Elvárások a NIS2 felkészítőkkel szemben, egy felkészítő megbízásának részletei

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/31

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.07.30	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1 VEZETŐI ÖSSZEFOGLALÓ

Jelen dokumentum azt határozza meg, hogy a kiberbiztonsági auditfelkészítéshez külső felkészítőt igénybe vevő szervezetnek milyen szakmai, szerződéses, módszertani, információbiztonsági és teljesítési követelményeket indokolt előírnia. Az állásfoglalás olyan megbízási modellt tekint megfelelőnek, amely egyértelműen és ellenőrizhető módon rögzíti a felkészítő feladatait, a szervezet közreműködési kötelezettségeit, az átadandó eredményeket, valamint azok mérhető és auditálható elfogadási kritériumait.

Az állásfoglalásban szereplő, jogszabályból közvetlenül következő előírások kötelezőek. A további elemek az állásfoglalás szakmai álláspontja szerint javasolt minimumelvárások, amelyek a megbízás egyértelmű, ellenőrizhető és auditálható kialakítását szolgálják. Az állásfoglalás nem minősül jogi tanácsadásnak vagy hatósági döntésnek.

A legfontosabb alapelvek:

- A felkészítő bevonása nem ruházza át a szervezet vezetőjének, az EIR biztonságáért felelős személynek, a kontrollgazdáknak vagy más kijelölt szerepköröknek a jogszabályi és szervezeti felelősségét.
- A megbízásnak pontosan meg kell határoznia az érintett szervezeti egységeket, EIR-eket, telephelyeket, folyamatokat, szolgáltatókat, vizsgált követelményeket és kizárásokat.
- A felkészítőnek a dokumentumok szerkesztése előtt meg kell ismernie a szervezet működését. A szervezetmegismerés történhet komplex adatbekérővel, interjúkkal, dokumentum- és bizonyítékvizsgálattal, gap elemzéssel, helyszíni felméréssel, valamint üzleti hatáselemzés felhasználásával.
- A felkészítés nem kizárólag szabályzatkészítés, ki kell terjednie a kontrollok tényleges működésére, a hiányosságokra, a javítóintézkedésekre és az auditbizonyítékok előállíthatóságára és az auditori adatbekérő kitöltésére is.
- A teljesítés csak előre rögzített, dokumentumonként és feladatonként meghatározott elfogadási kritériumok alapján igazolható.

2 HATÓKÖR ÉS ALAPFOGALMAK

2.1 A felkészítő szerepe

Felkészítő alatt az a külső szakértő, tanácsadó vagy szolgáltató értendő, aki a szervezetet a kiberbiztonsági követelmények felmérésében, értelmezésében, a hiányosságok azonosításában, a szükséges kontrollok és dokumentáció kialakításában, valamint az auditálhatóság megteremtésében támogatja. A „felkészítő” nem önálló jogszabályi jogállás; a tényleges feladataitól függően a Kiberbiztonsági tv. szerinti közreműködőként kezelendő lehet.

A felkészítő nem dönthet a szervezet helyett a kockázatok elfogadásáról, a szabályzatok jóváhagyásáról, a kontrollok működtetéséről vagy a megfelelőségi státusz végleges

megállapításáról. A felkészítő megállapításokat, ajánlásokat és dokumentumtervezeteket készít; a szervezeti döntés és végrehajtás a kijelölt helyi szerepköröknél marad.

2.2 Jogi és auditálhatósági alapelv

„(5) A szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében

d) ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek;”

[2024. évi LXIX. törvény 6. § (5) bekezdés d) pont]

A Kiberbiztonsági tv. alapján a közreműködő bevonásakor a szükséges kiberbiztonsági követelményeket szerződéses kötelemként kell érvényesíteni.

„(3) Az auditor jogosult a kiberbiztonsági audit során minden, a szervezet és elektronikus információs rendszerei biztonságával kapcsolatba hozható dokumentum megismerésére.”

[1/2025. (I. 31.) SZTFH rendelet 5. § (3) bekezdés]

A kiberbiztonsági audit során az auditor jogosult a szervezet és EIR-jei biztonságával kapcsolatba hozható dokumentumok megismerésére. Emiatt a felkészítő megbízását, módszertanát, eredményeit és a szervezet által elfogadott dokumentumokat olyan módon kell kezelni, hogy azok utólag is visszakövethetők és bemutathatók legyenek.

3 A SZERVEZET ÁLTAL ELŐZETESEN MEGHATÁROZANDÓ ELVÁRÁSOK

3.1 A megbízás célja és hatóköre

Az „auditfelkészítés” vagy „szabályzatok elkészítése” önmagában nem megfelelő teljesítési leírás. Az eredményeket tételesen, formátummal, határidővel és elfogadási feltétellel kell meghatározni. A szervezetnek a beszerzés vagy megbízás előtt írásban és ellenőrizhető módon meg kell határoznia:

- a felkészítés célját, valamint az alkalmazandó jogszabályi, szabályozási, szabványi és belső követelményeket;
- az érintett jogi személyeket, szervezeti egységeket, telephelyeket, üzleti folyamatokat, EIR-eket, rendszerelemeket és szolgáltatói függőségeket;
- az EIR-ek biztonsági osztályát és a megbízás részleteit, így különösen:

- szabályozások és más szabályozó esetleg sablon dokumentumok készítése;
- kockázatelemzés készítése;
- oktatások tartása, oktatási anyagok készítése;
- rendszer dokumentáció - készítés (kiemelten rendszerbiztonsági terv);
- rendszer konfigurációs ellenőrzés vagy technikai teszt alkalmazását;
- Az Eltérések és helyettesítő védelmi intézkedések nyilvántartása az I/2025 (I.31.) SZTFH rendelet 4-es mellékletének kitöltésével;
- audit kérdőívek kitöltését, segítségnyújtást bizonyítékgyűjtésben, illetve audit támogatást;

- az átadandó eredmények formai (például szervezet által biztosított sablon használata) és tartalmi elfogadási kritériumait, továbbá a véleményezés és jóváhagyás rendjét;
- a hatókörből kizárt területeket, a kizárások és feltételezések indokát, valamint ezek kockázati hatását;
- a projekt mérföldköveit, az audit vagy más külső határidőt továbbá a hatókör módosításának és a többletfeladatok elszámolásának rendjét.

Javasolt, hogy a megbízásban a szervezet kifejezetten térjen ki arra, amennyiben valamely szabályozást vagy dokumentumot NEM a felkészítő fogja elkészíteni. Természetesen a szervezetnek minden eredménytermék elkészítése során részt kell vennie a folyamatban.

3.2 Szakmai alkalmasság és függetlenség

A felkészítő kiválasztásakor a szakmai követelményeket a megbízás összetettségéhez, az érintett EIR-ekhez és a felmérés tervezett mélységéhez kell igazítani. Elvárható alkalmassági követelmények:

- igazolható kiberbiztonsági tapasztalat; NIS2-szabályozási ismeret, speciális esetben az érintett iparághoz és technológiákhoz igazodó szakértelem, tanúsítványok;
- bármely auditfelkészítési, kontrollértékelési és dokumentációs tapasztalat;
- a vállalt határidőkhöz megfelelő kapacitás, megnevezett szakértői csapat, és szakmai referenciák vagy tanúsítványok;
- a felkészítő, kapcsolt vállalkozásai, alvállalkozói és szakértői esetleges auditori, vizsgáló laboratóriumi, technológiai beszállítói vagy kontrollüzemeltetői szerepének előzetes feltárása, valamint az összeférhetetlenség dokumentált kezelése.

A tanúsítvány vagy referencia önmagában nem helyettesíti a konkrét feladatot végző szakértők alkalmasságának, kapacitásának és függetlenségének értékelését.

4 PROJEKTIRÁNYÍTÁS, INFORMÁCIÓBIZTONSÁG ÉS FELELŐSSÉG

4.1 Ajánlatadás előtt

Amennyiben egy felkészítő adatbekérő vagy interjú, illetve a feladat részleteinek definiálása előtt ajánlatot tud adni, feltételezhető, hogy árazása nem realitásokon alapul, tehát ár-érték arányban biztosan nem lesz megfelelő.

4.2 Ajánlat

Az ajánlatban várjuk el, hogy a felkészítő nevezze meg az általa elkészített eredménytermékeket, illetve azt is, hogy a 100%-os felkészüléshez a szervezetnek még milyen dokumentumokat kell elkészítenie vagy folyamatokat bevezetnie, nyilvántartásokat kialakítania.

A felkészítő feladata a megbízás szerint legalább az alábbiakra terjedjen ki:

- az érintett szervezet, EIR-ek, rendszerelemek, szolgáltatások és külső függőségek azonosítása;
- az EIR-ek biztonsági osztályának és az alkalmazandó követelményeknek a szakmai áttekintése;
- a helyi, anyavállalati, szolgáltatói és megosztott kontrollok elkülönítése;
- a követelmények összevetése a bemutatott kontrollokkal és auditbizonyítékokkal;
- a nem teljesített, részben teljesített, bizonyítékhiányos és nem vizsgált területek egyértelmű rögzítése, kockázatalapú prioritással.

Így amennyiben az audittámogatást is a felkészítő végzi, egyértelmű lesz hogy teljes hiány esetén kinek a felelőssége lett volna adott feladat elkészítése.

4.3 Projektirányítás és kommunikáció

A megbízás után meg kell határozni a projektvezetőket és döntéshozókat, a státuszok és vezetői riportok rendjét, a feladat- és döntésnyilvántartást, a dokumentumok véleményezési határidejét, az eszkalációt, valamint a mérföldköveket és függőségeket. A projekttervben a felkészítői és a szervezeti feladatokat egyaránt szerepeltetni kell, hiszen minden feladatot el kell végezni egy sikeres audithoz.

4.4 Titoktartás, információbiztonság és adatvédelem

A felkészítő által kezelt információk védelmére legalább az engedélyezett információmegosztási platformokat, az adatok megőrzését és törlését, az incidensértesítés szereplőit kell rögzíteni. E követelményeket az alvállalkozókra is tovább kell hárítani.

4.5 Felelősség és korlátozások

A felkészítő felel a szakmai gondosságért, az általa készített eredmények minőségéért, a hiányosságok és korlátozások egyértelmű jelzéséért, valamint a titoktartási és biztonsági kötelezettségeiért. A szervezet felel az átadott információkért, a vezetői döntésekért, a kontrollok tényleges működtetéséért és a kockázatelfogadásért.

Fontos, hogy a felkészítő nem garantálhat meghatározott audit- vagy hatósági eredményt, hiszen munkájának eredménye nagyban függ a szervezettől kapott információk minőségétől, a definiált folyamatok betartásától.

5 A FELKÉSZÍTŐ FELADATAI

5.1 A szervezet megismerése

A felkészítőnek a követelmények részletes értékelése és a dokumentumok kidolgozása előtt megfelelő mélységben meg kell ismernie a szervezet tényleges működését. A cél annak feltárása, hogy a szervezet milyen tevékenységeket végez, hogyan épül fel a felelősségi rendje, mely EIR-eket és szolgáltatókat veszi igénybe, továbbá milyen kontrollok és bizonyítékok állnak már rendelkezésre.

A megismerés a megbízás jellegéhez igazodó, egymással kombinálható módszerekkel történhet:

- komplex szervezeti és technológiai adatbekérővel;
- vezetői, folyamatgazdai, informatikai és kontrollgazdai interjúkkal;
- dokumentum-, nyilvántartás- és bizonyítékvizsgálattal;
- helyszíni vagy távoli működési felméréssel;
- követelmény- és kontrollalapú hiányosságelemzéssel, továbbá korábbi auditok, incidensek és kockázatelemzések, valamint BIA-, BCP- vagy DRP-dokumentumok felhasználásával.

A felmérés eredményeként a felkészítőnek értenie kell a szervezet folyamatait, EIR-jeit, függőségeit, szerepköreit és meglévő biztonsági működését. Általános sablondokumentumok szervezetmegismerés nélküli előállítása nem tekinthető megfelelő felkészítésnek.

5.2 Dokumentáció, kontrollok és bizonyítékok

Teljes körű auditfelkészítési megbízás esetén a felkészítő feladatának az alábbiakra kell kiterjednie:

- szabályzatok, eljárásrendek, nyilvántartások és sablonok elkészítése vagy felülvizsgálata;
- a kontrollgazdák, felelősök, gyakoriságok, bemenetek, kimenetek és elfogadási kritériumok meghatározásának támogatása;
- a dokumentált előírások és a tényleges technológiai, illetve szervezeti működés összehangolására javaslattétel;
- a kialakítási, működési és eredményességi bizonyítékok kontrollonkénti azonosítása és EIR-hez rendelése (amennyiben az audit bizonyíték gyűjtést támogatja);
- a külső szolgáltatóktól vagy anyavállalattól szükséges bizonyítékok és adatszolgáltatások meghatározása.

A dokumentum elkészülte önmagában nem bizonyítja a kontroll teljesülését. A felkészítőnek külön jeleznie kell, ha a kontroll működése vagy eredményessége még nem igazolt.

Példák: a jogszabályi elvárás szerint amennyiben a szervezetnek valamit meg kell határoznia azt ténylegesen eljárásrendben vagy mellékletében vagy valamely dokumentumában konkrétan meg kell határozni, mint például a naplózandó eseményeket. Ilyen esetben konkrét listát kell írni arról, hogy milyen események naplózását várja el a szervezet.

Folyamatok leírásakor nem javasolt a „szervezet előállítja" és hasonló kifejezésekkel élni, a felelősöket és a felelősségi köröket pontosan meg kell határozni:

- milyen input alapján;
- ki, mikor, milyen gyakran, milyen rendszerességgel;
- milyen formátumban;
- riportálja-e valakinek… stb.

Aranyszabályként lehet azt gondolni, hogy a végső felelős a szervezet legfelsőbb vezetője, ugyanakkor nem minden feladatot ő végez el. Amennyiben valamely feladatért a „szervezet" felelős akkor a feladat teljesülését nincs kitől elvárni, amennyiben valamely részlet nincs definiálva akkor pedig a teljesítést nem lehet bizonyítani.

A dokumentált előírások és a tényleges technológiai, illetve szervezeti működés összehangolására egy felkészítő tehet javaslatot, de a szervezet működésére alapvetően nincsen ráhatása. Olyan esetekben fontos erre odafigyelni mikor a szervezeti folyamaton módosításokat kell eszközölni annak érdekében, hogy a szabályozásokat a jogszabálynak megfelelően lehessen kialakítani. (Például dokumentált jogosultságigénylések bevezetése)

A külső szolgáltatóktól vagy anyavállalattól szükséges bizonyítékok és adatszolgáltatások meghatározása tekintetében ismét egy felkészítő adhat listát és készíthet követelményeket, de sokszor a szervezetnek kell ezeket egyeztetnie beszállítóival, alvállalkozóival, illetve az anyavállalattal (ahol ez releváns).

5.3 Kockázatelemzés, javítóintézkedések és záró értékelés

A feltárt hiányosságokhoz legalább az érintett követelményt és EIR-t, a megállapítást, a kockázatot, a javasolt intézkedést, a szervezeti felelőst, a határidőt és a lezárási kritériumot kell hozzárendelni. Ez olyan esetekben fordulhat elő amikor az audit felkészülésig – vagy egyáltalán – egy rendszer például nem teljesíti a naplózási követelményeket, vagy nem biztosítható az elvárható tárhely a megfelelő mentéseknek, mely problémák közül egyesek középtávon megoldhatók, mások csak felmenő rendszerben rendszer cserével, de fontos, hogy az ilyen nem megfelelőséget a szervezet kockázatként és intézkedési tervében kezelheti.

Ugyanakkor megjegyezzük, hogy a 2025 januárja óta érvényben lévő követelményjegyzék esetében az oktatások hiányát kockázatnak felvenni mert nem volt még rá idő nem javasolt, az auditorok ezeket nem veszik jó néven.

6 A SZERVEZET KÖZREMŰKÖDÉSI KÖTELEZETTSÉGEI

A felkészítés eredményességéhez a szervezetnek legalább az alábbi feltételeket kell biztosítania:

- vezetői szponzor, projektvezető, szakmai kapcsolattartó és helyettes kijelölése;
- az EIR biztonságáért felelős személy, az EIR-tulajdonosok, folyamatgazdák, kontrollgazdák és technikai szakértők bevonása;
- a szükséges információk, dokumentumok, nyilvántartások, bizonyítékok és hozzáférések határidőben történő biztosítása;
- az átadott információk pontosságának, teljességének és aktualitásának ellenőrzése;
- az interjúk, workshopok, felmérések és döntési fórumok megszervezése;
- a dokumentumtervezetek határidőben történő véleményezése és jóváhagyása;
- a javítóintézkedések végrehajtásához szükséges döntések és erőforrások biztosítása;
- a projektet érintő jelentős szervezeti, technológiai vagy szolgáltatói változások bejelentése.

A szervezeti késedelem vagy hiányos adatszolgáltatás projekt- és határidőhatását a megbízásban rendezni, a projekt során pedig dokumentálni kell.

7 MÓDSZERTAN ÉS MUNKAVÉGZÉSI REND

A felkészítési módszertan javasolt fő szakaszai:

1. Projektindítás, cél, hatókör, felelősségek, ütemezés és kommunikációs rend rögzítése.
2. Szervezetmegismerés, adatbekérés, interjúk, dokumentum- és működésvizsgálat.
3. Hatókör- és követelménytérkép, kiinduló állapotfelmérés, az EIR-ek, szolgáltatók és alkalmazandó kontrollok, hiányosságok és korlátozások meghatározása.
4. Megvalósítás támogatása, dokumentáció, nyilvántartások, folyamatok, technikai kontrollok, kialakítása.
5. Zárás, átadás-átvétel és szükség esetén audit alatti támogatás.

8 A MEGBÍZÁS DOKUMENTÁLÁSA ÉS MINIMUMTARTALMA

A megbízás dokumentumainak együttesen, egyértelműen és ellenőrizhetően kell rögzíteniük a felek kötelezettségeit és a teljesítés módját. A részletek kezelhetők szerződésben, szakmai feladatleírásban, projekttervben vagy azok mellékleteiben.

Tárgy	Rögzítendő minimum
Felek és szakértői csapat	A szerződő felek, szakmai vezető, tényleges szakértők, kapcsolattartók, helyettesítés és alvállalkozók.

Tárgy	Rögzítendő minimum
Cél és hatókör	Az érintett szervezeti egységek, EIR-ek, követelmények, szolgáltatók, felmérési mélység, kizárások és feltételezések.
Feladatok és módszertan	A szervezetmegismerés, hatókör-meghatározás, értékelés, dokumentáció, kontrolltámogatás és záró felmérés pontos köre.
Felelősségek és közreműködés	A felkészítő, a szervezet, a vezetés és a kontrollgazdák feladatai, döntési pontjai, adatszolgáltatása és eszkalációja.
Átadandó eredmények	A dokumentumok, mátrixok, jelentések, nyilvántartások és bizonyítékjegyzék tételes felsorolása, formátuma és határideje.
Elfogadási kritériumok	A szervezetre és EIR-re szabott tartalom, pontosság, végrehajthatóság, véleményezési körök, javítási fordulók és elfogadó.
Projektirányítás	Mérföldkövek, függőségek, státuszriportok, döntési határidők, változáskezelés és audit előtti belső lezárás.
Felhasználási jogok	Az átadott dokumentumok, sablonok, mátrixok és egyéb eredmények szervezeten belüli használatának, módosításának, továbbfejlesztésének és audit célú átadásának joga, továbbá a harmadik féltől származó tartalmak korlátozásai.
Információbiztonság és adatvédelem	Engedélyezett eszközök és csatornák, hozzáférés, titkosítás, megőrzés, törlés, incidensértesítés és személyes adatok kezelése.
Díjazás és lezárás	Elszámolási modell, többletfeladatok, teljesítésigazolás, dokumentumátadás, hozzáférésmegszüntetés és audit alatti támogatás.

9 A MEGBÍZÁS LEZÁRÁSA ÉS AUDIT ALATTI TÁMOGATÁS

A lezáráskor legalább az alábbiakat kell rendezni:

- a végleges, szerkeszthető dokumentumok és kapcsolódó sablonok, egyéb elemek átadását;
- a nyitott intézkedések, maradványkockázatok és függő döntések jegyzékét;
- a felkészítő hozzáféréseinek megszüntetését, valamint az adatok visszaadását vagy igazolt törlését;
- az audit alatti támogatás terjedelmét, válaszidejét, kapcsolattartóit és elszámolását.

Az audit alatti támogatás keretében a felkészítő közreműködhet a dokumentumok, bizonyítékok és korábbi megállapítások bemutatásában, azonban a szervezet nevében kizárólag előzetesen jóváhagyott információt közölhet, és nem vállalhatja át a szervezet döntési felelősségét.

10 FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

11 MELLÉKLET

Magas szintű feladatlista Alap biztonsági osztályhoz való felkészüléshez

Információbiztonsági szabályzat (IBSZ), amely a szabályozási környezet alapdokumentuma. Ez a szabályzat fogja tartalmazni a törvény, illetve a kapcsolódó rendelet által előírt, szükséges szabályokat.

Szabályzatok:

A Szervezet igényeinek megfelelően a dokumentumok pontos megnevezése, helye (külön dokumentum, IBSZ melléklet stb.) és mennyisége változhat – de a bennük foglalt tartalmat minden esetben a jogszabály követelményei határozzák meg,

- Hozzáférés-felügyeleti szabályzat;
- Tudatosság és képzés szabályzat;
- Naplózás és elszámoltathatóság szabályzat;
- Értékelés, engedélyezés és monitorozás szabályzat;
- Konfigurációkezelési szabályzat;
- Készenléti tervezés (Üzletmenet-folytonossági) szabályzat;
- Azonosítás és hitelesítési szabályzat;
- Biztonsági események kezelése szabályzat;
- Karbantartási szabályzat;
- Adathordozók védelme szabályzat;
- Fizikai és környezeti védelmi szabályzat;
- Viselkedési szabályok szabályzat;
- Személyi biztonság szabályzat;
- Kockázatkezelési szabályzat;
- Rendszer- és szolgáltatásbeszerzési szabályzat;
- Rendszer- és kommunikációvédelem szabályzat;
- Rendszer- és információsértetlenségi szabályzat.

Kockázatelemzési és kockázatkezelési módszertan kialakítása és az elemzés elvégzése a Szervezetre, illetve az EIR-ekre.

A 2024. LXIX tv. elvárja az információbiztonsági rendszer működtetésének kockázati szemléletű megközelítését és a kockázatelemzés rendszeres elvégzését a Szervezetre és az egyes rendszerekre vonatkozóan.

Üzleti folyamatok biztonságát támogató stratégiák, tervek, egyéb dokumentumok:

- BCP (üzletmenet- folytonossági terv);
- DRP (katasztrófa utáni helyreállítási terv);
- Biztonsági eseménykezelési terv;
- Folyamatos felügyeleti stratégia;

- Kockázatmenedzsment stratégia;
- Rendszerbiztonsági terv(ek);

Egyéb dokumentumok:

- Biztonsági események nyilvántartása;
- Az EIR-eknek helyet adó létesítményekbe belépésre jogosultak listája;
- Fizikai belépést ellenőrző eszközök nyilvántartása;
- Látogatói belépések nyilvántartása;
- Be- és kiszállítások nyilvántartása - informatikai eszközök;
- Karbantartási nyilvántartás;
- Konfiguráció változás nyilvántartása;
- Rendszerelem leltár;
- Licensz nyilvántartás;
- Külső szolgáltatókkal szembeni biztonsági követelmények dokumentuma;
- Mentési rend;
- Alapkonfiguráció dokumentáció;
- Munkaköri leírások kiegészítése NIS2 elvárásoknak megfelelően;
- Biztonsági tesztelések, képzések és felügyeleti tevékenységek szabályozása;

Oktatási anyagok:

- Folyamatos működésre felkészítő képzés;
- Biztonsági eseménykezelési képzés;
- Képzés rendszerelem hamisítások felismerésére;
- Nyilvánosan elérhető információk kezelésére vonatkozó képzés;
- Biztonsági személyzet képzését és fejlesztését elősegítő program;
- Fenyegetettség tudatosító program;
- Szerepkör alapú biztonságtudatossági képzés.