Az Informatikai Audit Minőségbiztosítási módszertana

Készítette: Erdősi Péter Máté, CISA

ISACA Budapest Chapter

Informatikai Audit Minőségbiztosítás Munkacsoport

2012. január 2.

Verzió: 2

1. Bevezetés

Az elmúlt években a kialakult gazdasági világválság, a terrorizmus megjelenése, és az információs hadviselés módszereinek megjelenése a privát szférában a szervezeteket, vállalatokat egyre növekvő mértékben késztette a küldetésük teljesítése érdekében speciális biztonsági intézkedésekre. Ezen intézkedések között kiemeljük az ellenőrzés előtérbe kerülését, és annak megbízhatósága, hitelessége érdekében tett intézkedéseket. Ilyen intézkedés a magas minőségű (High Quality) audit kérdése. Ma már e követelmény kielégítésének egyik fontos eszköze az informatikai audit minőségbiztosítása, ami igazolt, módszeres tevékenység, és amely megfelelő bizalmat hivatott kelteni arra, hogy a termék teljesíti a minőségi követelményeket, továbbá rendszerezett és független vizsgálat annak meghatározásra, hogy az audit minőségével kapcsolatos tevékenységek és eredmények megfelelnek és hatékonyan valósítják meg a követelményeket, illetve alkalmasak ezen célok elérésére.

1. A szervezetek, vállalatok elemi érdeke, hogy a végrehajtott informatikai auditokat külső független auditor rendszeresen minőségbiztosítsa. Ezért az ISACA Budapest Chapter javasolja, és támogatja az ilyen irányú tevékenységeket.

2. Az auditornak megfelelő kompetenciával kell rendelkeznie a minőségbiztosítás elvégzéséhez, ami azt igényli, hogy az auditor megfelelő szaktudással, gyakorlattal (referenciával), a teljesítmény eléréséhez szükséges magatartással, képesítéssel, továbbá ISACA tagsággal, és CISA vagy CISM minősítéssel rendelkezzen.

Az audit minőségének biztosítására számos módszer és ajánlás létezik ma már szerte a világban, ezek feldolgozásával készült el ez a módszertani ajánlás, a magyarországon végrehajtott informatikai auditok minőségének megőrzése és magasabb szintre emelése érdekében.

2. Az Informatikai Audit Minőségbiztosítása

Az Informatikai Audit Minőségbiztosítása az audit megfelelőségének garanciális követelménye. Ennek érdekében a minőségbiztosító alapfeladata kettős lehet:

a) az auditor tevékenységének vizsgálata

b) az audit dokumentációs környezetének vizsgálata.

Az első a) tevékenységet a minőségbiztosító kizárólag az audit folyamat végzésével párhuzamosan folytathatja, míg a b) tevékenység végezhető az auditot követően bármikor – amennyiben az audit dokumentációs környezete a rendelkezésre áll, de ekkor a minőségbiztosítónak figyelemmel kell lennie arra, hogy az audit dokumentáció teljessége eltér a folyamat megfigyelésekor szerezhető teljességtől.

Felhívjuk itt a figyelmet arra, hogy a minőségbiztosítónak nem feladata az auditori megállapítások

vitatása vagy javítása, de lehetőséget kell a minőségbiztosító számára biztosítani, hogy az auditot érintő szakmai észrevételeket az auditor felé megtehesse – ez azonban nem bír semmilyen kötelező érvénnyel. A minőségbiztosítás nem párhuzamos auditot jelent, hanem az audit-folyamat megfelelőségének tényszerű és vizsgálaton alapuló ellenőrzését foglalja magában.

Más szavakkal a minőségbiztosítás független, professzionális és etikus minőségi szakvélemény szolgáltatásának a biztosítása (a minőségbiztosítás tárgyáról), amelyet professzionális és etikus audit folyamatok, bizonyítékok, és objektív megítélések támasztanak alá – mondja ki a Basel Committee of Banking Supervision anyaga.

2.1. A megbízás átvétele

A minőségbiztosító a tevékenységét a megbízólevél átvétele után kezdheti meg. A megbízólevélben szabályozni kell a megbízás

- célját,
- vizsgálati kereteit (megfelelőségi elvárások),
- határidejét,
- címzettjét.

A megbízólevél keletkezhet papír alapon és elektronikus formában is, mindkét esetben a megbízónak (legfelső szintű szükséges mértékű kompetenciával rendelkező vezetőjének) hiteles aláírásával kell ellátnia azt.

2.2. A minőségbiztosítás előkészítése

A minőségbiztosítási tevékenység előkészítése két lépést foglal magában:

- a tevékenység megtervezése,
- a tevékenység kockázatainak feltárása és értékelése.

2.2.1. Tervezés

A tervezés során a minőségbiztosítónak Minőségbiztosítási Tervet kell készítenie, melyben ki kell térnie az alábbiak részletes leírására:

- minőségbiztosítás tárgya,
- minőségbiztosítás értelmezése,
- minőségellenőrzési listák felsorolása,
- audit minőségi követelmények,
- megvizsgálni kívánt dokumentumok, evidenciák listája,
- interjú-terv,
- szemle-terv,
- megbízólevél.

A tervet a megbízóval jóvá kell hagyatni, valamint az auditorral is ismertetni javasolt.

2.2.2. Kockázatok elemzése

A minőségbiztosítónak kockázat-elemzésen alapuló intézkedéseket kell tennie az alábbi kockázatok csökkentése érdekében:

1. auditálási tevékenységek kockázatai,
2. minőségbiztosítási tevékenységek kockázatai.

Mindkét területen fel kell mérnie a releváns kockázatokat, értékelnie kell azt kvantitatív vagy kvalitatív módon, majd intézkedéseket kell megfogalmaznia azok csökkentése érdekében.

Itt fel kell hívnunk arra a figyelmet, hogy az auditor tevékenységeinek bizonyos kockázatait maga a minőségbiztosítási tevénység végzése is csökkenti, de ennek kimondása nem elegendő, szükséges a minőségbiztosítónak azokat a fókusz-pontokat is meghatároznia, melyek figyelembe vételével az adott auditálás kockázatait, mint minőségbiztosító, csökkenteni tudja.

A kockázatok bekövetkezésére és a bekövetkezés mértékének elemzésére a minőségbiztosítási záradékban ki kell térnie a minőségbiztosítónak.

2.3. Helyzetfeltárás

A helyzetfeltárás során a minőségbiztosító a tervben kijelölt evidenciákat begyűjti, dokumentálja és értékeli addig, amíg a szükséges evidencia-halmaz nem áll a rendelkezésre.

2.3.1. Evidenciák gyűjtése, dokumentálása

A minőségbiztosítónak elegendő, megbízható, érdemi és hasznos evidenciát kell feltárniuk és rögzíteniük a megbízás célkitűzéseinek megvalósításához. Az elégséges információnak olyan tényszerűnek, megfelelőnek és meggyőzőnek kell lennie, hogy az alapján egy szakmailag jól tájékozott szakember ugyanazokat a következtetéseket vonja le, mint a minőségbiztosító. Megbízható információnak nevezzük a rögzített vizsgálati módszerekkel elérhető legpontosabb információt. Az érdemi információ alátámasztja a vizsgálat megállapításait és intézkedési javaslatait, és összhangban van a vizsgálat célkitűzéseivel. A hasznos informácó segíti a szervezetet céljainak elérésében.

Jól alkalmazható itt is a célkitűzések-evidenciák párba állítása, és ellenőrzési listába szervezése annak a kérdésnek a megválaszolására, hogy létezik-e minden kérdéshez evidencia, valamint elegendő evidenciát tárt-e fel a minőségbiztosító.

Az evidenciák rögzítését olyan módon kell megtenni, mely minden későbbi jogosulatlan módosítást kizár vagy észlelhetővé tesz. Az előre meghatározott archiválási időtartamtól függően a minőségbiztosítónak az evidenciák olvashatóságának hosszú távú fenntarthatóságáról is javasolt gondoskodnia.

2.3.2. Evidenciák értékelése

A begyűjtött evidenciákat a minőségbiztosítónak értékelnie kell az alábbi dimenzók mentén, jól definiált skálák használatával:

1. elegendő (igen-nem vagy 0, 1, 2, 3, 4, 5)
2. megbízható (igen-nem vagy 0, 1, 2, 3, 4, 5)
3. érdemi (igen-nem vagy 0, 1, 2, 3, 4, 5)

4. hasznos (igen-nem vagy 0, 1, 2, 3, 4, 5)

A fókuszpontok és az evidenciák összerendelésével a minőségbiztosító meggyőződhet arról, hogy vajon minden vizsgálati területhez lett-e begyűjtve evidencia, és azok minősége megfelelő-e. Amennyiben az értékelés során nem megfelelő egy evidencia értékelése, haladéktalanul kiegészítő evidenciákat kell a minőségbiztosítónak beszereznie. Ezt követően az értékelést újra el kell végeznie, mindaddig, amíg a szükséges evidencia-halmazt össze nem gyűjtötte a minőségbiztosító.

3. Minőségbiztosítási Riport / Záradék készítése

A megfelelő evidenciák rendelkezésre állását követően a minőségbiztosító megteszi megállapításait. A megállapítások mindegyikéhez evidenciákkal kell rendelkeznie. A megállapítások strukturált felépítést kell követniük, amit a Minőségbiztosítási Tervnek már tartalmaznia kell. A Tervben foglaltaktól a helyzet megismerése után el lehet térni, de csak a szükséges mértékig.

A Minőségbiztosítási Riportnak mindenképpen ki kell térnie az alábbiakra:

1. Az auditor által végzett ellenőrzés, vizsgálat szabályozottsága
2. Az auditor kellő szakmai gondossága
3. Az auditor kockázatbecslése
4. Vizsgálati bizonyítás
5. A vizsgálati anyag és módszer
6. Az audit jelentés tartalma és formája
7. Az auditor megállapításainak értékelése
8. Az auditor javaslatainak értékelése
9. Az auditori megbízás teljesítésének értékelése
10. Az audit minőségének összefoglaló értékelése

A Minőségbiztosítási Jelentést a Minőségbiztosító a Megbízóval és az Auditorral is véleményezteti, véleményeiket elfogadás után átvezeti a Jelentésen és véglegesíti azt. A Minőségbiztosítási Jelentés véglegesítését olyan módon kell megtennie, hogy minden későbbi jogosulatlan módosítás felismerhető legyen a Jelentésen. Lehetséges, hogy a Minőségbiztosító egy egyoldalas összefoglaló záradékot is készít a Minőségbiztosítási Jelentésről, amit az Auditor és a Megbízó is nyilvánosságra hozhat a saját honlapjukon, ily módon is növelve az audit és a minőségbiztosításba vetett bizalmat.

4. Mellékletek

4.1. Megbízólevél tervezet az informatikai audit minőségbiztosítója számára

A *Megbízó* megbízza a *Minőségbiztosítót (*száma: 1234567), hogy az *Auditor* által az alábbi azonosítókkal készített *Audit Jelentést* különösen a következő ISACA szabványoknak való megfelelőség tekintetében minőségbiztosítsa:

Magyar nyelvű szabványok esetében használható:

- Ellenőrzési alapszabályzat 010.010.010.
- A jelentés tartalma és formája 070.010.010.

- A vizsgálat bizonyítási követelménye 060.020.030.
- Kellő szakmai gondosság 030.020.020.
- Kockázatbecslés alkalmazása az ellenőrzés tervezésben 050.010.030.
- Vizsgálati anyag 060.020.010.
- Vizsgálati mintavétel 060.020.040.

Angol nyelvű szabványok esetében használható:

- Ellenőrzési alapszabályzat S1 Audit Charter
- A jelentés tartalma és formája S7 Reporting
- Tervezés S5 Planning
- A vizsgálat bizonyítási követelménye S6 Performance of Audit Work
- Kellő szakmai gondosság G7 Due Professional Care
- Kockázatbecslés alkalmazása a tervezésben S11 Use of Risk Assessment in Audit Planning
- Vizsgálati anyag S14 Audit Evidence
- Vizsgálati mintavétel G10 Audit Sampling

A minőségbiztosítandó anyag megnevezése:

Audit Riport a Megbízó részére, készítette: Auditor, Dátum: xxxx.xx.xx, Verzió: zz.yy (OID: 1.2.3.4.5.6.7.8.9.10.11.12)

Megbízó kijelenti, hogy a *Minőségbiztosító* díjazása nem függ a megállapításaitól.

Kérjük, hogy megállapításait különálló minőségbiztosítási záradékban rögzítse, és a megfelelő személyek (*itt felsorolva)* számára juttassa el *év.hó.nap.óra.perc-ig.*

Helység, Dátum

……

Megbízó