A független ITB műszaki ellenőr

A **Digitális Megújulás Operatív Program Plusz** (a továbbiakban: DIMOP Plusz) keretében *elektronikus információs rendszer* (a továbbiakban: EIR) kialakítására, bővítésére vagy átalakítására irányuló projekt megvalósítása során a projektgazda köteles az EIR biztonságára vonatkozó jogszabályi követelményeknek való megfelelést biztosítani és ennek érdekében *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény* (továbbiakban: Ibtv.), valamint *az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet* (továbbiakban: Kr.) 8. § szerint a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel (a továbbiakban: információbiztonsági hatóság) együttműködni.

A DIMOP Plusz projektek végrehajtása során **független,** megfelelő képzettséggel, képességekkel és tapasztalattal rendelkező *ITB műszaki ellenőrt* kell alkalmazni a biztonsági szempontok érvényre juttatása érdekében. Az *ITB műszaki ellenőrre* vonatkozó fontos elvárás, hogy olyan szerződéses jogviszonyban álljon, amiből a projekt időtartama alatt a személyes felelőssége egyértelműen megállapítható. A további elvárások részleteit, az *ITB műszaki ellenőr* pontos feladatait és a projekt során felmerülő kötelezettségeit az alábbi táblázatok és folyamatábra foglalja össze.

|  |  |
| --- | --- |
| **Elvárások** | **Igazolás módja** |
| Szakmai elvárások | |
| Szakirányú végzettség vagy szakmai szakirányú képzettség (CISA, CISM, CISSP, ISO 27001 LA, elektronikus információbiztonsági vezető, információbiztonsági szakmérnök/szakember, kiberbiztonsági szakmérnök/szakember, okleveles kiberbiztonsági szakértő) | Igazoló okirat benyújtása |
| Igazolt információbiztonsági auditori tapasztalat | Akkreditált tanúsító szervezet által kiadott igazolás |
| Igazolt információ és informatikai biztonsági tanácsadói tapasztalat | Tanácsadó szervezet által kiadott igazolás |
| Információbiztonsághoz kapcsolódó szabványok, ajánlások, jogszabályok ismerete (pl.: ISO 27001, NIST 800-53, 41/2015. BM. rendelet) | Információbiztonsághoz kapcsolódó szabványok, ajánlások, jogszabályok felsorolása, hozzájuk kapcsolódó projektek, referenciaszervezetek és személyek felsorolása |
| Általános elvárások | |
| Legalább 3 éves szakirányú tapasztalattal rendelkezik az elmúlt 5 évből | Kapcsolódó projektek, referenciaszervezetek és személyek valamint kapcsolódó időszakok felsorolása |
| Szoft skillek | |
| Projekmenedzsment képességek | - |
| Alkalmasság komplex feladatok tervezésére, követésére | - |
| Jó kommunikációs készség | - |
| Döntési képesség | - |
| Projekttel kapcsolatos magas szintű felelősségvállalási képesség | - |

# A projektek életciklusának rövid áttekintése

Előzetes kockázatértékelés

Rendszerbiztonsági terv

Előzetes besorolás

Biztonság tervezés

Megvalósítás

Rendszerbiztonsági dokumentum (aktualizált terv)

Megvalósíthatósági tanulmány

Lezárás

Információbbiztonsági terv

III. Megvalósítási

fázis

IV. Lezárási

fázis

Előzetes információbiztonsági kockázatok, biztonsági követelmények

Előzetes biztonsági osztályba sorolás

biztonsági követelmények

I. Tervezési fázis -

biztonsági koncepció

II. Tervezési fázis –

funkcionális

biztonságtervezés

# Az ITB műszaki ellenőr feladatai

| **Támogatói feladatok** | **Ellenőrzési feladatok** | **Jelentési feladatok** |
| --- | --- | --- |
| **I. Tervezési fázis – biztonsági koncepció** | | |
| Konzultáció a biztonságtervezés kereteinek meghatározásával kapcsolatban (módszerek, feladatok, ütemezés, felelősségek) |  | Az egyes fázisok eredménytermékeihez tartozó szakvéleményeknek az információbiztonsági hatóság részere történő megküldése, tájékoztatás, illetve véleményezés céljából. |
|  | előzetes kockázatértékelési és előzetes biztonsági osztályba sorolási tevékenység ellenőrzése (folyamat ellenőrzés) |  |
|  | előzetes kockázatértékelés és előzetes biztonsági osztályba sorolás eredménytermékének szakmai validálása (eredménytermék ellenőrzés) | előzetes kockázatértékelés és előzetes biztonsági osztályba sorolás szakvélemény |
|  | információbiztonsági terv készítésének ellenőrzése (folyamat ellenőrzés) |  |
|  | információbiztonsági terv eredménytermékének szakmai validálása (eredménytermék ellenőrzés) | információbiztonsági terv szakvélemény |
| **II. Tervezési fázis – funkcionális biztonságtervezés** | | |
|  | rendszerbiztonsági terv készítésének ellenőrzése (folyamat ellenőrzés) |  |
|  | rendszerbiztonsági terv eredménytermékének szakmai validálása (eredménytermék ellenőrzés) | rendszerbiztonsági terv - szakvélemény |
|  | GovProbe (honeypot) rendszerhez való kapcsolódás szintjének vizsgálatának (kedvezményezett végzi a vizsgálatot) ellenőrzése | GovProbe (honeypot) rendszerhez való kapcsolódás szintjének vizsgálata - szakvélemény |
|  | Reaktív, IDS típusú eseménydetekciós céllal létrehozott korai megelőző rendszerhez (EWS) való csatlakozás vizsgálatának (kedvezményezett végzi a vizsgálatot) ellenőrzése | Reaktív, IDS típusú eseménydetekciós céllal létrehozott korai megelőző rendszerhez (EWS) való csatlakozás vizsgálatána - szakvélemény |
| A szakvélemények eklészítése során észrevételi és javaslattételi lehetőséggel élhet |  | Észrevételi, javaslattételi jelentés |
| **III. Megvalósítási fázis** | | |
|  | az információbiztonsági tervben valamint a rendszerbiztonsági tervben meghatározott biztonsági követelmények megfelelő megvalósulásának ellenőrzése (folyamat és eredménytermék ellenőrzés)   * részvétel az érintett szakmai egyeztetéseken * információ kérése, feldolgozása * a biztonsági követelmények megvalósításának ellenőrzése során tapasztalt eltérések megfogalmazása, kockázatainak bemutatása és prezentálása a projekt vezető felé * szükség esetén eszkaláció a projekt irányító bizottság valamint a projekt szponzorok felé. (A kedvezményezett és a műszaki ellenőr közötti egyet nem értés esetén az infromációbiztonsági hatóság bevonása) * időszaki riportok készítése a biztonsági követelmények megvalósulásának előrehaladásáról, esetleges problémáiról | Negyedéves valamint mérföldkövekhez kapcsolódó jelentés elkészítése és az információbiztonsági hatóság részére – tájékoztatás céljából – történő megküldése az információbiztonsági tervben valamint a rendszerbiztonsági tervben meghatározott biztonsági követelmények megvalósulásáról  A biztonsági követelmények megvalósulásának előrehaladásáról, esetleges problémáiról készülő riportok továbbítása az információbiztonsági hatóság felé tájékoztatásra. |
|  | A megvalósítás során, a tervektől történő eltérések átvezetésének (Rendszerbiztonsági terv -> Rendszerbiztonsági dokumentum) ellenőrzése (folyamat és eredménytermék ellenőrzés) | Rendszerbiztonsági dokumentum - szakvélemény |
|  | sérülékenység vizsgálati tevékenység tervének ellenőrzése | sérülékenység vizsgálati terv – szakvélemény |
| Az információbiztonsági tervben valamint a rendszerbiztonsági tervben meghatározott biztonsági követelmények megfelelő megvalósulásának ellenőrzése során észrevételi és javaslattételi lehetőséggel élhet |  | Észrevételi, javaslattételi jelentés |
| **IV. Lezárási fázis** | | |
|  | CTI (Cyber Threat Intelligence) platformhoz való kapcsolódási dokumentum biztonsági fókuszú ellenőrzése | CTI (Cyber Threat Intelligence) platformhoz való kapcsolódási dokumentum - szakvélemény |
|  | Az információbiztonsági tervben valamint a rendszerbiztonsági tervben meghatározott biztonsági követelmények végső megvalósulásának ellenőrzése | javaslattétel a biztonsági követelmények megvalósulásának belső elfogadására |