányosságokkal, félig kitesztelt funkciókkal rendelkezik. Ennek következtében az elkészült rendszer jogosulatlan hozzáférést lehetővé tevő biztonsági réseket tartalmazhat, azaz illetéktelenek férhetnek hozzá a rendszerben tárolt és feldolgozott adatokhoz.

A második, rendszerint problémás terület a jogosultsági rendszer kialakítása, amelynek hiányosságai miatt a felhasználók többletjogosultsághoz juthatnak. A nem megfelelő körültekintéssel összeállított jogosultsági rendszer nem biztosítja a felhasználási környezetben szükséges jogosultsági követelményeknek megfelelő eszközkészletet a felhasználói szerepkörök és jogosultságok kialakításához és kiosztásához.

Az informatikai rendszerek fejlesztése során vannak olyan feladatok, amelyek elvégzése hatással van a teljes rendszer működésére. Ezek közé a feladatok közé tartozik a biztonsági követelmények összegyűjtése, a bizalmassági körök meghatározása, a tesztelési feladatok megtervezése és a rendelkezésre állás és a performancia meghatározása. A sprintekben gondolkodó agilis módszertan lényege, hogy megkerülve a hosszas elkészítést és tervezést gyakorlat-orientáltan, egymásra épülő kis feladatokban hajtja végre a projektet, amelyek nyomán kész, használható rendszerfunkciók készülnek el. Ez a hozzáállás nem mindig támogatja megfelelő módon a rendszertervezést és biztonsági tervezést (a biztonsági követelmények összegyűjtését), azaz nem készülnek megfelelő szintű architektúra és biztonsági tervek. Ennek hatására funkcionális és biztonsági hiányosságok jelenhetnek meg az elkészült funkciókban, amelyek veszélyeztethetik a rendszerben tárolt adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

A projekt kereteiben sprintekben megvalósított funkciók átadása folyamatosan zajlik és a projekt részfeladatainak elkészüléséhez kötődik. Előfordulhat, hogy egy-egy sprint végére nem mindig készül el egy-egy funkció teljes mértékben, adott esetben nem teljes körű a tesztelése. Ezen funkciók átadása és élesítése biztonsági réseket nyithat a rendszerben, amelyek adott esetben ismertek is lehetnek. Előfordul, hogy a sprint során elkészült funkciók oktatása nem történik meg, az oktatás részleges vagy csak a funkció végrehajtására fókuszál és nem tér ki annak biztonságos használatával kapcsolatos tudnivalókra, ami adatszivárgáshoz, jogosulatlan hozzáféréshez, adatsérüléshez vagy akár rendelkezésre állási problémákhoz is vezethet.

b. Sértetlenség

Az elkészült eredménytermékek minősége nagymértékben befolyásolja, a rendszer biztonságos használatát és működtetését. Agilis módszertan alkalmazása esetén az elkészült funkciók tesztelése a sprintekhez kapcsolódik, a projekt során a dokumentáció készítése nem tartozik az elsődleges feladatok közé, a tesztelés tervezése és elvégzése kapcsolódik a megfogalmazott követelményekhez. A nem dokumentált vagy hiányosan megírt követelmény specifikáció megnehezíti a teljeskörű tesztelést. Elmaradhat a tesztelés, a sprintek funkcionális tesztelése hiányos dokumentumokon, vagy informálisan közölt követelményeken is alapulhat. Ennek következtében sok esetben csak a funkcionális tesztek végrehajtása az, ami megtörténik. Ugyanakkor előfordulhat, hogy a tesztelés, csak azokra a tesztesetekre terjed ki, amelyek a munkafolyamat részét képezik. Nem történik olyan jellegű tesztelés, hogy mi történik akkor, ha a felhasználói felületen illegális adatokat próbál rögzíteni a felhasználó. Ebből kifolyólag akár rendszerhibák is előfordulhatnak, amelyek feltárják a teljes rendszerarchitektúrát a felhasználó számára. Ez adatszivárgáshoz, hibás adatok rögzítéséhez és adott esetben rendszerkieséshez is vezethetnek.

A sprintekben való fejlesztés, a gyakori verziókiadás, jelentős regressziós tesztelési munkamennyiséget ró a fejlesztőre, hiszen az újonnan elkészült modulok keretében előállított funkciók befolyásolhatják a már meglévő kódbázis működését, megtörténhet egy-egy korábban átadott funkció kibővítése, vagy új funkciók dolgozhatnak

a már átadott rendszerfunkciók által kezelt adatokon. Ezen a funkciómódosítások tesztelése sok esetben csak az új modulra vonatkozóan történik meg, de hatással van a korábban megírt és átadott rendszerfunkciókra is.

Mint láthatjuk fontos szerepet játszik a verziókövetés, az átadott és készülőben lévő funkciók kódjainak szétválasztása. Az agilis módszertan kevés hangsúlyt fektet a dokumentálásra, a sprintek során kiadott szoftververziók kezelése nagy odafigyelést és precíz dokumentálást igényel. A verziókiadás minőségbiztosításának és dokumentálásának elmaradása vagy elnagyolása minőségi kérdéseket vet fel, telepítési és rendszer hibákhoz és hiányosságokhoz vezethetnek, amelyek adatsérüléssel járhatnak.

c. Rendelkezésre állás

Mint tudjuk a rendelkezésre állás egyre fontosabb szerepet játszik a rendszerek által nyújtott szolgáltatások biztosításában. Minél magasabb rendelkezésre állást kell biztosítani, annál komolyabb tervezésre van szükség. Ahhoz, hogy ez a tervezés megtörténhessen, rendszerarchitektúrát kell tervezni, 7x24 órában működő rendszerek esetében nem elég összegyűjteni a követelményeket, fel kell mérni a rendszert futtató környezetet, kialakítani a rendszerek redundanciáját. Mivel a fizikai redundancia megvalósításán túl a fejlesztett rendszerkomponenseket úgy kell kialakítani, hogy kihasználhassak a fizikai architektúra adta redundanciát. A rendszerek rendelkezésre állásának tervezése függ a rendelkezésre álló hardver és szoftver infrastruktúrától, továbbá a rendszerszoftver tervezésétől és megvalósításától. A sprintekben gondolkodó agilis módszertan nem támogatja a projekt elején való részletes tervezést, ez a hiányosság komoly kockázatot hordoz magában magas rendelkezésre állású rendszerek kialakítása során, ugyanis kimarad a koncepcionális és részletes tervezési szakasz, mindig csak a soron következő komponens megvalósítására fókuszál a csapat.

VI. Összefoglalás

Az agilis módszertan információbiztonsági szempontból a klasszikus módszertanok kockázatain túlmenő kockázatokat is magában hordoz. Ezek a kockázatok részben a projektmenedzsmenthez, részben pedig az eredménytermékhez kapcsolódnak. Minkét kategóriában azonosíthatók mind a bizalmassághoz, mind a sértetlenséghez, mind a rendelkezésre álláshoz kapcsolódó kockázatok.

VII. Hivatkozások

1. Az informatikai biztonság kézikönyve, szerkesztő: Muha Lajos, Verlag Dashöfer Szakkiadó, 2000. (folyamatosan aktualizált kiadvány)

2. Csutorás Zoltán, Árvai Zoltán, Novák István: A Scrum keretrendszer és agilis módszerek használata a Visual Studióval, https://www.devportal.hu/download/E-bookok/A%20Scrum%20keretrendszer%20es% 20agilis%20 modszerek% 20hasznalata%20a%20Visual%20Studioval/A%20Scrum%20keretrendszer%20es%20agilis%20modszerek%20 hasznalata%20a%20Visual%20Studioval.pdf (letöltve: 2016.09.10.)

3. Gopal K. Kapur: Project Management for Information, Technology, Business and Certification, Prentice Hall, New Jersey, ISBN 978-0131123359

4. Görög Mihály: Általános projektmenedzsment: Aula Kiadó Kft. 2012.Általános Informatikai Projektmenedzsment Eljárásrend, Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ), 2015.

5. Projektmenedzsment útmutató - PMBOK Guide, Akadémiai Kiadó Zrt. Budapest, ISBN 9789630584012

6. Szilagyi Laszlo Robert, Agilis módszerek és alkalmazásaik, https://prezi.com/tankl7jgozyt/az-agilis-modszerek-es-alkalmazasaik/ (letöltve: 2016.08.30)