A független ITB műszaki ellenőr

# Az 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.

Az ITB műszaki ellenőr feladatkör létrehozásának célja a Kedvezményezett és a Hatóság között egy olyan független szakmai (ellenőri) entitás közreműködésének megteremtése, amely felel a projektek megvalósítása során vállalt és a jogszabályok szerint elvárt biztonsági szempontok érvényre juttatásáért. Feladatai közé tartozik továbbá, hogy naprakész információt tudjon szolgáltatni az EIR fejlesztések vonatkozásában.

Az ITB műszaki ellenőri feladatokat gazdasági társaság abban az esetben láthatja el, ha rendelkezik olyan szakemberrel, aki a szakmai elvárásoknak mindenben megfelel. A feladatokat kizárólag az elvárásoknak igazoltan megfelelő szakember végezheti.

Amennyiben az ITB műszaki ellenőri szolgáltatás beszerzési/közbeszerzési eljárás keretében kerül beszerzésre, úgy műszaki és szakmai alkalmassági minimumkövetelményként szükséges előírni legalább egy, valamennyi szakmai elvárásnak (képzettség, végzettség, szakmai tapasztalat) megfelelő szakember meglétét azzal, hogy az ITB műszaki ellenőri feladatokat kizárólag az alkalmassági követelmények teljesítése igazolására bemutatott szakember végezheti el.

**Az ITB műszaki ellenőr vonatkozásában a projektek közti átfedés megengedett,** vagyis egy ellenőr több projektben is betöltheti a jelen dokumentumban meghatározott feladatait.

Ebben az esetben valamennyi ellenőrnek meg kell felelnie a DIMOP Plusz releváns felhívásainak „*7.4 Milyen feltételei vannak az elszámolhatóságnak?”* című fejezet *„Összeférhetetlenségi szabályok”* alfejezéteben meghatározott függetlenségre vonatkozó kritériumoknak.

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** |
| **Végzettséggel kapcsolatos szakmai elvárások** | |
| Felsőfokú szakirányú és szakirányú végzettségek az alábbiak szerint:   * Certified Information System Auditor (CISA), vagy * Certified Information Security Manager (CISM), vagy * Certified in Risk and Information Systems Control (CRISC), vagy * International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP), vagy * ISO/IEC 27001 Lead Auditor, vagy * Elektronikus információbiztonsági vezető, vagy * Információbiztonsági szakmérnök/szakember, vagy * Kiberbiztonsági szakmérnök/szakember. | Igazoló okirat benyújtása |
| **Tapasztalattal kapcsolatos szakmai elvárások[[1]](#footnote-1)** | |
| * Igazolt - legalább 3 éves - információbiztonsági auditori tapasztalat, és/vagy * Igazolt - legalább 3 éves - információ és/vagy informatikai biztonsági tanácsadói tapasztalat | A szakmai gyakorlat időtartama a szakmai önéletrajz saját kezűleg aláírt példányának egyszerű másolatban történő benyújtásával igazolandó. A szakmai önéletrajzban fel kell tüntetni az ellátott feladat tartalmát olyan részletességgel, hogy abból az alkalmassági minimumkövetelménynek megfelelő tapasztalat megállapítható legyen, ezen belül meg kell jelölni a szervezete(ke)t, aki(k) részére a szakmai tapasztalat körében bemutatott feladatok elvégzésre kerültek, valamint az elvégzett tevékenység kezdő és befejező időpontját ÉV/HÓNAP részletességgel. |

|  |  |
| --- | --- |
| **Nem kötelező elvárások:** | |
| * Európai Uniós projektek lebonyolításában szerezett tapasztalat, | * Kapcsolódó projektek, valamint a kapcsolódó időszakok felsorolása |
| * 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 |
| * Az ITB ellenőr 3 éves szakirányú tapasztalata az elmúlt 5 évből származik. | * Kapcsolódó projektek, referenciaszervezetek és személyek, valamint kapcsolódó időszakok felsorolása |

# Az ITB műszaki ellenőr feladatai[[2]](#footnote-2)

| **Támogatói feladatok** | **Ellenőrzési feladatok** | **Jelentési feladatok** |
| --- | --- | --- |
| **I. Tervezési fázis – biztonsági koncepció** | | |
| Szakmai támogatás és  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 szakvélemény |
| Előzetes kockázatértékelés és előzetes biztonsági osztályba sorolás eredménytermékének szakmai validálása (eredménytermék ellenőrzés) |
| Információbiztonsági terv készítésének ellenőrzése (folyamat ellenőrzés) | Információbiztonsági terv szakvélemény |
| információbiztonsági terv eredménytermékének szakmai validálása (eredménytermék ellenőrzés) |

| **Támogatói feladatok** | **Ellenőrzési feladatok** | **Jelentési feladatok** |
| --- | --- | --- |
| **II. Tervezési fázis – funkcionális biztonságtervezés** | | |
| Szakmai támogatás és  konzultáció a biztonságtervezés kereteinek meghatározásával kapcsolatban (módszerek, feladatok, ütemezés, felelősségek) | Rendszerbiztonsági terv készítésének ellenőrzése (folyamat ellenőrzés) |  |
| Rendszerbiztonsági terv eredménytermékének szakmai validálása (eredménytermék ellenőrzés) | rendszerbiztonsági terv - szakvélemény |
| A GovProbe (honeypot) rendszerhez való kapcsolódás szintjének vizsgálata Kedvezményezett, vagy az általa beszerzett gazdasági társaság által lefolytatott vizsgálat (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 |
| Az incidenskezelési platformhoz való csatlakozás vizsgálatának (kedvezményezett végzi a vizsgálatot) ellenőrzése. |  |
| A CTI - Tudásmegosztó platformhoz való csatlakozás vizsgálatának (kedvezményezett végzi a vizsgálatot) ellenőrzése. |  |
| A szakvélemények eklészítése során észrevételi és javaslattételi lehetőséggel élhet |  | Észrevételi, javaslattételi jelentés |

| **Támogatói feladatok** | **Ellenőrzési feladatok** | **Jelentési feladatok** |
| --- | --- | --- |
| **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 |

# A projektek életciklusának rövid áttekintése

Előzetes kockázatértékelés

Rendszerbiztonsági terv

Előzetes besorolás

Biztonság tervezés

Megvalósítás

Rendszerbiztonsági dokumentum (aktualizált terv)

Megvalósíthatósági tanulmány

Lezárás

Információbiztonsági 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

1. Az alábbi elérhetőségeken lehet olyan gazdasági társaságokat találni, amelyek a kiberbiztonsági és információbiztonsági vonatkozású kérdések tekintetében megfelelő szakmai segítséget tudnak nyújtani:

   <https://nah.gov.hu/hu/kategoriak/ibir-tanusitas--isms-certification/>

   <https://sztfh.hu/nyilvantartasok/auditorok/>

   <https://sztfh.hu/nyilvantartasok/megfelelosegertekelo-szervezetek/>

   <https://www.mnb.hu/letoltes/tanusito-szervezetek-jegyzeke.pdf>

   <https://nah.gov.hu/hu/kategoriak/vizsgalolaboratorium--testing/>

   **Nevezett listák nem teljeskörűek, valamint nem minden, az adott listán található cég a releváns. Kizárólag az információbiztonsághoz, kiberbiztonsághoz kapcsolódó találatok a relevánsak.** [↑](#footnote-ref-1)
2. **Az ITB műszaki ellenőrhöz tartozó feladatok tekintetében nem elvárás az egyes fázisokhoz tartozó eredménytermékek elkészítése, azonban nem kizáró tényező, hogy Kedvezményezett az ITB műszaki ellenőrnek delegálja azokat.** [↑](#footnote-ref-2)