

G42 Continuous Assurance

G42 neprekinjeno izvajanje nadzora

Standardi

- S5 Planning (Načrtovanje)
- S6 Performance of Audit Work (Izvedba revizije)
- S7 Reporting (Poročanje)
- S14 Audit evidence (revizijski dokazi)

Smernice

- G2 audit evidence (revizijski dokazi)
- G3 USE of CAATS (uporaba RPT)
- G10 – Audit Sampling (revizijsko vzorčenje)

- **Primarni cilji: učinkovitost, uspešnost, zaupnost, celovitost**
 - AI1 - Identify automated solutions (Določite avtomatizirane rešitve)
 - ME2 - Monitor and evaluate internal controls (Spremljate in vrednotite kontrole IT)
 - DS5 - Ensure system security
- **Sekundarni cilji: razpoložljivost, skladnost, zanesljivost**

- **Continuous assurance, auditing and monitoring –**
 - **CAATS and continuous assurance (redno poročanje IT revizorjem in IT strokovnjakom glede kritičnih dogodkov in alarmov)**
 - **Neprekinjeno revidiranje (stalno identifikacijo tveganj na osnovi selektivnih preddefiniranih indikatorjev)**
 - **Neprekinjeno spremljanje (učinkovito zbiranje informacij za potrebe odločanja)**

- Identificirati področja koristnosti pristopa
- Uporaba predhodnih izkušenj
- Definirati cilje izvajanja
- Preveriti / zagotoviti obstoj podatkov za uporabo v “procesu neprekinjenega revidiranja”

Uvedba neprekinjenega revidiranja

- Buy IN s strani vodstev
- Buy IN s strani revizorjev in revidirancev
- Izbor orodja
- Oceniti celovitost podatkov
- Priprava poročil
- Zagotoviti ustrezno razumevanje poročil in sistema (revizorji, vodstva)

Uvedba neprekinjenega revidiranja

- Developing Continuous Auditing Routine (Follow SDLC!)
- Scoupe of Continuous Testing (testiranje kontrol v skladu z ocenjeno stopnjo tveganja z namenom zagotovitve, da so kritične odstopanja v delovanju identificirana in je dosežena zelena stopnja zanesljivosti)

Uvedba neprekinjenega revidiranja

- Definiranje urnikov preizkušanja – opredelitev izvedb avtomatiziranih procesov
- Definiranje vsebine in obsega preverjanja podatkov (ne zgolj upoštevati zahteve regulatorjev, ampak tudi oceno tveganja in posledic delovanja groženj, ter stopnje zanašanja vodstev na avtomatizirana poročila)

Uvedba neprekinjenega revidiranja

- Obravnava podatkov en integritete in varnostnih vprašanj (preverjanje celovitosti razpoložljivih podatkov, preverjanje varnostne občutljivosti podatkov glede vpliva na zasebnost in zaupnost, ter zagotavljanje nivoja varovanja skladno s tem)
- Ponovitev ocene ustreznosti rutin ob vseh spremembah – tudi tistih, ki zadevajo vire

Nadzor neprekinjenega revidiranja / spremljanja

- Ugotavljanje učinkovitosti in uspešnosti – tudi glede na tradicionalne postopke revizije vključno s potrebo informiranja vodstev
- Določitev vloge vodstva – identifikacija odstopanj, ovrednotenje, priprava korektivnih ukrepov
- Dodatni ukrepi: postopki dodatnih preverjanj zlasti v primeru kršitev varnosti, prevar, goljufij ,

Uvedba neprekinjenega revidiranja

- **Odgovornost vodstva**
 - odločanje katere kontrole so predmet neprestanega nadzora,
 - opredelitev indikatorjev povečanega tveganja,
 - priprava preddefiniranih scenarijev ukrepanja,
 - Obravnava odstopanj

- **Odgovornost IT revizorjev**
 - Preveritev / testiranje ustreznosti sistema v vseh fazah SDLC rešitve,
 - Pregled ustreznosti vodstvenih poročil, alarmov in drugih sporočil ob odstopanjih
 - Obravnava poročil z vodstvu in preddefiniranih in naknadno sprejetih ukrepov

- Preverjanje izhodov glede smiselnosti
- Tolmačenje / razumevanje rezultatov (False Positive / False Negative)
- Določanje in usposabljanje izvajalcev
- Optimiranje rutin
- Dokumentiranje sistema, hramba dokazil,

- kdaj se konča obdobje “Field work” za revizorjevo poročanje? Kako zagotoviti koristnost periodičnega poročila za vodstvo
- Revizor se mora v večji meri zanašati na poročanje revidiranca pri pripravi svojega poročila (? Stopnje zanesljivosti in celovitosti virov)
- Revizor mora v poročilu podati jasen opis sistema neprekinjenega nadzora, ki mu je vir

Veljavnost 1. Maj 2010

VPRAŠANJA