



NEMZETI
AKKREDITÁLO
TESTÜLET

Nemzeti Akkreditálási Rendszer

**EA Útmutató
információbiztonság-irányítási
rendszerek
tanúsítását/regisztrálását
végző szervezetek
akkreditálásához**

NAR-EA-7/03

1. kiadás

2004. március



Európai
Akkreditálási
Együttműködés

Kiadvány
Referencia

EA 7/03

**EA Irányelvek:
információbiztonság-irányítási
rendszerek tanúsítását/regisztrálását
végző szervezetek akkreditálására**

CÉL

E dokumentum szövegét az Európai Akkreditálási Együttműködés (EA) munkacsoportja dolgozta ki. E dokumentum célja, hogy magyarázatokat szolgáltatson azzal a céllal, hogy összhangba hozza az ISO/IEC Guide 62/EN 45012 alkalmazását az információbiztonság-irányítási rendszerek területén az akkreditáló testületek, azok minősítői és az akkreditálásra előkészítő tanúsító/regisztráló szervezetek által. E dokumentumot az EA Közgyűlése hagyta jóvá 1999 novemberében.

A mérvadó dokumentum az ISO/IEC Guide 62/EN 45012 marad és e dokumentum alkalmazására vonatkozó vitás kérdésekben az egyes akkreditáló testületek határoznak a megoldatlan kérdésekben.

EA-7/03 EA Útmutató az információbiztonsági irányítási rendszerek tanúsítását/registrlását végző szervezetek akkreditálására

Szerzők

E kiadványt az EA CS WG7 Informatika és Kommunikációs Technológia munkacsoport készítette.

Hivatalos nyelv

A szöveg szükség szerint fordítható különböző nyelvekre. Az angol nyelvű változat a meghatározó.

Szerzői jog

E szöveg szerzői jogát az EA fenntartja magának. A szöveg továbbértékesítés céljából nem sokszorosítható.

További információ

Jelen kiadványt érintő további információval kapcsolatosan az EA nemzeti tagjához fordulhat.

Friss információért keresse fel weboldalunkat:

<http://www.european-accreditation.org>



TARTALOM

BEVEZETÉS AZ INFORMÁCIÓBIZTONSÁG-IRÁNYÍTÁSI RENDSZEREK TANÚSÍTÁSÁT/REGISZTRÁLÁSÁT VÉGZŐ SZERVEZETEK AKKREDITÁLÁSÁRA VONATKOZÓ EA IRÁNYELVEKHEZ (ISMS)

BEVEZETÉS AZ ISMS TANÚSÍTÁSÁHOZ/REGISZTRÁLÁSÁHOZ

1. FEJEZET: ÁLTALÁNOS RÉSZ

- 1.1. Alkalmazási terület
- 1.2. Hivatkozások
- 1.3. Meghatározások

2. FEJEZET: KÖVETELMÉNYEK A TANÚSÍTÓ/REGISZTRÁLÓ SZERVEZETEKRE

- 2.1. Tanúsító/regisztráló szervezet
- 2.2. A tanúsító/regisztráló szervezet személyzete
- 2.3. A tanúsítási/regisztrálási követelmények módosítása
- 2.4. Felszólalások, panaszok és viták

3. FEJEZET: TANÚSÍTÁSI/REGISZTRÁLÁSI KÖVETELMÉNYEK

- 3.1. A tanúsítás/regisztrálás kérelmezése
- 3.2. Felkészülés a minősítésre
- 3.3. Minősítés
- 3.4. Minősítő jelentés
- 3.5. Döntés a tanúsításról/regisztrálásról
- 3.6. Felügyelet és újraminősítési eljárások
- 3.7. Tanúsítványok és emblémák alkalmazása
- 3.8. Hozzáférés a szervezetekhez eljuttatott panaszokról készült feljegyzésekhez

1. MELLÉKLET: AZ AKKREDITÁLÁS TÁRGYKÖREI

BEVEZETÉS AZ INFORMÁCIÓBIZTONSÁG-IRÁNYÍTÁSI RENDSZEREK (ISMS) TANÚSÍTÁSÁT/REGISZTRÁLÁSÁT VÉGGŐ SZERVEZETEK AKKREDITÁLÁSÁRA VONATKOZÓ EA IRÁNYELVEKHEZ

E dokumentum szövege három fő forrásból származik: az ISO/IEC Guide 62:1996 eredeti szövege (amellyel azonos az EN 45012:1998), az IAF útmutató az ISO/IEC Guide 62 eredeti szövegéhez és egyedi szöveg, amely kiegészítő útmutatót ad az ISMS tanúsításban/regisztrálásban résztvevő szervezeteknek az EN 45012 alkalmazására. A Guide 62 és az IAF útmutató szövegét szükség szerint módosították, hogy feleljen meg az információbiztonság-irányítási rendszereknek (ISMS). A (minimális) változtatásokat az eredeti szövegekben és az egyedi ISMS útmutató szövegében eredetileg egy UKAS által finanszírozott UK munkacsoport alakította ki és továbbfejlesztette az EA-C5-WG7 „Információ és kommunikációs technológia” EA munkacsoport.

A szövegek eredetét különböző szedéstípusok használatával lehet azonosítani:

- **Az ISO/IEC Guide 62 szövege: minimális változtatásokkal, hogy alkalmazható legyen az ISMS területén. Az EA elismeri ennek az anyagnak az ISO szerzői jogát és módosítani fogja ezt a dokumentumot, amikor az ISO/IEC az anyagot végleges formában közli.**
- IAF útmutató az ISO/IEC Guide 62-höz: minimális változtatásokkal, hogy alkalmazhatóvá tegye az ISMS területén.
- EA útmutató az ISO/IEC Guide 62-höz, speciálisan az ISMS részére.

A „shall” (kell) kifejezést használják e dokumentumban, hogy mutassák azokat a rendelkezéseket, amelyek az ISO/IEC követelményeit kifejezve kötelezők. A „should” (célszerű, ajánlatos) kifejezést alkalmazzák, hogy azokat a rendelkezéseket, amelyek bár útmutatást fejeznek ki a követelmények alkalmazásához, várhatóan a tanúsító/regisztráló szervezet részéről elfogadásra találjanak. Egy tanúsító/regisztráló szervezet útmutatójától való bármilyen eltérés kivétel kell legyen. Ilyen eltérések csak esetenként megengedettek, miután a tanúsító/regisztráló szervezet igazolta az akkreditáló testületnek, hogy a kivétel kielégíti az ISO/IEC Guide 62 megfelelő követelményeit és ezen útmutató szándékát valamilyen egyenértékű módon.

BEVEZETÉS AZ ISMS TANÚSÍTÁSHOZ/REGISZTRÁLÁSHOZ

Az információbiztonság-irányítás rendszereinek (ISMS) szabványai a legjobb gyakorlati szabályokat nyújtják a szervezeteknek. A BS 7799 szabvány 2. része és más rendelkező dokumentumok előírások az információbiztonság irányítására, amelyek alkalmasak az ISMS alapú tanúsításra/registrlásra. Ezek átfogó biztonsági szabályozásegüttest alkotnak, amely a jelenleg használt legjobb információbiztonsági gyakorlatot tartalmazza. Céljuk, hogy a szervezeteket ellássák az információbiztonság közös alapjával és lehetővé tegyék, hogy az információt a szervezetek között megosszák. Ez különösen fontos, ahol a szervezetek egymással elektronikus kapcsolatban kívánnak lenni.

Egy információbiztonság-irányítási rendszer (ISMS) tanúsítása/registrlása egyik eszköze annak, hogy biztosítékot nyújtsanak, hogy a tanúsított/registrlált szervezet egy szabványnak vagy a rendelkező dokumentumnak megfelelő információbiztonság-irányítási rendszert bevezetett.

Ez a közlemény követelményeket ír elő, amelyek megtartásának célja, hogy biztosítsa, hogy a tanúsítási/registrlási szervezetek következetesen és megbízhatóan működtessenek független tanúsítási/registrlási rendszereket, ezáltal elősegítsék azok elfogadását nemzeti és nemzetközi alapon. Ez a közlemény megalapozásul kíván szolgálni a nemzeti rendszerek elismeréséhez a nemzetközi kereskedelem érdekében.

A közlemény célja, hogy olyan tetszés szerint leírt szervezetek alkalmazzák, amelyek minősítési és ISMS tanúsítási/registrlási funkciókat hajtanak végre. A megfogalmazás kényelme szempontjából ezekre a szervezetekre általában mint „tanúsítási/registrlási szervezetek”-re hivatkoznak. Ez a megfogalmazás nem lehet akadálya, hogy ezt a dokumentumot más rendeltetésű szervezetek használják, olyan tevékenységeket vállalva, amelyeket ez a közlemény tartalmaz. Valójában ez a közlemény használható kell legyen az ISMS tanúsításban/registrlásban résztvevő bármely szervezetben.

Az ISMS tanúsítás/registrlás magába foglalja egy szervezet ISMS minősítését, de nem foglalja magába a termékeire és szolgáltatásaira vonatkozó információbiztonság egyedi szintjeit. A szabványnak vagy rendelkező dokumentumnak és bármely kiegészítő dokumentációnak való megfelelés bizonyítéka egy tanúsítási/registrlási dokumentum alakjában történik. Az ISMS tanúsítás/registrlás biztosítja, hogy a szervezet kockázatminősítést végzett és az üzletvitel információbiztonság igényeinek megfelelő szabályozásokat határozott meg és vezetett be.

Egy ISMS tanúsítása/registrlása teljes mértékben önkéntes. Azokban a szervezetekben, amelyekben sikeresen végrehajtják a tanúsítási/registrlási folyamatot nagyobb bizalmat élvezhetnek információbiztonsági irányításuk iránt és képesek lesznek a tanúsítvány olyan használatára, hogy segítsék üzleti ügyfeleiket biztosítani, akikkel megosztják az információt. A tanúsítvány a képesség nyilvános kinyilvánítása, miközben megengedi a szervezetnek, hogy információbiztonsági intézkedéseinek részleteit bizalmasan kezelje. Míg ennek a közleménynek célja, hogy a tanúsítási/registrlási szervezetek felkészültségének elismerésében érdekelt szervezetek használják, az abban levő számos intézkedés hasznos lehet második fél minősítési eljárásaiban is.



1. FEJEZET: ÁLTALÁNOS RÉSZ

1.1. Alkalmazási terület

Ez a közlemény általános követelményeket ír elő egy független ISMS tanúsítást/regisztrálást végző szervezet részére, amelynek meg kell feleljen, ha azt mint felkészültet és megbízhatót kell elismerni az ISMS tanúsítás/regisztrálás végzésében.

1. MEGJEGYZÉS: egyes országokban azokat a szervezeteket, amelyek az ISMS-nek való megfelelést igazolják, előírt szabványok szerint „tanúsító szervezetek”-nek, másokban „regisztráló szervezetek”-nek, ismét másokban „minősítő és regisztráló szervezetek”-nek vagy „tanúsító/regisztráló szervezetek”-nek és még „regisztrálók”-nak nevezik. Könnyű érthetőség kedvéért ez a közlemény ezekre a szervezetekre mindig úgy utal, mint „tanúsító/regisztráló szervezetek”-re. Ezt nem szabad korlátozásként felfogni.

Az ebben a közleményben levő követelményeket mindenekelőtt azért írták, hogy általános követelményeknek tekintsék bármely szervezet részére, amely ISMS tanúsítást/regisztrálást végez.

1.2. Hivatkozások

ISO/IEC Guide 2:1996 Általános fogalmak és azok meghatározása a szabványosításra és rokon tevékenységekre

ISO 8402: 1994 Minőségirányítás és minőségbiztosítás. Szótár

ISO/IEC Guide 62:1996 Általános követelmények a minőségrendszerek minősítését és tanúsítását/regisztrálását végző szervezetekre

BS 7799 Part 1:1999 Rendszabály információbiztonság irányítására

BS 7799 Part 2:1999 Előírás információbiztonság-irányítási rendszerekre

ISO 10011-1:1990 Irányelvek minőségügyi rendszerek auditálására. 1. rész: Auditálás

ISO 10011-2:1991 Irányelvek minőségügyi rendszerek auditálására. 2. rész: Minősítési követelmények minőségügyi rendszer auditorokra

ISO 10011-3:1991 Irányelvek minőségügyi rendszerek auditálására. 3. rész: Auditprogramok irányítása

1.3. Meghatározások

E közlemény céljára az ISO/IEC Guide 2, BS 7799 Part 1 és BS 7799 Part 2 vonatkozó meghatározásai és a következő meghatározások érvényesek.

1.3.1. Szervezet

Vállalat, társaság, cég, vállalkozás, hatóság vagy intézmény, ezek része vagy kombinációja, akár bejegyzett, akár nem, közületi vagy magán, melynek saját funkciói és adminisztrációja van és képes biztosítani, hogy az információ biztonságát ellátják.

1.3.2. Tanúsító/registrláló szervezet

Független (harmadik) fél, amely egy szervezet ISMS-ét minősíti és tanúsítja/registrlálja, tekintetbe véve a közzétett ISMS szabványokat és minden kiegészítő, a szabványban megkövetelt dokumentációt.

1.3.3. Tanúsítási/registrlási dokumentum

Dokumentum, amely mutatja, hogy egy szervezet ISMS-e megfelel az előirt ISMS szabványoknak és minden, a rendszerben megkövetelt kiegészítő dokumentációnak.

1.3.4. Tanúsító/registrláló rendszer

Olyan rendszer, amelynek saját szabályai vagy eljárása és vezetősége van, hogy elvégezze azt a minősítést, amely egy tanúsítási/registrlási dokumentum kiadásához és azt követő fenntartásához vezet.

IAF útmutató

G.1.3.1. A következő meghatározások érvényesek az ebben a dokumentumban levő útmutatóra:

Minősítés: Egy szervezet tanúsítására/registrlására vonatkozó összes tevékenység, hogy meghatározza, hogy a szervezet teljesíti-e a tanúsítás/registrlálás megadásához szükséges, előirt szabvány vonatkozó fejezeteinek összes követelményeit és hogy azokat megfelelően bevezették-e, beleértve a dokumentáció-átvizsgálást, az audit előkészítést és az auditjelentés megfontolását és más vonatkozó tevékenységeket, amelyek szükségesek, hogy elegendő információt nyújtsanak, amely lehetővé teszi, hogy döntsenek, hogy a tanúsítást/registrlást meg kell-e adni.

Embléma: Egy szervezet által használt jelkép, mint az azonosítási forma, rendszerint stilizálva. Az embléma lehet jel is.

Jel: Törvényesen bejegyzett kereskedelmi jel vagy más módon védett jelkép, amelyet egy akkreditálási testület vagy egy tanúsító/registrláló szervezet szabályai szerint bocsátanak ki, amely azt mutatja, hogy a testület/szervezet által működtetett rendszerekben kellő bizalmat bizonyítottak, vagy hogy a vonatkozó termékek vagy egyének egy előirt szabvány követelményeinek megfelelnek.

Nemmegfelelés: Az irányítási rendszer megkövetelt elemei közül egy vagy több hiánya, vagy bevezetésének és fenntartásának hiányossága, vagy olyan helyzet, amely objektív bizonyíték alapján jelentős kétséget ébreszt az ISMS azon képességével szemben, hogy elérje a biztonsági politikát és szervezeti célokat.

A tanúsító/registrláló szervezetnek szabadon áll módjában, hogy hiányossági fokozatokat és jobbítási területeket határozzon meg (pl. nagyobb vagy kisebb nemmegfelelés, észrevételek stb.). Azonban az összes hiányosságokat, amelyek megfelelnek a fenti megfelelési meghatározásnak, a G.3.5.2. és G.3.6.1. útmutató szerint kell kezelni.

- G.1.3.2. Egy tanúsító/regisztráló szervezet akkreditált alkalmazási területét/területeit az iparágak vagy termékkategóriák jegyzékének egy vagy több eleme szerint kell kifejezni, amely az „akkreditálás tárgyköre”-ként ismert (lásd az 1. mellékletet).
- G.1.3.3. Az akkreditálásra vonatkozóan más korlátozások is vonatkozhatnak, pl. szűkítés bizonyos irodákra vagy helyekre.

ISMS útmutató

- IS.1 Egy tanúsító/regisztráló szervezet akkreditált alkalmazási területe(i) szorosan kapcsolódnak az auditor felkészültségéhez, amely többek között fontos a szervezetek által az ISMS-ük kialakítása és fenntartása során végzett kockázatelemzés auditálásában. A tanúsító/regisztráló szervezettől megkívánják, hogy mutassa be az akkreditáló testületnek hogy az auditorok felkészültek azokban az iparágakban, amelyekben az ISMS-eket minősítik és tanúsítják/regisztrálják.

The logo for NAT (National Accreditation Authority for IT) is displayed in a large, light gray font. It consists of the letters 'N', 'A', and 'T' in a bold, serif typeface, set against a dark gray rectangular background.

2. FEJEZET: KÖVETELMÉNYEK A TANÚSÍTÓ/REGISZTRÁLÓ SZERVEZETEKRE

2.1. Tanúsító/regisztráló szervezet

2.1.1. Általános rendelkezés

2.1.1.1. Az eljárásrendek és eljárások, amelyek szerint a tanúsító/regisztráló szervezet működik, ne legyenek megkülönböztetők és ezeket nem megkülönböztető módon kell kezelni. Az eljárásokat nem szabad arra használni, hogy megakadályozzák vagy meggátolják kérelmezők hozzáférését, e közleményben előírttól eltérően.

2.1.1.2. A tanúsító/regisztráló szervezet tegye szolgáltatásait minden kérelmező számára elérhetővé. Nem lehetnek indokolatlan pénzügyi vagy más feltételek. Az igénybevétel nem függhet a szervezet nagyságától vagy bármely egyesülés vagy csoport tagságától, sem a már tanúsított/regisztrált szervezetek számától.

2.1.1.3. A kritériumok, amelyek szerint egy kérelmező ISMS-ét minősítik, az ISMS szabványban vagy más rendelkező dokumentumokban a végzett funkcióra vonatkozók legyenek. Ha ezeknek a dokumentumoknak egy egyedi tanúsító/regisztráló programban való alkalmazásához magyarázat szükséges, ezt az illetékes és pártatlan bizottságok vagy személyek kell megfogalmazzák, amelyeknek a szükséges műszaki felkészültségük megvan és a tanúsító/regisztráló szervezet hozza nyilvánosságra.

2.1.1.4. A tanúsító/regisztráló szervezet korlátozza a tanúsításra/regisztrálásra vonatkozó követelményeit, minősítését és döntését azokra a kérdésekre, amelyek kifejezetten a szóban forgó tanúsítás/regisztrálás alkalmazási területére vonatkoznak.

IAF útmutató

G.2.1.1. Az ISO/IEC Guide 62 2.2.1.3. szakaszában szereplő rendelkezést „ha magyarázat szükséges” úgy kell alkalmazni, hogy ezeket a dokumentumokat az akkreditáló testület által elismert dokumentumokra kell korlátozni. Az ISO/IEC Guide 62 1.3.1. és 1.3.3. szakaszaiban használt „és kiegészítő dokumentáció, amelyet a rendszerben kívánnak” kifejezés az akkreditáló testület által elismert dokumentációt kívánja jelteni, amely további vagy kiegészítő útmutatást ad a vonatkozó szabvány vagy irányelv alkalmazására (lásd még G.2.1.9. útmutatót). Kivételes esetekben maga a tanúsító/regisztráló szervezet adhat ki kiegészítő dokumentációt, az ISO/IEC Guide 62 2.1.1.3. szakasz követelményeitől függően.

G.2.1.2. Egy ISMS tanúsítása/regisztrálása megfelelő bizalmat kell keltsen, hogy a rendszer megfelel az előírt követelményeknek. Egy szervezet ISMS-ének megfelelési tanúsítása/regisztrálása be kell mutassa, hogy egy szervezet hatásos ISMS-et vezetett be és tart fenn a tanúsítványban előírt területen és folyamatait ezzel a rendszerrel összhangban működteti.

- G.2.1.3. A gyakorlatban „előírt követelmények” a G.2.1.2. útmutatóban az ügyfél és a szervezet közötti megállapodásos követelményeket jelenti. Ha egy szervezet egy megkívánt előírás szerinti szolgáltatásokat ad, az ügyfél ezeket a vásárlási tevékenységgel „megállapodott követelmények”-ké teheti. A „megállapodott követelmények” magukba foglalják a „jogi követelményeket”, ha ezeknek való megfelelést kéri a szervezet vagy ránézve ez kötelező. Bármely esetben a vonatkozatható jogi követelményeknek való megfelelés, mely vonatkozik egy termékre vagy szolgáltatásra, normális esetben csak akkor lesz egy ügyfél követelménye, ha a szerződésbe beleértendő fogalom, amelyet a szerződés átvizsgáláskor figyelembe kell venni.
- G.2.1.4. A tanúsító/registrláló szervezetek a megkülönböztetés semmilyen formáját nem alkalmazhatják, mint pl. rejtett megkülönböztetés, a kérelmezés felgyorsításával vagy késleltetésével.
- G.2.1.5. Az ISO/IEC Guide 62 2.1.1.2. szakasza megköveteli, hogy a tanúsító/registrláló szervezetek tegyék szolgáltatásaikat elérhetővé minden kérelmezőnek. Nyújthatnak azonban egy tanúsítási/registrlási szolgáltatást, amely kizárja azokat a tevékenységi területeket, amelyeken a tanúsító/registrláló szervezet nincs tanúsításra/registrlásra minősítve vagy azt választotta, hogy nem nyújt szolgáltatást valamilyen szervezetnek egy meghatározott kategóriában. Például egy tanúsító/registrláló szervezet, amennyiben a törvény megengedi, korlátozza szolgáltatását olyan kérelmezőkre, akik meghatározott földrajzi körzetben tevékenykednek vagy korlátozhatja szolgáltatását olyan szervezetekre, amelyek egy meghatározott műszaki ágazatban vagy annak egy részében működnek, amelyben a tanúsító/registrláló szervezetnek az akkreditált alkalmazási területe van.
- G.2.1.6. Egy tanúsító/registrláló szervezet felajánlhat termékmegfelelési vagy minőségügyi rendszertanúsítást/registrlást összekötve ISMS tanúsítással/registrlással vagy csak egyedül ISMS tanúsítást/registrlást.
- G.2.1.7. Ha a tanúsító/registrláló szervezet szervezeteket egy olyan rendelkező dokumentum szerint tanúsít/registrlál, amely nem szabvány, az a dokumentum nyilvánosan hozzáférhető kell legyen.
- G.2.1.8. Az ISO/IEC Guide 62 2.1.1.3. szakaszában használt „egy egyedi tanúsítási/registrlási program” kifejezés tartalmazhat ágazatspecifikus alrendszereket.
- G.2.1.9. Az ISO/IEC Guide 62 2.1.1.3. szakaszában említett ilyen dokumentumok alkalmazására vonatkozó magyarázatok megfogalmazását a tanúsító/registrláló szervezetek, amelyeket egy EA tag akkreditáló testület akkreditált, korlátozzák az EA által közzétett útmutatás szerint, lásd G.2.1.1. útmutatót.

2.1.2. Szervezeti felépítés

A tanúsító/registrláló szervezet felépítése keltsen bizalmat a tanúsításai/registrlásai iránt.

A tanúsító/registrláló szervezet különösen feleljen meg a következőknek:

- a) legyen pártatlan;**
- b) legyen felelős a tanúsítás/registrlálás megadására, fenntartására, kiterjesztésére, szűkítésére, felfüggesztésére és visszavonására vonatkozó döntéseikért;**
- c) határozza meg azt a vezetőséget (bizottság, csoport vagy személy), amely átfogóan felelős a következőkért:**
 - 1) e közleményben meghatározott minősítés és tanúsítás/registrlálás elvégzéséért,**
 - 2) a tanúsító/registrláló szervezet működésére vonatkozó politikai kérdések megfogalmazásáért,**
 - 3) a tanúsítási/registrlálási döntésekért,**
 - 4) az eljárásrendjei megvalósításának felügyeletéért,**
 - 5) a tanúsító/registrláló szervezet pénzügyeinek felügyeletéért,**
 - 6) a hatásköröknek bizottságokra vagy egyénekre való átruházásáért ahogy az szükséges ahhoz, hogy azok meghatározott tevékenységeket vállaljanak a maguk nevében;**
- d) legyenek jogi személyiségét igazoló dokumentumai;**
- e) legyen pártatlanságát biztosító dokumentált szervezeti felépítése, beleértve a tanúsító/registrláló szervezet működésének pártatlanságát biztosító intézkedéseket; ez a szervezeti felépítés tegye lehetővé a tanúsító/registrláló rendszer tartalmára és működésére vonatkozó eljárásrendek és elvek kialakításában jelentős mértékben érdekelt minden fél részvételét;**
- f) biztosítsa, hogy a tanúsításra/registrlálásra vonatkozó minden döntést olyan személy/ek/ végezze/végezzék, akik a minősítést végzőktől különbözők;**
- g) legyenek a tanúsító/registrláló tevékenységre vonatkozó jogai és felelőssége;**
- h) tegye meg a megfelelő intézkedéseket, amelyek a tevékenységekből és/vagy működésből származó felelősségeket fedezik;**
- i) legyen meg a pénzügyi stabilitása és erőforrásai a tanúsítási/registrlálási rendszer működtetésére;**
- j) alkalmazzon egy felelős, felső vezető alá tartozó megfelelő létszámú személyzetet, amelynek megvan a szükséges képesítése, gyakorlati képzettsége, műszaki ismerete, gyakorlata az elvégzendő munka jellegének, körének és terjedelmének megfelelő tanúsítási/registrlálási feladatok elvégzéséhez;**
- k) legyen a 2.1.4. szakaszban körvonalazott minőségügyi rendszere, amely bizalmat nyújt arra, hogy a szervezetek részére képes egy tanúsítási/registrlálási rendszert működtetni;**
- l) legyen eljárásrendje és eljárásai, amelyek különbséget tesznek a szervezetek tanúsítása/registrlálása és minden egyéb, a szervezet által vállalt tevékenységek között;**

- m) a szervezet felső vezetőségével és személyzetével együtt legyen mentes minden kereskedelmi, pénzügyi és más ráhatástól, amely befolyásolhatná a tanúsítási/registrlációs folyamata eredményeit;
- n) legyenek hivatalos szabályai és szervezeti felépítése a tanúsítási/registrlási folyamatban részt vevő minden bizottság kijelölésére és működtetésére, ezek legyenek mentesek mindenféle kereskedelmi, pénzügyi és más ráhatástól, amely befolyásolhatná döntéseiket (lásd 2. megjegyzést);
- o) biztosítsa, hogy a kapcsolódó szervezetek tevékenységei ne befolyásolják a tanúsítások/registrlások bizalmas jellegét, tárgyilagosságát vagy pártatlanságát és ne ajánljanak vagy ne végezzenek
 - 1) olyan szolgáltatásokat mások részére, amelyeket a szervezet tanúsít/registrlál,
 - 2) tanácsadó szolgáltatásokat a tanúsítás/registrlálás megszerzéséhez vagy megtartásához,
 - 3) szolgáltatásokat ISMS vagy kapcsolt irányítási rendszerek tervezéséhez, bevezetéséhez vagy fenntartásához (lásd 3. megjegyzést);
- p) legyen eljárásrendje és eljárásai a szervezetektől vagy más felektől a tanúsítások/registrlások vagy bármely ezzel kapcsolatos ügyek kezelésére vonatkozóan kapott panaszok, felszólalások és vitás kérdések megoldására.

MEGJEGYZÉSEK:

- 2. Azt a szervezeti felépítést, ahol a tagokat úgy választják, hogy az megvalósítsa az érdekek egyensúlyát és ahol egyes érdekek nincsenek túlsúlyban, olyannak kell tekinteni, mint amely ennek az intézkedésnek megfelel.
- 3. Más termékeket, folyamatokat vagy szolgáltatásokat akkor lehet közvetlenül vagy közvetve felajánlani, ha ezek nem veszélyeztetik a szervezet tanúsítási/registrlási folyamatának és döntéseinek bizalmas jellegét, tárgyilagosságát vagy pártatlanságát.

IAF útmutató

- G.2.1.10. Akkreditálást csak olyan testületnek lehet adni, amely jogi személyiség az ISO/IEC Guide 62 2.1.2. d) szakasz értelmében és kinyilvánított alkalmazási területekre, tevékenységekre és helyekre szorítkozik. Ha a tanúsítási/registrlási tevékenységeket olyan jogi személyiség végzi, amely egy nagyobb jogi személyiség része, a nagyobb egység többi részével való kapcsolatokat egyértelműen meg kell határozni és bizonyítani kell, hogy nem lép fel a G.2.1.22. és G.2.1.23. útmutatóban meghatározott érdekütközés. A vonatkozó információt a nagyobb jogi személyiség más részei által végzett tevékenységekre vonatkozóan a tanúsító/registrláló szervezet kell közölje az akkreditáló testülettel.

G.2.1.11. Annak bizonyítása, hogy egy tanúsító/regisztráló szervezet az ISO/IEC Guide 62 2.1.2. d) szakasz szerint megkívánt jogi személyiség, azt jelenti, hogy ha egy kérelmező tanúsító/regisztráló szervezet egy nagyobb jogi egység része, az akkreditálást csak az egész jogi személyiségnek lehet megadni. Ilyen helyzet esetén az egész jogi személyiség szervezeti felépítését auditálhatja az akkreditáló testület azért, hogy egyedi auditnaplókat és/vagy átvizsgálási feljegyzéseket kövessen a tanúsító/regisztráló szervezetre vonatkozóan. A jogi személyiségnek az a része, amely a tényleges tanúsító/regisztráló szervezetet alkotja, egy külön név alatt folytathat kereskedést, ez meg kell célszerűen jelenjen az akkreditálási tanúsítványon.

Az ISO/IEC Guide 62 2.1.2. d) céljából azok a tanúsítók/regisztrálók, amelyek a kormányzat/közigazgatás részei vagy kormányzati részlegek, jogi személyiségeknek fognak minősülni kormányzati státuszuk miatt. Ezeknek a részlegeknek a státuszát és szervezeti felépítését hivatalosan dokumentálni kell és annak meg kell felelnie az ISO/IEC Guide 62 összes követelményének.

G.2.1.12. A tanúsító/regisztráló szervezet pártatlanságát és függetlenségét három szinten kell biztosítani:

- 1) stratégia és politika;
- 2) a tanúsításra/regisztrálásra vonatkozó döntések;
- 3) auditálás.

Az ISO/IEC Guide 62 2.1.2. szakaszához való útmutató célja, hogy gondoskodjék a pártatlanságról és függetlenségről mind a három szinten.

G.2.1.13. Az ISO/IEC Guide 62 2.1.2. a) szakaszban megkívánt pártatlanság csak olyan felépítéssel biztosítható, ahogy azt az ISO/IEC Guide 62 2.1.2. e) szakasz követeli, amely lehetővé teszi "mindazon felek részvételét, akik jelentős mértékben érdekeltek a tanúsító/regisztráló rendszer tartalmát és működését illető eljárásrendek és elvek kialakításában".

G.2.1.14. Az ISO/IEC Guide 62 2.1.2 c) szakasz követelményeinek kielégítésére létrehozott vezetőség nem kell ugyanaz legyen, mint az ISO/IEC Guide 62 2.1.2. e) szakaszban megkövetelt szervezeti felépítés.

G.2.1.15. Az ISO/IEC Guide 62 2.1.2. e) szakaszra vonatkozó megfelelésnek az a hatása, hogy egy tanúsító/regisztráló szervezet tulajdonosai részéről jövő mindenféle olyan tendenciát ellensúlyozza, hogy kereskedelmi vagy más megfontolásokat tegyen lehetővé szolgáltatása következetes, műszakilag objektív nyújtása megelőzésére. Ez különösen szükséges, ha egy tanúsító/regisztráló szervezet felállításához a pénzalapot egy speciális érdekeltég nyújtotta, amely túlnyomó többségben van a részvényesek között és/vagy az igazgatótanácsban.

G.2.1.16. Az ISO/IEC Guide 62 2.1.2. e) szakasz azért azt kívánja, hogy a tanúsító/regisztráló szervezet dokumentált szervezeti felépítésébe legyen beépítve intézkedés az összes jelentősen érdekelt fél részvételére. Ez rendszeren valamilyen bizottság által történik. A létrehozott szervezeti felépítés legyen előírva a

tanúsító/registrláló szervezet írott alapszabályában és nem módosítható az akkreditáló testület értesítése nélkül.

- G.2.1.17. Mindig megítélés kérdése, hogy a rendszerben jelentős mértékben érdekelt összes fél képes-e részt venni. Ami lényeges, hogy minden azonosítható nagyobb érdekeltiségnek meg kell adni a lehetőséget a részvételre és hogy az érdekegyensúlyt elérjék, ahol egyetlen érdekeltiség sincs túlsúlyban.

ISMS útmutató

- IS.2 A 2.1.2. e) szakaszban említett felek lehetnek vevők és szállítók az iparban és kereskedelemben, szabályozó szervek, kereskedelmi szervezetek, információbiztonság-irányítási szakemberek és ezzel kapcsolódó szakemberek és a kormányzat.

IAF útmutató

- G.2.1.18. Az ISO/IEC Guide 62 2.1.2. c) szakaszban leírt különböző feladatkörökért felelős vezetőség adja meg a tanúsítás/registrlálás szempontjából az összes szükséges információt, beleértve az összes jelentős döntés és beavatkozás indokait és az egyes tevékenységekért felelős személyek kiválasztását a tanúsítás/registrlálás szempontjából az ISO/IEC Guide 62 2.1.2. e) szakaszban hivatkozott bizottságnak vagy ezzel egyenértékű szervnek, hogy lehetővé tegye megfelelő és pártatlan tanúsítás/registrlálás biztosítását. Ha a vezetőség bármely kérdésben nem veszi figyelembe ennek a bizottságnak vagy a vele egyenértékű szervnek a tanácsát, a bizottság vagy a vele egyenértékű szerv megfelelő intézkedéseket kell tegyen, amely magába foglalhatja az akkreditáló testület tájékoztatását.
- G.2.1.19. Ha a tanúsító/registrláló szervezet és egy kérelmező vagy tanúsított/registrlált szervezet együttesen részei a kormányzatnak, ezek ne jelentsenek közvetlenül olyan személynek vagy csoportnak, amelynek operatív felelőssége van mindkettőért. A tanúsító/registrláló szervezet pártatlanság követelménye tekintetében képes legyen bemutatni, hogy hogyan kezel egy ilyen esetet.
- G.2.1.20. Ha a döntést, hogy az ISO/IEC Guide 62 2.1.2. n) szakasz szerint adjanak ki vagy vonjanak vissza egy tanúsítványt/registrlálást, egy bizottság hozza, amelynek tagjai között vannak többek között egy vagy több tanúsított/registrlált szervezet képviselői, a tanúsító/registrláló szervezet operatív eljárásai biztosítsák, hogy ezek a képviselők ne rendelkezzenek jelentős befolyással a döntéshozásra. Ez például a szavazati jog elosztásával vagy más egyenértékű módszerrel biztosítható.
- G.2.1.21. Az ISO/IEC Guide 62 2.1.2. o) szakasza két különálló követelménnyel foglalkozik. Először, a tanúsító/registrláló szervezet semmilyen körülmények között ne nyújtsa e szakasz 1), 2) és 3) pontban meghatározott szolgáltatásait. Másodszor, bár nincs konkrét korlátozás azokra a szolgáltatásokra vagy tevékenységekre, amelyeket egy kapcsolódó szervezet nyújthat, ezek ne

befolyásolják a tanúsító/registrláló szervezet bizalmas kezelését, tárgyilagosságát vagy pártatlanságát.

G.2.1.22. Tanácsadás aktív és alkotó módon való részvételnek tekintendő a minősítésre kerülő ISMS kialakításában, például:

- a) kézikönyvek, gépkönyvek vagy eljárások előkészítése vagy előállítása;
- b) részvétel a döntéshozási folyamatban az irányítási rendszer kérdéseiben;
- c) egyedi tanácsadás a végleges tanúsítás/registrlálás számára az irányítási rendszerek kialakításához és vezetéséhez.

Megjegyzés: A G.2.1.22. útmutatóban hivatkozott irányítási rendszerek az ilyen rendszerek minden szempontját magukba foglalják, beleértve a pénzügyieket.

G.2.1.23. A tanúsító/registrláló szervezetek a következő feladatokat elvégezhetik, anélkül, hogy azokat tanácsadásnak vagy lehetséges érdekellentétnek lehetne tekinteni:

- a) tanúsítás/registrlálás, beleértve az informáló és tervezési összefüggéseket, a dokumentumok megvizsgálását, auditálást (nem véve ide a belső auditálást és a belső biztonsági átvizsgálásokat) és a nemmegfelelések követését;
- b) képzési tanfolyamok rendezése és azokon előadóként való részvétel, feltéve, hogy amikor ezek a tanfolyamok az információbiztonság irányítására, a kapcsolódó irányítási rendszerekre vagy auditálásra vonatkoznak, ezek korlátozódnak az általános információ és tanácsadásra, amely ingyen elérhető nyilvános területen, azaz nem tartalmazhatnak vállalat-specifikus tanácsot, amely ellentmond a G.2.1.22. c) szakasz követelményeinek;
- c) információ elérhetővé tétele vagy kérésre adása a tanúsító/registrláló szervezetnek a minősítési szabványok követelményeire vonatkozó magyarázata alapján;
- d) audit előtti tevékenységek, amelyek csak a minősítésre való felkészültség meghatározására szolgálnak, de ezeknek a tevékenységeknek nem lehet az eredménye, hogy a G.2.1.22. útmutatóban ellentmondó ajánlásokat vagy tanácsokat közöljenek és a tanúsító/registrláló szervezet képes legyen megerősíteni, hogy az ilyen tevékenységek nem mondanak ellent ezeknek a követelményeknek és nem használják arra, hogy a végleges minősítési időtartam csökkenését igazolják;
- e) második és harmadik fél általi (független) auditok végzése olyan szabványok vagy szabályzatok szerint, amelyek nem részei az akkreditálás alkalmazási területének;
- f) hozzáadott érték a minősítések és felügyeleti látogatások során, például a jobbítási lehetőségek meghatározása, ahogy azok nyilvánvalóvá válnak az audit során, anélkül, hogy egyedi megoldásokat ajánlanának.

G.2.1.24. Egy illető szervezet tanácsadása és tanúsítás/registrlálás sohasem értékesíthető együtt és semmit sem szabad az értékesítési anyagban vagy előadáson, akár szóban, akár írásban állítani, hogy azt a benyomást keltse, hogy a kétféle tevékenység össze van kötve. A tanúsító/registrláló szervezet kötelessége, hogy

biztosítsa, hogy egyik ügyfelének se legyen az a benyomása, hogy mindkét szolgáltatás (a tanúsítás/registrlálás és tanácsadás) az ügyfél számára bármilyen üzleti előnnyel járna, úgyhogy a tanúsítás/registrlálás pártatlan marad és annak is látszik.

- G.2.1.25. Egy tanúsító/registrláló szervezet nem mondhat semmi olyat, ami azt a látszatot keltené, hogy a tanúsítás/registrlálás egyszerűbb, könnyebb vagy olcsóbb lenne, ha bármilyen előírt tanácsadást vagy képzési szolgáltatást alkalmaznának.
- G.2.1.26. Az ISO/IEC Guide 62 2.1.2. o) szakaszban hivatkozott kapcsolódó (érintett) szervezet az olyan, amely a tanúsító/registrláló szervezethez közös tulajdon vagy igazgatók, szerződéses megállapodás, közös név, nem hivatalos megállapodás révén vagy más módon kapcsolódik, hogy a kapcsolódó szervezetnek anyagi érdekeltsége van egy minősítés eredményében vagy lehetősége, hogy egy minősítés eredményét befolyásolja.
- G.2.1.27. A tanúsító/registrláló szervezet elemezze és dokumentálja a kapcsolatát az ilyen kapcsolódó szervezetekkel, hogy meghatározza az érdekütközés lehetőségét a tanúsítás/registrlálás megadásával kapcsolatban és meghatározza azokat a szervezeteket és tevékenységeket, amelyek megfelelő ellenőrzés hiányában befolyásolhatják a bizalmas kezelést, tárgyilagosságot vagy pártatlanságot.
- G.2.1.28. A tanúsító/registrláló szervezetek mutassák be, hogy hogyan irányítják tanúsítási/registrlálási üzletvitelüket és mindenféle más tevékenységüket, úgy, hogy kiküszöböljék a tényleges érdekütközést és a legkisebbre szorítsák a pártatlanság bármilyen kockázatát. A bemutatás az összes lehetséges érdekütközési forrást le kell fedje, akár a tanúsító/registrláló szervezettől, akár a kapcsolódó szervezetek tevékenységeiből származnak. Az akkreditáló testületek elvárják a tanúsító/registrláló szervezetektől, hogy ezeket a folyamatokat tárják fel az audit számára. Ez jelentheti azt, hogy gyakorlatilag elvégezhető és indokolt mértékben kövessék az audit naplóit, hogy átvizsgálják mind a tanúsító/registrláló szervezet, mind a kapcsolódó szervezet feljegyzéseit a szóban forgó tevékenység érdekében. Az ilyen auditnaplók terjedelmét tekintve számba kell venni a tanúsító/registrláló szervezet pártatlan tanúsításának/registrlálásának múltját. Ha bizonyítékot találnak a pártatlanság fenntartásának hiányára, szükséges lehet az audit visszafelé követése a kapcsolódó szervezetekhez, hogy biztosítékot nyújtsanak, hogy a lehetséges érdekütközés feletti ellenőrzést újból helyreállították.
- G.2.1.29. Az ISO/IEC Guide 62 2.1. és 2.2.3. szakaszának követelményei azt jelentik, hogy azok az emberek, akiknek tanácsot adtak, beleértve azokat, akik vezető állásban tevékenykednek nem alkalmazhatók a tanúsítási/registrlálási folyamat részét képező audit vezetésére, ha azok a szóban forgó szervezetben bármilyen tanácsadó tevékenységben részt vettek (vagy bármely a szervezethez kapcsolódó vállalatban) az utóbbi két évben. Az olyan helyzetek, amikor egy alkalmazó részvétele vagy korábbi részvétele a minősített szervezetnél azt jelentheti, hogy az egyének a tanúsítási/registrlálási folyamat bármely részében érdekütközéssel járó folyamatban részt vettek. A tanúsító/registrláló szervezet felelőssége, hogy az

ilyen helyzeteket megállapítsa és értékelje és kijelölje a felelősségeket és feladatokat, hogy biztosítsa, hogy a pártatlanság nem sérül.

- G.2.1.30. Az ISO/IEC Guide 62 2.1.2. szakaszában említett felső vezető, személyzet és/vagy törzskar nem kell szükségszerűen teljes munkaidejű legyen, de más alkalmazása nem veszélyeztetheti pártatlanságát.
- G.2.1.31. A tanúsító/registrláló szervezet követelje meg az összes minősítő alvállalkozótól vagy külső minősítőktől/auditoroktól, hogy kötelezettségeket vállaljanak bármilyen tanácsadási szolgáltatásnak a G.2.1.24. és G.2.1.25. szerintivel egyenértékű értékesítéshez.
- G.2.1.32. A tanúsító/registrláló szervezet felelős kell legyen, hogy biztosítsa, hogy sem a kapcsolódó szervezetek, sem az alvállalkozók, sem a külső minősítők/auditorok nem működnek a megígért kötelezettségük megszegésével. Felelős kell azért is legyen, hogy megfelelő helyesbítő intézkedést hajt végre, ha ilyen kötelezettségzegést állapítanak meg.
- G.2.1.33. A tanúsító/registrláló szervezet legyen független attól a szervezettől vagy szervezetektől (beleértve minden egyént), amelyek belső auditot vagy belső biztonsági átvizsgálást végeznek a szervezet ISMS-ében, amely tanúsítás/registrlálás alatt áll.
- G.2.1.34. Egy auditor meg kell magyarázza az audit megállapításait és/vagy tisztáznia kell a minősítő szabvány követelményeit az audit alatt és/vagy a záróértekezleten, de nem adhat előírás jellegű tanácsot vagy tanácsadást a minősítés részeként.
- G.2.1.35. Az ISO/IEC Guide 62 2.1.2. p) szakaszban hivatkozott eljárásrendek és eljárások biztosítsák, hogy az összes vitás kérdéseket és panaszokat építő módon és kellő idő alatt tárgyalják meg. Ha az ilyen eljárások működésének eredménye nem ad az ügyre elfogadható megoldást vagy ahol a javasolt eljárás elfogadhatatlan a panasztevő vagy más résztvevő felek számára, a tanúsító/registrláló szervezet eljárásai gondoskodjanak egy felszólalási folyamatról. A felszólalási eljárás tartalmazzon intézkedést a következőkre:

- a) lehetőség a kérelmező részére, hogy hivatalosan jelentse az esetet;
- b) egy független elemről vagy más eszközről való gondoskodás, hogy a felszólalási folyamat pártatlanságát biztosítsa;
- c) a felszólaló értesítése egy írásbeli határozattal a felszólalás megállapításairól, beleértve az elért döntések indokait.

A tanúsító/registrláló szervezet biztosítsa, hogy az érdekelt felekkel tudassák, ahogy és amikor megfelelő, a felszólalási folyamat létéről és a követendő eljárásokról.

2.1.3. Alvállalkozás

Ha egy tanúsító/registrláló szervezet elhatározza, hogy alvállalkozásba ad egy tanúsításra/registrlálásra vonatkozó munkát (pl. auditokat) egy külső szervezetnek vagy személynek, meg kell írnia a rendelkezéseket tartalmazó

dokumentált megegyezést, beleértve a bizalmas kezelést és az érdekütközést. A tanúsító/regisztráló szervezet

- a) teljes felelősséget kell vállaljon az ilyen alvállalkozói munkáért és fenn kell tartania felelősségét a tanúsítás/regisztrálás megadásáért, fenntartásáért, kiterjesztéséért, bővítéséért, szűkítéséért, felfüggesztéséért vagy visszavonásáért;
- b) biztosítania kell, hogy az alvállalkozó szervezet vagy személy felkészült legyen és megfeleljen e követelmény vonatkozatható rendelkezéseinek és alkalmazottján keresztül sem közvetlenül, sem közvetve nem vehet részt egy ISMS vagy kapcsolódó irányítási rendszer(ek) tervezésében, bevezetésében vagy fenntartásában, oly módon, hogy pártatlansága sérülhet;
- c) meg kell szerezni a kérelmező vagy a tanúsított/regisztrált szervezet egyetértését.

4. MEGJEGYZÉS: Az a) és b) követelmények kiterjesztve szintén vonatkoznak, amikor egy tanúsító/regisztráló szervezet saját tanúsítása/regisztrálása megadásához használ egy olyan másik tanúsító/regisztráló szervezet által teljesített munkát, amellyel egy megállapodást írt alá.

IAF útmutató

- G.2.1.36. Egy tanúsító/regisztráló szervezet kiadhat tanúsítványokat egy másik szervezet által végzett minősítés alapján, feltéve, hogy egy alvállalkozó szervezet megköveteli, hogy az ISO/IEC Guide 62 összes vonatkozó követelményének feleljen meg, vagy bármely más dokumenumnak, amely az akkreditálás alkalmazási területének megfelel, különösen az ISO/IEC Guide 62 2.2. szakasz követelményeinek. Az alvállalkozó szervezetek által végzett minősítések ugyanazt a biztonságot kell nyújtsák, mint azok a minősítések, amelyeket maga a tanúsító/regisztráló szervezet végzett. Az auditjelentés értékelését és a tanúsításra/regisztrálásra vonatkozó döntést csak maga a tanúsító/regisztráló szervezet végezheti, semmilyen más tanúsító/regisztráló szervezet nem. Ha közös minősítéseket végeznek, minden tanúsító/regisztráló szervezet meg kell győződjön, hogy a teljes minősítést felkészült minősítők/auditorok kellő módon vállalták.
- G.2.1.37. Amikor egy tanúsító/regisztráló szervezet tanúsítványokat bocsát ki a G.2.1.36. útmutatóval összhangban, legyenek eljárásai, amelyek megfelelést biztosítanak az alvállalkozó szervezet részéről e dokumentum minden vonatkozó szakaszával.

2.1.4. Minőségügyi rendszer

2.1.4.1. A tanúsító/regisztráló szervezet vezetősége, a minőség iránti végrehajtási felelősséggel, meg kell határozza és dokumentálja minőségpolitikáját, beleértve a minőségcélokat és elkötelezettségét a minőség iránt. A vezetőségnek

biztosítania kell, hogy ezt a politikát megértsék, bevezessék és fenntartsák a tanúsító/registrláló szervezet minden szintjén.

2.1.4.2. A tanúsító/registrláló szervezetnek olyan minőségügyi rendszert kell működtetnie, amely e közlemény vonatkozó elemeivel összhangban van és megfelel a végzett munka jellegének, terjedelmének és mennyiségének. Ezt a minőségügyi rendszert dokumentálni kell és ezt a dokumentációt elérhetővé kell tenni felhasználás céljából a tanúsító/registrláló szervezet személyzete részére. A tanúsító/registrláló szervezetnek gondoskodnia kell a dokumentált minőségügyi rendszer eljárásainak és utasításainak hatásos megvalósításáról. A tanúsító/registrláló szervezetnek ki kell jelölnie egy személyt, akinek közvetlen kapcsolata van a legfelső végrehajtó szinttel és aki – egyéb felelősségétől függetlenül – meghatározott hatáskörrel rendelkezzék ahhoz, hogy

- a) gondoskodjék e közleménynek megfelelő minőségügyi rendszer kialakításáról, bevezetéséről és fenntartásáról és**
- b) beszámoljon a tanúsító/registrláló szervezet vezetőségének a minőségügyi rendszer működéséről átvizsgálás és a minőségügyi rendszer jobbításának megalapozása céljából.**

2.1.4.3. A minőségügyi rendszert egy minőségügyi kézikönyvben és hozzá tartozó minőségügyi eljárásokban kell dokumentálni. A minőségügyi kézikönyvben legalább a következők legyenek vagy az utaljon a következőkre:

- a) minőségpolitikai nyilatkozat;**
- b) a tanúsító/registrláló szervezet jogállásának rövid leírása, beleértve a tulajdonosok nevét, ha ez értelmezhető, és az azt ellenőrző személyek nevét, ha ezek nem azonosak a tulajdonoséval;**
- c) a felső vezető és a tanúsító/registrláló tevékenység minőségét befolyásoló többi tanúsító/registrláló személyek neve, képzettsége, gyakorlata és hatásköre;**
- d) szervezeti vázlat, amely megmutatja a hatásköröket, a felelőségeket és a feladatkörök elosztását a felső vezetőtől kiindulva és különösen a kapcsolatot azok között, akik a minősítésért felelősek és tanúsítási/registrlálási döntést hoznak;**
- e) a tanúsító/registrláló szervezet szervezeti felépítésének leírása, beleértve a 2.1.2. c) szakasz szerinti vezetőség (bizottság, csoport vagy személy), az alapszabály, hatáskörök és eljárási szabályai részletezését;**
- f) a vezetőségi átvizsgálások végzésének politikája és eljárásai;**
- g) az adminisztratív eljárások, ezek között a dokumentumok kezelése;**
- h) a minőséggel kapcsolatos működési és feladatköri kötelezettségek és szolgáltatások úgy, hogy minden személy felelősségi körének terjedelme és határai ismertek legyenek minden érintett előtt;**

- i) a politika és eljárások a tanúsítási/regisztrálási szervezet személyzetének (beleértve az auditorokat) felvételi meghirdetésére, képzésére és teljesítésük figyelemmel kísérésére;
- j) a szervezet alvállalkozóinak jegyzéke és azok felkészültségének minősítésére, feljegyzésére és figyelemmel kísérésére vonatkozó részletes eljárások;
- k) a szervezet eljárásai a nemmegfelelések kezelésére és minden megtett helyesbítő intézkedés hatásosságának biztosítására;
- l) politika és eljárások a tanúsítási/regisztrálási folyamat bevezetésére, beleértve a következőket:
 - 1) a tanúsítási/regisztrálási dokumentumok kiadásának, fenntartásának és visszavonásának feltételeit,
 - 2) az ISMS tanúsítás/regisztrálás során alkalmazott dokumentumok használatának és alkalmazásának ellenőrzését,
 - 3) a szervezet ISMS-e minősítésének és tanúsításának/regisztrálásának eljárásait,
 - 4) a tanúsított/regisztrált szervezetek felügyeletére és újraminősítésére vonatkozó eljárásokat;
- m) a felszólalások, panaszok és vitás kérdések kezelésére vonatkozó politika és eljárások;
- n) a belső auditok végzésének az ISO 10011-1 szabvány rendelkezésein alapuló eljárásai.

IAF útmutató

G.2.1.38. Az ISO/IEC Guide 62 2.1.4.3. e) szakasz által megkívánt leírás tartalmazzon egy utalást, hogy melyik felet vagy feleket képviseli a bizottság minden tagja, csoport vagy személy.

2.1.5. A tanúsítás/regisztrálás megadásának, fenntartásának, kiterjesztésének, szűkítésének, felfüggesztésének és visszavonásának feltételei

2.1.5.1. A tanúsító/regisztráló szervezetnek elő kell írnia a tanúsítás/regisztrálás megadására, fenntartására, szűkítésére és kiterjesztésére vonatkozó, továbbá azon feltételeket, amelyek esetén a tanúsítás/regisztrálás részben vagy teljes egészében felfüggeszthető vagy visszavonható a szervezet tanúsítási/regisztrálási területe teljes egészében vagy részében. A tanúsító/regisztráló szervezet különösen arra kell kérje a (tanúsítandó) szervezetet, hogy azonnal értesítse őt az ISMS-ben tervezett vagy más módosításról, amelyek a megfelelőséget befolyásolhatják.

2.1.5.2. A tanúsító/regisztráló szervezet követelje meg a szervezettől, hogy legyen egy dokumentált és bevezetett ISMS rendszere, amely megfelel az ISMS szabványoknak vagy más rendelkező dokumentumoknak.

2.1.5.3. A tanúsító/regisztráló szervezetnek legyenek eljárásai:

- a) a tanúsítás/regisztrálás megadására, fenntartására, visszavonására, és ha ez értelmezhető, felfüggesztésére;
- b) a tanúsítás/regisztrálás területének kiterjesztésére vagy szűkítésére;
- c) új minősítés végzésére abban az esetben, amikor olyan módosítások történnek, amelyek jelentősen befolyásolják a szervezet tevékenységét és működését (mint pl. tulajdonosváltás, változások a személyzetben vagy berendezésekben) vagy ha egy panasz vagy bármely más információ elemzése azt mutatja, hogy a tanúsított/regisztrált szervezet már nem felel meg a tanúsító/regisztráló szervezet követelményeinek.

2.1.5.4. A tanúsító/regisztráló szervezetnek legyenek kérésre hozzáférhető dokumentált eljárásai a következőkre:

- a) egy szervezet ISMS-ének első minősítésére az ISO 10011-1 és más vonatkozó dokumentumok rendelkezéseivel összhangban;
- b) egy szervezet ISMS-ének időszakosan ismétlődő felügyeletére és újraminősítésére az ISO 10011-1 intézkedései szerint, hogy az folyamatosan megfeleljen a rá vonatkozó követelményeknek, továbbá annak igazolására és feljegyzésére, hogy egy szervezet időben helyesbítő intézkedéseket tesz minden nemmegfelelés kijavítására;
- c) a nemmegfeleléseknek és a szervezet által végzendő helyesbítő intézkedéseknek időben való megállapítására és feljegyzésére olyan kérdéseket illetően, mint helytelen hivatkozások a tanúsításra/regisztrálásra vagy a tanúsítási/regisztrálási információ félrevezető használata.

IAF útmutató

G.2.1.39. A tanúsítási/regisztrálási döntés kérdésében az ISO/IEC Guide 62 2.1.5. szakasza nem említ meghatározott időszakot, amely alatt egy teljes belső auditot és egy vezetőségi átvizsgálást és egy biztonsági átvizsgálást a szervezet ISMS-ében végezni kell. A tanúsító/regisztráló szervezet előírhat egy időszakot. Függetlenül attól, hogy a tanúsító/regisztráló szervezet választott egy minimális időköz-előírást, a tanúsító/regisztráló szervezet intézkedéseket kell tegyen, hogy biztosítsa a szervezet vezetőségi átvizsgálása, biztonsági átvizsgálása és a belsőaudit-folyamatok hatásosságát.

G.2.1.40. Tanúsítást/regisztrálást nem szabad a szervezetnek megadni, amíg nincs kellő igazoló bizonyíték, hogy az intézkedéseket a vezetőségi és biztonsági átvizsgálásokra bevezették, azok hatásosak és meg fogják azokat tartani.

2.1.6. Belső auditok és vezetőségi átvizsgálások

2.1.6.1. A tanúsító/registrláló szervezet végezzen időszakosan ismétlődő belső auditokat, amelyek tervezetten és módszeresen terjedjenek ki minden eljárásra, annak igazolására, hogy a minőségügyi rendszert bevezették és az hatásos. A tanúsító/registrláló szervezet gondoskodjon arról, hogy:

- a) az auditált területért felelős személyzet tájékoztatva legyen az audit eredményéről;
- b) a helyesbítő tevékenységet időben és megfelelő módon elvégezték;
- c) az audit eredményeit feljegyezték.

2.1.6.2. A szervezet végrehajtói felelősséggel rendelkező vezetősége a minőségügyi rendszert meghatározott időközökben vizsgálja át. Ez legyen elég ahhoz, hogy biztosítsa annak folyamatos alkalmasságát és hatásosságát ezen irányelv követelményei, a kitűzött minőségpolitika és célok teljesítéséhez. Ezeknek az átvizsgálásoknak a feljegyzéseit meg kell őrizni.

IAF útmutató

G.2.1.41. Az ISO/IEC Guide 62 2.1.6. szakasza nem említi egy meghatározott időszakot, amely alatt egy teljes belső auditot a tanúsító/registrláló szervezet minőségügyi rendszerében és ugyanott egy vezetőségi átvizsgálást el kell végezni. A szervezet minőségügyi rendszerének egy teljes belső auditját, az azt követő vezetőségi átvizsgálással legalább évente célszerű végezni. Az akkreditáló testület rövidebb időszakot írhat elő az ISO/IEC Guide 62 követelményeinek való megfelelés fokától függően, ahogy azok a belső auditokban és átvizsgálásokban, valamint az akkreditáló testület jelentéseiben található.

G.2.1.42. A belső auditok és vezetőségi átvizsgálások feljegyzéseit kérésre az akkreditáló testület számára elérhetővé kell tenni.

2.1.7. Dokumentáció

2.1.7.1. A tanúsító/registrláló szervezet dokumentálja, rendszeres időközökben korszerűsítse és kérésre tegye elérhetővé (kiadványokon, elektronikus médian keresztül vagy más módon) a következőket:

- a) információt arról, hogy mely hatóság felügyelete alatt működik a tanúsító/registrláló szervezet;
- b) dokumentált nyilatkozatot a tanúsító/registrláló rendszeréről, beleértve a tanúsítás/registrlálás megadására, fenntartására, kiterjesztésére, szűkítésére, felfüggesztésére és visszavonására vonatkozó szabályait és eljárásait;
- c) információt a minősítési és tanúsítási/registrlálási folyamatról;

- d) azoknak az eszközöknek a leírását, amelyek révén a tanúsító/regisztráló szervezet pénzügyi támogatást kap és általános információt a kérelmezőket és tanúsított/regisztrált szervezeteket terhelő díjakról;
- e) a kérelmezők és tanúsított/regisztrált szervezetek jogainak és kötelezettségeinek leírását, beleértve a tanúsító/regisztráló szervezet emblémájának alkalmazására vonatkozó követelményeket, megszorításokat vagy korlátozásokat és azokat a módokat, ahogyan az elnyert tanúsításra/regisztrálásra hivatkozni lehet;
- f) információt a panaszok és felszólalások, vitás kérdések folyamatairól;
- g) a tanúsított/regisztrált szervezetek címjegyzékét, amely tartalmazza telephelyüket, leírva mindegyikük esetén a megadott tanúsítás/regisztrálás területét.

2.1.7.2. A tanúsító/regisztráló szervezetnek eljárásokat kell kidolgoznia és fenntartania a tanúsítási/regisztrálási feladatkörre vonatkozó összes dokumentum és adat kezelésére. Ezeket a dokumentumokat megfelelés szempontjából kellően meghatalmazott és felkészült személyzetnek kell átvizsgálnia és jóváhagynia, minden dokumentum kiadása előtt, a kezdeti kialakítás vagy azt követő változtatás vagy módosítás után. Az összes megfelelő dokumentum jegyzékét a hozzátartozó kiadási és/vagy módosítási állapot megadásával meg kell őrizni. Az összes ilyen dokumentum elosztását szabályozni kell, hogy a megfelelő dokumentáció elérhető legyen a tanúsító/regisztráló szervezet vagy a (tanúsítandó) szervezet számára, ha szükséges egy kérelmező vagy a tanúsított/regisztrált szervezet tevékenységeire vonatkozó bármilyen teendő elvégzéséhez.

IAF útmutató

G.2.1.43. Az ISO/IEC Guide 62 2.1.7. d) szakaszban hivatkozott eszközök leírása, amellyel a szervezet pénzügyi támogatást kap, ahhoz kell elegendő legyen, hogy megmutassa, hogy a szervezet meg tudja-e őrizni pártatlanságát vagy nem.

2.1.8. Feljegyzések

2.1.8.1. A tanúsító/regisztráló szervezet tartson fenn olyan feljegyzési rendszert, amely megfelel sajátos körülményeinek és az érvényes jogszabályoknak. A feljegyzések igazolják, hogy a tanúsítási/regisztrálási eljárásokat hatáson elvégezték, különös tekintettel azokra a kérelmezési formanyomtatványokra, minősítési jelentésekre és más dokumentumokra, amelyek a tanúsítás/regisztrálás megadására, fenntartására, kiterjesztésére, szűkítésére, felfüggesztésére vagy visszavonására vonatkoznak. A feljegyzéseket úgy kell azonosítani, kezelni és selejtezni, hogy biztosítva legyen a folyamat tisztességes elvégzése és az információ bizalmas kezelése. A feljegyzéseket bizonyos ideig meg kell őrizni úgy, hogy a folyamatos bizalmas kezelést igazolni lehessen legalább egy teljes tanúsítási/regisztrálási időszakra vagy a törvény által megkövetelt időre.

2.1.8.2. A tanúsító/regisztráló szervezetnek legyen politikája és eljárásai, amelyek szerint a feljegyzéseket szerződéses, jogi vagy más kötelezettségeinek megfelelően megőrzi. A tanúsító/regisztráló szervezetnek legyen politikája és legyenek eljárásai, amelyek szerint ezekhez a feljegyzésekhez a 2.1.9. szakasznak megfelelően hozzá lehet férni.

2.1.9. Bizalmas kezelés

2.1.9.1. A tanúsító/regisztráló szervezetnek legyenek a vonatkozó törvényekkel összhangban álló megfelelő intézkedései abból a célból, hogy szervezetének minden szintjén megtartsák a tanúsítási/regisztrálási tevékenységek során szerzett információk bizalmas kezelését, beleértve a bizottságokat és azokat a külső szervezeteket vagy egyéneket, amelyek vagy akik a szervezet nevében eljárnak.

2.1.9.2. Az e közleményben megkövetelt esetek kivételével egy adott szervezetre vonatkozó információt nem szabad egy harmadik féllel közölni a szervezet írásbeli engedélye nélkül. Ha a törvény megköveteli, hogy egy harmadik féllel információt kell közölni, a szervezetet tájékoztatni kell a törvény által megengedett információ közléséről.

IAF útmutató

G.2.1.44. A bizalmas kezelésre vonatkozó követelmény mindenkit érint, aki információhoz hozzájuthat, amit a tanúsító/regisztráló szervezet bizalmasan kell kezeljen. Az alvállalkozó személyzetét meg kell kérni, hogy minden ilyen információt bizalmasan kezeljen, különösen az alkalmazott munkatársaktól és más alkalmazóitól származókat.

G.2.1.45. Az ISO/IEC Guide 62 2.1.9.2. szakaszban említett „írásbeli engedély” csak a bizalmas jellegű információra vonatkozik.

2.2. A tanúsító/regisztráló szervezet személyzete

2.2.1. Általános előírás

2.2.1.1. A tanúsító/regisztráló szervezet tanúsításba/regisztrálásba bevont személyzete legyen felkészült az általa végzett feladatok betöltésére.

2.2.1.2. A tanúsítási/regisztrálási folyamatba bevont személyzet minden tagjának a tárgyra vonatkozó képzettségére, képzésére és gyakorlatára vonatkozó információt a tanúsító/regisztráló szervezetnek meg kell őriznie. A képzésre és gyakorlatra vonatkozó feljegyzéseket naprakészen kell tartani.

2.2.1.3. Egyértelműen dokumentált utasításoknak kell a személyzet rendelkezésére állniuk, amelyek leírják kötelezettségeiket és feladataikat. Ezeket az utasításokat naprakészen kell tartani.

IAF útmutató

- G.2.2.1. Az ISO/IEC Guide 62 2.1.2. j) szakasza azt jelenti, hogy a teljes akkreditált szakterületén (vagy azon a területen, ahol működik) a tanúsító/registrláló szervezet képes kell legyen minősítések végzésére a saját ellenőrzés alatt álló erőforrásokot felhasználva, melyeknek teljesíteniük kell az ISO 10011 követelményeit és a vonatkozatható ágazati alrendszereket.
- G.2.2.2. A „saját ellenőrzése alatt álló erőforrások” kifejezés magába foglalhatja az egyéni minősítőket/auditorokat, akik szerződéses alapon dolgoznak a tanúsító/registrláló szervezetnek, vagy más külső erőforrásokot. A tanúsító/registrláló szervezet olyan helyzetben legyen, hogy irányítsa, ellenőrizze és legyen felelős az összes erőforrásai teljesítményéért és tartson fenn átfogó feljegyzéseket, amelyek ellenőrzik az egyes területeken alkalmazott személyzet egészének alkalmasságát, akár alkalmazottak, szerződéses alkalmazottak vagy külső szervezetek bocsátják rendelkezésre.
- G.2.2.3. A tanúsító/registrláló szervezet vezetőségének legyenek erőforrásai, amelyek képessé teszik, hogy meghatározza, hogy az egyéni minősítő/auditorok felkészültek-e azokra a feladatokra, amelyeket tőlük megkívánnak, hogy elvégezzék azon a tanúsítási/registrlási területen, amelyen működnek és eljárásaik, hogy ezt biztosítsák. A minősítő/auditorok felkészültségét létre lehet hozni igazolt háttér tapasztalattal és külön képzéssel vagy tájékoztatással (amelyet ki lehet mutatni egy akkreditált auditor tanúsító/registrláló szervezet által ISMS auditorként való registrlással). A tanúsító/registrláló szervezet tudjon hatásosan kommunikálni mindazokkal, akiknek szolgáltatásait használja.
- G.2.2.4. A tanúsító/registrláló szervezeteknek olyan személyzete legyen, amely felkészült:
- az audit számára megfelelő auditsoportok ISMS auditorainak kiválasztására és felkészültsége igazolására;
 - az ISMS auditorok tájékoztatására és a szükséges képzés megrendezésére;
 - döntésre a tanúsítás/registrlálás megadására, fenntartására, visszavonására, felfüggesztésére, kiterjesztésére vagy szűkítésére vonatkozóan;
 - egy felszólalási, panasz és vitás kérdés intézési eljárás összeállítására és működtetésére.

ISMS útmutató

IS.3 A vezetőség felkészültsége

IS.3.1 Általános rész

Ebben az útmutatóban a hangsúly a tanúsító/registrláló szervezet felkészültségére van helyezve, hogy az a tanúsítási/registrlási folyamatot irányítsa és vezesse. Az ISMS tanúsítás/registrlálás elvégzéséhez szükséges felkészültség alapvető elemei, hogy kiválasszák, szolgáltatassák és irányítsák azokat az egyéneket, akik kollektív felkészültsége megfelel azoknak a tevékenységeknek, amelyeket auditálni kell és a kapcsolódó információbiztonsági kérdések.

IS.3.2 Felkészültség elemzés és szerződés-átvizsgálás

A tanúsító/registrláló szervezetnek legyenek rendszerei, amelyek azon szervezetek ISMS-ére vonatkozó technológiai és jogi fejlődés ismeretét biztosítják, amelyeket minősít.

A tanúsító/registrláló szervezetnek legyen hatásos rendszere az információbiztonsági rendszerhez való azon felkészültségek elemzésére, amelyek számára elérhetők kell legyenek, tekintettel az összes műszaki területekre, amelyeken tevékenykedik.

A tanúsító/registrláló szervezetnek képessége legyen a vonatkozó szerződések átvizsgálására és tudja igazolni, hogy egy felkészültségi elemzést végzett (a készségek minősítése a kiértékelt igényekhez viszonyítva) minden vonatkozó ipari ágazat követelményeire, mielőtt a szerződés-átvizsgálást vállalta minden ügyfélre. A tanúsító/registrláló szervezet különösen legyen képes igazolni, hogy megvan a felkészültsége a következő tevékenységek végzésére:

- a) a jellegzetes információbiztonság azonosítása a vagyon veszélyeztetése, az ágazat tevékenységi területeinek a szervezetre vonatkozó hatásai és sebezhetőség szempontjából;
- b) a szervezet tevékenységi területeinek meghatározása;
- c) annak megerősítése, hogy a jellegzetes információbiztonsági vonatkozású vagyontárgy veszélyeztetés, szervezeti hatások, sebezhetőség, amelyek a szervezeti tevékenységek teljes köréből származnak, megfelelnek az előbbi a) szerint meghatározottaknak;
- d) a tanúsító/registrláló szervezetben szükséges felkészültségek meghatározása, hogy a meghatározott tevékenységek és a vagyontárgyak veszélyeztetésére, sebezhetőségre és a szervezetre való hatásokra vonatkozó információbiztonság tekintetében tanúsítani/registrlálni tudjon;
- e) a megkövetelt felkészültségek elérhetőségnek megerősítése.

IS.3.3 Képzés és az auditsoportok kiválasztása

A tanúsító/registrláló szervezetnek legyenek ismérvei az auditsoportok képzésére és kiválasztására, amely megfelelő szinteket biztosít:

- a) az ISMS szabvány vagy rendelkező dokumentum megértéséhez;
- b) az információbiztonság kérdéseinek megértéséhez;
- c) kockázatminősítés és kockázatkezelés megértéséhez;
- d) az auditált tevékenység műszaki ismeretéhez;
- e) az ISMS-re vonatkozó szabályozási követelmények ismeretéhez;
- f) irányítási-rendszerauditához való felkészültséghez;
- g) az irányítási rendszer ismeretéhez.

IS.3.4 A döntéshozó folyamat irányítása

Az irányítási feladatkörnek legyen meg a felkészültsége és megfelelő eljárásai, hogy irányítsák a döntéshozás folyamatát az ISMS tanúsítás/ regisztrálás megadására, fenntartására, kiterjesztésére, szűkítésére, felfüggesztésére és visszavonására.

2.2.2. Az auditorokra és műszaki szakértőkre vonatkozó képzettségi kritériumok

2.2.2.1. A tanúsító/regisztráló szervezetnek meg kell határozni a felkészültségre vonatkozó minimális ismérveket, hogy biztosítva legyen a minősítések hatásos és egységes elvégzése.

2.2.2.2. Az auditorok feleljenek meg a megfelelő nemzetközi dokumentáció követelményeinek. Az ISMS minősítéshez auditálási irányelvek található az ISO 10011-1 és az auditorokra az ISO 10011-2-ben.

2.2.2.3. A műszaki szakértőkre vonatkozóan nem követelmény, hogy megfeleljenek az ISO 10011-2 szerinti ismérveknek. A személyi tulajdonságaikra vonatkozó útmutatás az ISO 10011-2 7. fejezetében található.

ISMS útmutató

IS.4 Az auditor felkészültsége

A tanúsító/regisztráló szervezetek által ISMS audit elvégzésére alkalmazott személyek feleljenek meg az ISO 10011-2 szabványon alapuló következő ismérveknek. Ha az ISMS auditok elvégzésére alkalmaznak személyeket, ezeket a tulajdonságokat az IS.5.3-ban leírtak szerint fel lehet osztani a csoport tagjai között:

- a) képesítés egyetemi szinten (kiterjedt gyakorlat és kiegészítő szakmai képesítés és képzés egyenértékű lehet az ilyen szintű képesítéssel);
- b) legalább 4 éves teljes idejű munkahelyi gyakorlati tapasztalat információtechnikában/technológiában, ebből legalább 2 év az információbiztonság szerepkörben vagy feladatkörben;
- c) 5 napos képzés sikeres elvégzése auditálás és auditirányítás területén;
- d) mielőtt vállalja a felelősséget, hogy auditorként működjön, a jelöltnek már tapasztalatot kell szereznie az információbiztonság-minősítés teljes folyamatában. Ezt a tapasztalatot legalább négy minősítésben való részvétellel kell megszerezze, amely legalább összesen 20 napig tart, beleértve a dokumentáció-átvizsgálást és a kockázatelemzést, a bevezetés minősítését és jelentést az auditról;
- e) a vonatkozó tapasztalat ésszerű és időszerű legyen;
- f) legyenek meg a következő személyes tulajdonságok: tárgyilagos, megfontolt, jó ítélőképességű, jó elemzőképességű, állhatatos, valósághoz ragaszkodó. A jelölt legyen képes összetett műveletek megfogalmazására széles távlatban és legyen képes megérteni az egyedi egységek szerepét nagyobb szervezetekben;

- g) tartsa szinten saját ismereteit és jártasságát az információbiztonságban és az auditálásban.

A vezető auditorként működő auditor ezen túl a következő követelményeknek feleljen meg:

- h) legyen ismerete és tulajdonságai a minősítési folyamat irányítására;
- i) auditorkénti működés legalább 3 teljes ISMS auditban;
- j) bizonyítás, hogy megfelelő ismerete és tulajdonságai vannak, hogy a minősítő folyamatot irányítsa;
- k) képesség bizonyítása, hogy hatásosan tud kommunikálni, szóban és írásban is.

2.2.3. Kiválasztási eljárás

2.2.3.1. Az ISMS auditorok és műszaki szakértők auditsoportokba való választásának általános szempontjai

A tanúsító/registrláló szervezetnek legyen eljárása a következőkre:

- a) auditorok kiválasztása felkészültségük, képzettségük, képesítésük és gyakorlatuk alapján, amennyiben szükséges, az auditsoportot ki lehet egészíteni műszaki szakértőkkel, akik az auditnak megfelelő műszaki területen egyedi felkészültséget tudnak bemutatni. Figyelembe kell venni, hogy a műszaki szakértők nem alkalmazhatók ISMS auditorok helyett;
- b) az auditorok és műszaki szakértők minősítés alatti viselkedésének kezdeti minősítése és ezt követően az auditorok és műszaki szakértők teljesítményének figyelemmel kísérése.

IAF útmutató

- G.2.2.5. A 2.2.3.1. b) szakasz megkívánja, hogy a tanúsító/registrláló szervezet minősítse és figyelje az ISMS auditorok és műszaki szakértők viselkedését és teljesítményét. Ez a minősítés és figyelés foglalja magába a minősítők/auditorok és műszaki szakértők tevékenységének helyszíni tanúsító/registrláló szervezet általi megfigyelését (witnessing).

2.2.3.2. Adott minősítésre való kijelölés

Amikor a tanúsító/registrláló szervezet egy auditsoportot egy adott minősítéshez való kijelölésre kiválaszt, gondoskodjék arról, hogy minden kijelöléshez adott készségek megfelelők legyenek. A csoport:

- a) legyen jártas a vonatkozó jogi szabályozásokban, tanúsítási/registrlási eljárásokban és a tanúsítási/registrlási követelményekben;
- b) legyen alapos ismerete a vonatkozó minősítési módszerekben és minősítési dokumentumokban;

- c) **rendelkezzen megfelelő műszaki ismerettel azokra a meghatározott tevékenységekre vonatkozóan, amelyekre a tanúsítást/regisztrálást kérték és ha szükséges, ismerje a hozzá tartozó eljárásokat és a lehetőségeket, hogy információbiztonsági meghibásodást okoznak (ezt a feladatot műszaki szakértők is teljesíthetik, akik nem auditorok);**
- d) **rendelkezzen kellő ítélőképességgel, hogy megbízhatóan minősíteni tudja a szervezet felkészültségét, hogy tevékenységei, termékei és szolgáltatásai információbiztonsági szempontjait kezelni tudja;**
- e) **tudjon hatásosan kapcsolatot tartani a kívánt nyelveken szóban és írásban;**
- f) **legyen mentes minden érdektől, amely a csoport tagjait arra készíthetné, hogy ne pártatlanul és ne megkülönböztetésmentesen cselekedjenek, például:**
 - 1) **sem az auditcsoport tagjai, sem alkalmazója/alkalmazói nem végezhetnek tanácsadó szolgáltatást a kérelmező vagy a tanúsított/regisztrált szervezetnek, amely veszélyeztethetné a tanúsítási/regisztrálási folyamatot és döntést,**
 - 2) **a tanúsító/regisztráló szervezet irányelveinek megfelelően az auditcsoport tagjainak tájékoztatnia kell a tanúsító/regisztráló szervezetet bármely meglévő, korábbi vagy tervezett kapcsolatról egymás között vagy alkalmazóik/alkalmazójuk és a minősítendő szervezet között.**

IAF útmutató

- G.2.2.6. Az akkreditálás feltétele, hogy az akkreditált tanúsítványokat nem adják ki, amíg megfelelő erőforrások nem használhatók hatásosan az ISO/IEC Guide 62 és e dokumentum követelményeit teljesítő auditok végzésére. A tanúsító/regisztráló szervezet eljárásai biztosítsák, hogy a szervezetek minősítésére alkalmazott személyzet felkészült legyen azon a szakterületen, amelyen működik. Az auditok irányításáért felelős személyzetet azonosítani kell és felkészültségüket dokumentálni kell.
- G.2.2.7. Az ISO/IEC Guide 62 2.2.3.2. f) szakasz „irányelvek” szakkifejezése azonos értelmű, mint az ISO/IEC Guide 62 3.2.5. szerinti „megbízás”.
- G.2.2.8. Az auditcsoportnak meg kell legyen a háttérismerete, hogy biztosítsa, hogy a tagok megértik arra a rendszerre vonatkozó követelményeket, amelyet minősítenek. Minden auditcsoportnak legyen átfogó ismerete és alapjai minden technológiai és ipari ágazatban, ahol dolgozik.
- G.2.2.9. Bizonyos esetekben, különösen ahol kritikus követelmények és különleges eljárások vannak, az auditcsoport háttérismerete kiegészíthető tájékoztatással, külön képzéssel és/vagy műszaki szakértők jelenlétével. A tanúsító/regisztráló szervezet az auditcsoportokhoz nem auditor szakértőket csatolhat. Ha a

tanúsító/registrláló szervezet műszaki szakértőket alkalmaz, rendszereik tartalmazzák részletesen, hogy a műszaki szakértőket hogyan választják ki és műszaki ismeretüket folyamatosan hogyan biztosítják. A tanúsító/registrláló szervezet számíthat egy külső segítségre, pl. az iparból vagy a szakmai intézményektől.

G.2.2.10. Az ISO/IEC Guide 62 2.1. és 2.2.3.2. követelményeinek hatása van azoknak az embereknek az alkalmazására, akik tanácsadást végeznek. Lásd 2.1.29. útmutatót.

ISMS útmutató

IS.5 Az auditcsoport felkészültsége

IS.5.1 A következő követelmények vonatkoznak a tanúsítási/registrlási minősítésre. A felügyeleti tevékenységekre csak azok a követelmények vonatkoznak, amelyek a programozott felügyeleti auditra vonatkoznak.

IS.5.2 A következő követelmények vonatkoznak, a műszaki szakértőket kivéve, az auditcsoport minden tagjára:

az auditcsoport minden tagja tudja igazolni megfelelő tapasztalatát és az összes továbbiak megértését:

- a) az ISMS szabvány és rendelkező dokumentum;
- b) általánosságban az irányítási rendszerek elgondolásai;
- c) az információbiztonság különböző területeire vonatkozó témák;
- d) a kockázatminősítésre és kockázatkezelésre vonatkozó alapelvek és folyamatok;
- e) az auditálási alapelvek.

IS.5.3 A következő követelmények vonatkoznak az auditcsoport egészére:

a) az alábbi területek mindegyikén legalább egy auditcsoport tag feleljen meg a csoporton belüli felelősség vállalására vonatkozóan a tanúsító/ registrláló szervezet kritériumainak:

- i) a csoport irányítása,
- ii) a törvényes szabályozási követelmények ismerete és a jogi megfelelés a speciális információbiztonsági területen,
- iii) az információbiztonságra vonatkozó fenyegetések megállapítása,
- iv) a szervezet sebezhetőségének megállapítása, hatásának, mérséklésének és szabályozásának megértése,
- v) az ágazat korszerű műszaki színvonalának ismerete,
- vi) a kockázatminősítés ismerete az információbiztonsággal kapcsolatban;

- b) az auditsoport legyen felkészült, hogy a szervezeti ISMS-ben fellépő biztonsági váratlan eredmények jelzéseit visszavezesse az ISMS megfelelő elemeire;
- c) egy auditsoport állhat egy emberből, feltéve, hogy az az előbbi a)-ban kifejtett kritériumoknak megfelel.

IS.5.4 A műszaki szakértők alkalmazása

A szervezetet érintő folyamatra, információbiztonságra és törvényhozásra vonatkozó kérdésekben konkrét ismerettel rendelkező műszaki szakértők, akik azonban nem felelnek meg az előbbi összes követelménynek, részt vehetnek az auditsoportban. A műszaki szakértők nem működhetnek függetlenül.

2.2.4. A minősítő személyzet szerződtetése

A tanúsító/registrláló szervezet követelje meg a minősítésben részt vevő személyzettől, hogy írjanak alá egy szerződést vagy más dokumentumot, amelyben kötelezik magukat, hogy a tanúsító/registrláló szervezet által meghatározott szabályokat teljesítik, beleértve a bizalmas kezelést, a kereskedelmi és más érdekektől való függetlenséget, valamint a minősítésre kerülő szervezetekkel való korábbi és/vagy jelenlegi kapcsolatokat. A tanúsító/registrláló szervezetnek gondoskodnia kell és dokumentálnia kell, hogy minden szerződéses minősítő személy kielégítse e közleményben meghatározott, a minősítő személyzetre vonatkozó követelményeket.

2.2.5. A minősítő személyzetre vonatkozó feljegyzések

2.2.5.1. A tanúsító/registrláló szervezetnek legyenek naprakész feljegyzései a minősítő személyzetre, amely a következőkből álljon:

- a) név és cím;
- b) szervezethez való tartozás és beosztás;
- c) képzés és szakmai beosztás;
- d) gyakorlat és képzettség a tanúsító/registrláló szervezet felkészültségének minden területén;
- e) feljegyzések legutolsó korszerűsítésének időpontja;
- f) a teljesítés minősítése.

2.2.5.2. A tanúsító/registrláló szervezet gondoskodjon arról és igazolja, hogy minden alvállalkozó szervezet megtartja az e közlemény követelményeinek megfelelő minősítő szervezetre vonatkozó feljegyzéseket a tanúsító/registrláló szervezet alvállalkozóinál.

2.2.6. Eljárások az auditsoportok számára

Az auditsoportok legyenek ellátva naprakész minősítési utasításokkal és a tanúsítási/registrlási intézkedésekre és eljárásokra vonatkozó információval.

2.3. A tanúsítási/registrlási követelmények módosítása

A tanúsító/registrláló szervezetnek megfelelő értesítést kell adnia minden módosításról, amelyet a tanúsítási/registrlási követelményekben végezni kíván. Mielőtt dönt a módosítások pontos formájáról és hatálybalépési időpontjáról, figyelembe kell vennie az érdekelt felek által nyilvánított véleményeket. Miután döntést hozott a módosított követelményekről és közzétette azokat, igazolnia kell, hogy minden tanúsító/registrláló szervezet elvégezze az esetleg szükséges módosításokat eljárásaiban a tanúsító/registrláló szervezet véleménye szerint ésszerű időn belül.

2.4. Felszólalások, panaszok és viták

2.4.1. A szervezetek vagy más felek által a tanúsító/registrláló szervezethez benyújtott felszólalásokat, panaszokat, vitás kérdéseket a tanúsító/registrláló szervezet eljárásai szerint kell kezelni.

2.4.2. A tanúsító/registrláló szervezet

- a) vezessen feljegyzést minden, a tanúsításra/registrlásra vonatkozó felszólalásról, panaszról és vitás kérdéstről és a javító intézkedéstről;**
- b) végezzen megfelelő helyesbítő és megelőző intézkedést;**
- c) dokumentálja a megtett intézkedéseket és minősítse azok hatásosságát.**

IAF útmutató

G.2.4.1. A panaszok információforrást képviselnek a lehetséges nemmegfelelések szempontjából. A tanúsító/registrláló szervezet a panasz átvételekor állapítsa meg a nemmegfelelés okát, és ahol szükséges, tegyen intézkedést, beleértve bármely előre meghatározó (vagy hajlamosító) tényezőt a tanúsító/registrláló szervezet irányítási rendszerében.

G.2.4.2. A tanúsító/registrláló szervezet végezzen vizsgálatot, hogy javító/helyesbítő intézkedést dolgozzon ki, amelyben lépések legyenek:

- a) a tanúsítás/registrlálás lehető leggyorsabban megvalósítható helyreállítására;
- b) a megisméltődés elkerülésére;
- c) a javító/helyesbítő elfogadott intézkedések hatásosságának minősítésére.

3. FEJEZET: TANÚSÍTÁSI/REGISZTRÁLÁSI KÖVETELMÉNYEK

3.1. A tanúsítás/regisztrálás kérelmezése

3.1.1. Információ az eljárásról

3.1.1.1. A 2.1.7.1. szakasz előírásai szerint naprakész állapotban kell tartani egy részletes leírást a tanúsítási/regisztrálási eljárásról, a tanúsítási/regisztrálási követelményeket tartalmazó dokumentumokat és a tanúsított/regisztrált szervezetek jogait és kötelezettségeit leíró dokumentumokat és ezeket a kérelmezők és a tanúsított/regisztrált szervezetek rendelkezésére kell bocsátani.

3.1.1.2. A tanúsító/regisztráló szervezet követelje meg, hogy egy szervezet

- a) mindig feleljen meg a tanúsítási/regisztrálási program/alrendszer rá vonatkozó rendelkezéseinek;**
- b) tegyen meg minden szükséges intézkedést a minősítés elvégzéséhez, beleértve a dokumentáció vizsgálatra vonatkozó intézkedést és az összes területhez való hozzáférést, a feljegyzéseket (beleértve a belső auditfeljegyzéseket és az információbiztonság független átvizsgálási jelentéseit) és személyzetet a minősítés, az újraminősítés és a panaszok elintézése céljából.**

ISMS útmutató

IS.6 Hozzáférés a személyzeti feljegyzésekhez

A tanúsító/regisztráló szervezet vizsgálja át a minősítés előtt, hogy mely feljegyzések tekintendők bizalmas jellegűnek vagy kényesnek a szervezet részéről úgy, hogy ezeket a feljegyzéseket ne tudja vizsgálni az auditscsoport a szervezet minősítése során. A tanúsító/regisztráló szervezet ítélje meg, hogy a vizsgálható feljegyzések biztosítják-e a hatásos minősítést. Ha a tanúsító/regisztráló szervezet arra a következtetésre jut, hogy a hatásos minősítés nem biztosított, a tanúsító/regisztráló szervezet informálja a szervezetet, hogy a minősítés csak akkor történhet, ha a szervezet elfogadott megfelelő hozzáférési intézkedéseket.

- c) csak azokra a tevékenységekre állítsa, hogy tanúsították/regisztrálták, amelyekre tanúsítást/regisztrálást kapott;**
- d) ne használja a tanúsítást/regisztrálást úgy, hogy az a tanúsító/regisztráló szervezetet rossz hírbe hozza és ne tegyen semmiféle olyan kijelentést tanúsított/regisztrált voltára vonatkozóan, amelyet a tanúsító/regisztráló szervezet félrevezetőnek vagy illetéktelennek ítélhet;**
- e) tanúsításának/regisztrálásának felfüggesztése vagy visszavonása esetén (bárhogy nevezik is ezt) hagyjon fel minden hirdetéssel, amely bármiféle hivatkozást tartalmaz erre vonatkozóan, és küldjön vissza minden**

tanúsítási/registrlási dokumentumot, amelyet tanúsító/registrláló szervezet kér;

- f) a tanúsítást/registrlást csak annak jelzésére használja, hogy az ISMS megfelel az előírt szabványoknak vagy más rendelkező dokumentumnak, és nem használja tanúsítását/registrlását, hogy olyan benyomást keltsen, hogy a tanúsító/registrláló szervezet egy terméket vagy szolgáltatást hagyott jóvá;
- g) biztosítja, hogy semmilyen tanúsítási/registrlási dokumentumot, jelet vagy jelentést, sem azok valamely részét nem használja félrevezető módon;
- h) ha tanúsítására/registrlására hivatkozik a hírközlési médiában mint pl. dokumentumok, füzetek vagy hirdetés útján, ez feleljen meg a tanúsító/registrláló szervezet követelményeinek.

3.1.1.3. Ha a tanúsító/registrláló szervezet megkívánt szakterülete egy meghatározott programhoz/alrendszerhez tartozik, a kérelmezőnek meg kell adni minden szükséges magyarázatot.

3.1.1.4. Ha megkívánják, a kérelmezőnek kiegészítő kérelmezési információt kell adni.

3.1.2. A kérelem

3.1.2.1. A tanúsító/registrláló szervezet követelje meg egy hivatalos kérelmezési formanyomtatvány megfelelő kitöltését, a kérelmező szabályosan felhatalmazott képviselőjének aláírásával ellátva, amelyben vagy amelyhez csatolva:

- a) meghatározott a kívánt tanúsítás/registrlálás szakterülete;
- b) a kérelmező egyetért, hogy a tanúsító/registrláló szervezet követelményeinek megfelel és hogy szolgáltat bármely információt, amely a kiértékeléséhez szükséges.

3.1.2.2. A kérelmezőnek a helyszíni minősítés előtt legalább a következő információt kell rendelkezésre bocsátania:

- a) a kérelmező általános jellemzőit, mint a szervezeti egység megadását, nevet, címet, jogállást és ha vonatkoztható, az emberi és műszaki erőforrásokat;
- b) az ISMS-re vonatkozó általános információt és az abban foglalt tevékenységeket;
- c) a tanúsítandó/registrlándó rendszerek leírását és szabványokat vagy más rendelkező dokumentumokat;
- d) az ISMS kézikönyvének egy példányát és ha megkívánják, a hozzá tartozó dokumentációt.

A kérelmezési dokumentációból és az ISMS dokumentumainak átvizsgálásából összegyűjtött információt fel lehet használni a helyszíni minősítés előkészítéséhez és megfelelő módon bizalmasan kell kezelni.

3.2. Felkészülés a minősítésre

- 3.2.1.** A minősítés végzése előtt a tanúsító/regisztráló szervezet végezze el a tanúsítási/regisztrálási kérelem átvizsgálását és tartsa meg az erre vonatkozó feljegyzéseket, hogy biztosítsa, hogy
- a) a tanúsítás/regisztrálás követelményei egyértelműen legyenek meghatározva, dokumentálva és ezeket értsék meg;
 - b) a tanúsító/regisztráló szervezet és a kérelmező közötti értelmezési különbséget oldják fel;
 - c) a tanúsító/regisztráló szervezetnek legyen meg a képessége a tanúsítási/regisztrálási szolgáltatás elvégzésére, tekintetbe véve a kívánt tanúsítás/regisztrálás szakterületét, a kérelmező tevékenységi helyét és bármely sajátos követelményt, mint pl. a kérelmező által használt nyelvet.
- 3.2.2.** A tanúsító/regisztráló szervezet készítsen tervet minősítő tevékenységei végzésére, hogy lehetővé váljon a szükséges intézkedések elvégzése.
- 3.2.3.** A tanúsító/regisztráló szervezet jelöljön ki egy képesített auditscsoportot a kérelmezőtől begyűjtött összes anyag kiértékelésére és az auditnak a szervezet részéről való elvégzésére. A minősítendő terület szakértőit a tanúsító/regisztráló szervezet csoportjához fel lehet venni tanácsadóként.
- 3.2.4.** A szervezetet tájékoztatni kell a minősítést végző auditscsoport tagjainak nevééről, kellően figyelmeztetve arra, hogy bármelyik auditor vagy szakértő kijelölése ellen fellebbezni lehet.
- 3.2.5.** Az auditscsoportot hivatalosan ki kell jelölni és el kell látni megfelelő munkadokumentumokkal. A szervezettel egyeztetni kell az audittervet és időpontját. Az auditscsoportnak adott megbízást egyértelműen meg kell határozni és tudatni kell a szervezettel. Meg kell kívánni az auditscsoporttól, hogy vizsgálja meg a szervezet szervezeti felépítését, eljárásrendjeit és eljárásait, és igazolni kell, hogy ezek a tanúsítás/regisztrálás szakterületére vonatkozó összes követelményt teljesítik, az eljárásokat bevezették és azok olyanok, hogy bizalmat keltenek a szervezet ISMS-ében.

ISMS útmutató

IS.7 Alkalmazhatósági Nyilatkozat

A kérelmező dolgozzon ki egy Alkalmazhatósági Nyilatkozatot, amely leírja, hogy az ISMS szabvány vagy előíró dokumentum mely részei vonatkoznak és alkalmazhatók a szervezet ISMS-ére. Ez az Alkalmazhatósági Nyilatkozat legyen az auditscsoportnak átadott munkadokumentumok része.

3.3. Minősítés

Az auditscsoport minősítse a meghatározott szakterülethez tartozó szervezeti ISMS rendszert az összes rá vonatkoztatható tanúsítási/regisztrálási követelmény szempontjából.

IAF útmutató

- G.3.3.1. A tanúsító/registrláló szervezet elegendő időt hagyjon az auditoroknak, hogy egy minősítésre vagy újraminősítésre vonatkozó minden tevékenységet elvégezzék. A kijelölt időt olyan tényezőkre kell alapozni, mint a szervezet nagysága, a telephelyek száma és a tanúsításra/registrlásra vonatkozó szabványok. A tanúsító/registrláló szervezet legyen felkészült, hogy bizonyítsa vagy indokolja az egyes minősítésekre, felügyeletre vagy újraminősítésre felhasznált időt.

ISMS útmutató

IS.8 A tanúsítás/registrlálás alkalmazási területe

A szervezet az ISMS-e alkalmazási területét határozza meg. A tanúsító/registrláló szervezet szerepe, hogy egyöntetűséget hozzon létre, biztosítva, hogy a szervezetek ne zárják ki ISMS alkalmazási területükből működésük olyan ISMS elemeit, amelyeknek helyesen befoglalva kellene lenniük abba.

A tanúsítási/registrlási szervezeteknek ezért biztosítaniuk kellene, hogy a szervezet információbiztonsági kockázaminősítése helyesen tükrözze tevékenységeit és terjessze ki a tevékenysége határára, ahogy az az ISMS szabványban vagy rendelkező dokumentumban meghatározott. A tanúsító/registrláló szervezetek meg kell erősítsék, hogy ez a szervezet Alkalmazhatósági Nyilatkozatában tükröződik.

A szolgáltatások vagy tevékenységek érintkezési felületeivel (interfészek), amelyek nincsenek teljesen az ISMS alkalmazási területén belül, az ISMS-en belül kell foglalkozni a tanúsításnak/registrlásnak alárendelve és a szervezet információbiztonsági kockázatminősítésébe kell befoglalni. Ilyen helyzetre példa a berendezések (pl. számítógépek, távközlési rendszerek) megosztása másokkal.

IS.8.1 Többszörös helyszínek

A többszörös mintavételi döntések az ISMS tanúsítás/registrlálás területén összetettebbek, mint ugyanezek a döntések a minőségügyi rendszerek esetében. A tanúsítási/registrlási szervezetek, amelyek mintavételen alapuló megközelítést kívánnak alkalmazni többszörös helyszíni minősítési igényeikhez, fenn kell tartásuk az eljárásokat, amelyek a következő teljes kérdéstartományt magukba foglalják a mintavételi programjuk felépítésekor.

Mielőtt az első mintavételen alapuló minősítésbe belefognak, a tanúsító/registrláló szervezet az akkreditáló testületnek át kell adja az általa használt módszertant és eljárásokat és igazolható bizonyítékot kell nyújtsanak, hogy ezek hogyan veszik figyelembe az alábbi kérdéseket, hogy a többszörös helyszíni ISMS minősítést irányítsák.

A tanúsító/registrláló szervezetnek az eljárásai biztosítsák, hogy a kezdeti szerződés-átvizsgálás a lehető legnagyobb mértékben meghatározza a helyszínek

közi különbséget, hogy megfelelő mintavételi szintet határozzanak meg az alábbi intézkedésekkel összhangban.

Ha egy szervezetnek számos hasonló helyszíne van, amelyre egy ISMS vonatkozik, lehet egy tanúsítványt kiadni a szervezetnek az összes ilyen helyszínre, feltéve, hogy:

- a) minden helyszín ugyanazon ISMS szerint működik, amelyet központilag adminisztrálnak és auditálnak és központi vezetőségi átvizsgálás alá tartozik;
- b) az összes helyszínt a szervezet belső biztonsági átvizsgálási eljárása(i)val összhangban auditálták;
- c) a tanúsító/registrláló szervezet a helyszínek reprezentatív számát mintavételezte, figyelembe véve az alábbi követelményeket:
 - i) a központi iroda és a helyszínek belső auditjainak eredményei,
 - ii) a vezetőségi átvizsgálás eredményei,
 - iii) a telephelyek méretének változásai,
 - iv) a helyszínek üzleti céljainak változásai,
 - v) az ISMS összetettsége,
 - vi) a különböző helyszíneken levő információrendszerek összetettsége,
 - vii) változatok a munkamódszerekben,
 - viii) változatok a vállalt tevékenységekben,
 - ix) lehetséges kölcsönhatás kritikus információrendszerekkel vagy érzékeny információt feldolgozó információs rendszerekkel,
 - x) eltérő jogi követelmények;
- d) a minta célszerűen részben szelektív legyen, az előbbi c) pontra alapozva és részben nem szelektív és célszerűen különböző helyszínek tartományát eredményezze, amelyet úgy választanak, hogy a helyszínválasztás véletlenszerű elemét ne zárja ki;
- e) minden helyszínt, amely az ISMS-hez tartozik és jelentős vagyoni veszélyeztetésnek, sebezhetőségnek vagy behatásnak van kitéve, a tanúsító/registrláló szervezet auditálja a tanúsítás/registrlálás előtt;
- f) a felügyeleti programot célszerű az előbb említett követelményeknek megfelelően tervezni és ésszerű időn belül a szervezet összes helyszínét vagy az ISMS tanúsítási/registrlási alkalmazási területét fedje az Alkalmazhatósági Nyilatkozat keretében;
- g) ha nemmegfelelést figyelnek meg akár a központi irodában, akár egy bizonyos helyszínen, a helyesbítő beavatkozási eljárás vonatkozzék a központi irodára és a tanúsítás/registrlálás területén minden helyszínen.

Az IS.9-ben a következőkben leírt audit célszerűen foglalkozzék a szervezet központi irodai tevékenységeivel, hogy biztosítsa, hogy egyetlen ISMS

vonatkozik minden helyszínre és központi irányítást ad az operatív szinten. Az auditnak foglalkoznia kell az összes előbb kifejtett témával.

IS.9 Az audit módszertana

Egy tanúsító/registrláló szervezet egy szervezet ISMS-ének auditját a szervezet helyszínén/helyszínein legalább két lépésben kell végezze, hacsak egy alternatív megközelítést nem tud igazolni. A tanúsítási/ registrlási folyamat hozzáigazítása az igen kis szervezetek igényeihez speciális körülmények között indoklást adhat. Ezen útmutató céljára két fokozatot írnak le, mint 1. fokozatú audit és 2. fokozatú audit. Mindegyik fő célját, együtt a minimális terjedelemmel, alább írjuk le.

A tanúsító/registrláló szervezetnek ajánlatos, hogy legyenek eljárásai, amelyek azt kívánják, hogy képes legyen az audit kezdete előtt bizonyítani, hogy a belső biztonsági átvizsgálási folyamat programozva van és a program és az eljárások kivitelezhetők legyenek és kimutatható legyen, hogy kivitelezhetők.

Megjegyzés: az audit tárgyában lásd az IAF útmutatót is a tanácsadásra (G.2.1.10-G.2.1.33. fentebb).

IS.9.1 1. fokozatú audit

Az auditnak ebben a fokozatában ajánlatos, hogy a tanúsító/registrláló szervezet kapjon az ISMS tervezésére dokumentációt, amely legalább a szervezet információbiztonsági elemzését tartalmazza a kockázatra, az Alkalmazhatósági Nyilatkozatra és az ISMS alapelemeire vonatkozóan.

Az 1. fokozatú audit céljai, hogy egy középpontot nyújtsanak a 2. fokozatú audit tervezésére, hogy az ISMS megértését ériék el, a szervezet biztonságpolitikája és céljai és különösen a szervezet auditra való felkészültsége állásának összefüggésében.

Az 1. auditfokozat tartalmazza a dokumentum-átvizsgálást, de nem kell arra korlátozódjék. A tanúsító/registrláló szervezet és maga a vállalat meg kell egyezzenek, hogy mikor és hol végzik el a dokumentum-átvizsgálást. A dokumentum-átvizsgálást a 2. fokozatú audit megkezdése előtt mindenkor be kell fejezni.

Az 1. auditfokozat eredményeit írott jelentésben kell dokumentálni. A tanúsító/registrláló szervezet át kell vizsgálja az 1. fokozatú audit jelentését, hogy eldöntse, hogy hogyan folytatja az auditot a 2. fokozatban és ehhez kiválassza a csoport megfelelő felkészültségű tagjait.

A tanúsító/registrláló szervezetnek tudatosítania kell a szervezetben a további információfelelőségeket és feljegyzéseket, amelyeket kérhetnek a 2. fokozatú audit alatti részletes ellenőrzésekhez.

Ha az 1. fokozatú auditot, beleértve a dokumentum-átvizsgálást, nem egy személy végzi, a tanúsító/registrláló szervezet célszerűen legyen képes annak bizonyítására, hogy a különböző csoporttagok tevékenységei hogyan vannak koordinálva.

IS.9.2 2. fokozatú audit

Ez mindig a szervezet helyszínén/helyszínein történik. Az 1. fokozatú auditjelentés dokumentált megállapításai alapján a tanúsító/registrláló szervezet megfogalmaz a 2. fokozatú audit végzésére vonatkozó audittervet. A 2. fokozatú audit célkitűzései:

- a) annak megerősítése, hogy a szervezet saját eljárásrendjét, céljait és eljárásait megtartja;
- b) annak megerősítése, hogy az ISMS az ISMS szabvány és rendelkező dokumentum követelményeinek megfelel és eléri a szervezeti politika céljait.

Ennek megítéléséhez az audit összpontosítson a szervezeten

- c) az információbiztonság minősítésére a vonatkozó kockázatok és az ISMS ebből következő tervezése tekintetében;
- d) az Alkalmazhatósági Nyilatkozatra;
- e) az ebből a folyamatból lezármaztatott távolabbi és közelebbi célokra;
- f) a teljesítmény figyelésére, mérésére, jelentésére és átvizsgálására a távolabbi és közelebbi célok szempontjából;
- g) a biztonsági és vezetőségi átvizsgálásokra;
- h) a vezetőség felelősségére az információbiztonság-politikáért;
- i) a kapcsolatokra a politika, az információbiztonság kockázatának minősítése, a távolabbi és közelebbi célok, felelősségek, programok, eljárások, teljesítményadatok és biztonsági átvizsgálások között.

IS.10 Az ISMS audit egyes elemei

IS.10.1 Az információbiztonságra vonatkozó vagyoni fenyegetések, a sebezhetőségek és a szervezeten vonatkozó hatások értékelése és a jelentősnek ítélt szabályozása/kezelése: a tanúsító/registrláló szervezet szerepe

Annak érdekében, hogy bizalmat keltsenek arra, hogy a szervezetek következetesen a következő eljárások kialakításában és fenntartásában: az információbiztonságra vonatkozó vagyoni fenyegetések, sebezhetőségek és a szervezeten vonatkozó hatások azonosítására, megvizsgálására és kiértékelésére vonatkozóan, a tanúsító/registrláló szervezetek fontolják meg a következő tényezőket:

- a) a szervezeten tartozik, hogy meghatározza azokat a kritériumokat, amelyekkel az információbiztonság vonatkozású vagyoni fenyegetéseket, sebezhetőséget és hatásokat a szervezeten jelentősként határozzák meg, és eljárás(oka)t fejlesszenek ki ennek megtételére;
- b) célszerű, ha a tanúsító/registrláló szervezet megkívánja a szervezettől, hogy igazolja, hogy a biztonsággal kapcsolatos fenyegetések elemzése fontos és megfelelő a szervezet működéséhez;
- c) nincs következtetés a szervezet politikája, távolabbi és közeli céljai és eljárása(i) vagy azok alkalmazási eredményei között.

Ajánlatos, hogy a tanúsító/registrláló szervezet kimutassa, hogy a jelentőség elemzésében alkalmazott eljárások megalapozottak és megfelelően vannak bevezetve. Ha jelentősnek határoznak meg egy vagyoni veszélyeztetésre, sebezhetőségre vagy a szervezetre való hatásra vonatkozó információt, annak kezelését az ISMS-en belül célszerű végezni.

IS.10.2 Megfelelés a szabályozásoknak: a tanúsító/registrláló szervezet szerepe

A szervezet felelős a törvényi megfelelés fenntartásáért és értékeléséért. A tanúsító/registrláló szervezet ellenőrzésekre és mintavételre szorítkozzék, hogy bizalmat keltsen az ISMS ezirányú működésében.

Egy tanúsított/registrlált ISMS-sel rendelkező szervezetnek olyan irányítási rendszere van, amely folyamatos megfelelést kell elérjen a szabályozási követelmények tekintetében, amelyek tevékenységei, termékei és szolgáltatásai információbiztonsági hatásaira vonatkozathatók. A tanúsító/registrláló szervezet megerősíti, hogy egy olyan rendszert vezettek be teljes mértékben, amely a megkívánt megfelelés elérésére képes.

A tanúsító/registrláló szervezetnek igazolni kell, hogy a szervezet kiértékelte a törvényes és szabályozási megfelelést és ki kell tudja mutatni, hogy beavatkoztak a vonatkozó szabályozások nemteljesítése esetén.

IS.10.3 Az ISMS dokumentáció egyesítése más irányítási rendszerek dokumentációival

Elfogadható, hogy az ISMS és más irányítási rendszer (mint pl. minőségügyi, egészségügyi és biztonsági, környezeti) dokumentációját összevonják, oly mértékben, amíg az ISMS világosan azonosítható a megfelelő interfészeivel/csatlakozó felületeivel a többi rendszerek felé.

IS.10.4 A vezetőségi auditok közös végzése

Az ISMS audit közösen végezhető más irányítási rendszerek auditjaival. Ez a kombináció lehetséges, feltéve, hogy kimutatható, hogy az audit megfelel az ISMS tanúsítás/registrlálás összes követelményének. Egy ISMS számára fontos minden elem egyértelműen kell megjelenjen és könnyen azonosítható kell legyen az auditjelentésekben. Az auditok kombinálása nem befolyásolhatja hátrányosan az audit minőségét.

3.4. Minősítő jelentés

3.4.1. A tanúsító/registrláló szervezet elfogadhat az igényeinek megfelelő jelentési eljárásokat, de ezek az eljárások legalább a következőket biztosítsák:

- a) **az auditcsoport és a szervezet vezetősége tartson megbeszélést a helyszín elhagyása előtt, ennek során az auditcsoport írásban vagy szóban adjon tájékoztatást a szervezet ISMS-ének a részletes tanúsítási/registrlási követelményeknek való megfeleléséről és adjon lehetőséget a szervezetnek kérdések feltevésére a megállapításokkal és azok alapjával kapcsolatban;**

- b) az auditscsoport a tanúsító/regisztráló szervezetnek tegyen jelentést a szervezet ISMS-ének megfelelésére vonatkozó megállapításairól az összes tanúsítási/regisztrálási követelményekre nézve;
- c) a minősítés eredményére vonatkozó jelentést a tanúsító/regisztráló szervezet azonnal hozza a szervezet tudomására, meghatározva minden nemmegfelelést, amelyet meg kell szüntetni, hogy az összes tanúsítási/regisztrálási követelmény ki legyen elégítve;
- d) a tanúsító/regisztráló szervezet kérje fel a szervezetet, hogy tegyen észrevételt a jelentésre és írja le a megtett vagy meghatározott időn belül megtenni szándékozott konkrét intézkedéseket a minősítés során a tanúsítási/regisztrálási követelményekkel kapcsolatban megállapított nemmegfelelések kijavítására és értesítse a szervezetet, hogy szükséges-e teljes vagy részleges újraminősítés vagy megfelelőnek tekinthető egy írott nyilatkozat, amelyet a felügyelet során meg kell erősíteni;
- e) a jelentésnek legalább a következőket kell tartalmaznia:
 - 1) az audit(ok) időpontja(i),
 - 2) a jelentésért felelős személy(ek) neve,
 - 3) az összes auditált egységek azonosítása (pl. a létesítmények neve és címe és az auditált szervezeti elemek azonosítása),
 - 4) a tanúsítás/regisztrálás minősített szakterülete vagy arra való hivatkozás, beleértve az alkalmazott szabványra vagy rendelkező dokumentumokra való hivatkozást,
 - 5) a szervezet ISMS-ének a tanúsítási/regisztrálási követelményének való megfelelésre vonatkozó megjegyzéseket, a nemmegfelelés egyértelmű megállapításával és ahol ez lehetséges, mindennemű hasznos összehasonlítást a szervezet korábbi minősítéseinek eredményeivel,
 - 6) magyarázatot a szervezettel a záróértekezleten közölt tájékoztatáshoz képest felmerült minden eltérésről.

3.4.2. Ha a tanúsító/regisztráló szervezet által jóváhagyott jelentés eltér a 3.4.1. c) és e) szakaszban hivatkozott jelentéstől, a szervezethez el kell juttatni az előző jelentéstől való eltérésekre vonatkozó magyarázattal.

A jelentés vegye tekintetbe:

- a) azoknak a személyeknek képzését, tapasztalatát és hatáskörét, akikkel találkoztak;
- b) a kérelmező által alkalmazott belső szervezet és eljárások megfelelőségét arra, hogy bizalmat keltsen az ISMS iránt;
- c) a megállapított nemmegfelelések helyesbítésére tett intézkedéseket, beleértve, ha ilyen van, az előző minősítések során megállapított nemmegfeleléseket is.

3.5. Döntés a tanúsításról/registrlásról

3.5.1. Egy szervezet ISMS-ének tanúsítására/registrlására vonatkozó igen vagy nem döntést a tanúsító/registrláló szervezet kell hozza a tanúsítási/registrlási folyamat során gyűjtött információ és bármely más vonatkozó információ alapján. A tanúsításról/registrlásról nem dönthetnek olyanok, akik az auditban részt vettek.

ISMS útmutató

IS.11 Tanúsítási/registrlási döntés

Az egység, amely dönt a tanúsítvány kiadásáról, normális esetben nem fordíthatja meg az auditsoport negatív ajánlását. Ha ilyen helyzet áll elő, a tanúsító/registrláló szervezetnek dokumentálnia és indokolnia kell a döntés alapját, hogy az ajánlást megváltoztatja.

3.5.2. A tanúsító/registrláló szervezet nem ruházhatja át a tanúsítás/registrlás megadására, fenntartására, kiterjesztésére, szűkítésére, felfüggesztésére vagy visszavonására vonatkozó hatáskörét külső személyre vagy szervezetre.

3.5.3. A tanúsító/registrláló szervezet minden szállítónak, akinek ISMS-ét tanúsította/registrlalta, tanúsítási/registrlási dokumentumot kell adnia, mint pl. egy irat vagy tanúsítvány, amelyet egy erre a feladatra kijelölt tisztviselő ír alá. Ezeknek a dokumentumoknak meg kell határozniuk a szervezet és a tanúsítás/registrlás által lefedett mindegyik információs rendszerére a következőket:

- a) a nevet és címet;
- b) a kiadott tanúsítás/registrlás szakterületét, beleértve:
 - 1) az ISMS szabványokat és más rendelkező dokumentumokat, amelyek szerint az ISMS-eket tanúsítják/registrlálják,
 - 2) a szervezetek tevékenységeit, tekintettel a termék, folyamat vagy szolgáltatási kategóriákra;
- c) a tanúsítás/registrlás hatálybalépési időpontját és a határidőt, ameddig a tanúsítás/registrlás érvényes;
- d) az Alkalmazhatósági Nyilatkozat konkrét változatára való utalást;
- e) a megfelelő tanúsító/registrláló szervezet akkreditálás és más vonatkozó emblémák vagy jelölések.

3.5.4. Bármely módosítási kérelmet a tanúsítás/registrlás szakterületére vonatkozóan, amelyet már megadtak, a tanúsító/registrláló szervezet fel kell dolgozza. A tanúsító/registrláló szervezet el kell döntse, hogy milyen minősítési eljárás felel meg, ha ilyen kell, megfelelő-e arra, hogy eldöntse, hogy a módosítást meg kell-e adni és ennek megfelelően kell tennie.

IAF útmutató

G.3.5.1. A tanúsítási/registrlási folyamat során gyűjtött információ elegendő kell legyen:

- 1) a tanúsító/registrláló szervezetnek, hogy képes legyen a tanúsításra/registrlásra tájékozott döntést hozni;
- 2) a nyomon követhetőségre, amely elérhető pl. egy felszólaláskor vagy a legközelebbi audit tervezéskor (esetleg egy eltérő csoport által);
- 3) a folyamatosság biztosítására.

A jelentési követelményekhez az ISO/IEC Guide 62 3.4.1. e) szakaszhoz kiegészítően legyen információ:

- a belső biztonsági átvizsgálásokba vethető bizalom fokára;
- a legfontosabb, akár negatív, akár pozitív megfigyelések összegzésére, tekintettel az ISMS bevezetésére és hatásosságára;
- az auditcsoport következtetéseire.

ISMS útmutató

IS.12 Az auditcsoportok jelentése a tanúsító/registrláló szervezetnek

Annak érdekében, hogy alapot teremtsenek a tanúsítási/registrlási döntéshez, a tanúsító/registrláló szervezet egyértelmű jelentéseket kér, amelyek elegendő információt szolgáltatnak a döntéshozatalhoz.

- a) Az auditcsoporttól a tanúsító/registrláló szervezetnek jelentések szükségesek a minősítési folyamat különböző fokozataiban. Az iratgyűjtőben tartott információval kombinálva ezek a jelentések legalább a következőket tartalmazzák:
 - i) beszámoló az auditról, a dokumentum átvizsgálás összegezésével,
 - ii) beszámoló a szervezet információbiztonsági kockázatelemzésének minősítéséről,
 - iii) a felhasznált audit összidő és részletes leírás arról az időről, amelyet a dokumentum-átvizsgálásra, a kockázatelemzés minősítésére, az audit megvalósítására és az audit jelentésére fordítottak,
 - iv) a nemmegfelelések tisztázása,
 - v) audit kérdésfeltevések, amelyeket követtek, indoklás ezek kiválasztására és az alkalmazott módszertan,
 - vi) az auditcsoport ajánlása az tanúsításra/registrlásra a tanúsító/registrláló szervezetnek;
- b) Egy felügyeleti jelentés tartalmazza, különösen a korábban felfedett nemmegfelelések megszüntetésére vonatkozó információt. A felügyeletből származó jelentések legalább úgy legyenek felépítve, hogy az előbbi a) pont követelményét teljességében tartalmazzák.

IAF útmutató

- G.3.5.2. A tanúsítványt/registrlációt nem szabad megadni, amíg az összes G.1.3.1. útmutatóban meghatározott nemmegfelelőséget ki nem javították és a javítást a tanúsító/registrláló szervezet nem igazolta (helyszíni látogatással vagy más, megfelelő formájú igazolással).
- G.3.5.3. Az ISO/IEC Guide 62 3.5.3. c) szakasza megkívánja, hogy egy tanúsító/registrláló dokumentum tartalmazzon egy érvényességi határidő nyilatkozatot. Egy tanúsítás/registrlás érvényességi határideje legyen összevethető az újraminősítés rendelkezéseivel.

ISMS útmutató

IS.13 Döntéshozás a tanúsítási/registrlási tevékenységi körre vonatkozóan

Az egység, amely lehet egy személy, amely döntést hoz egy tanúsítás/registrlás megadására/visszavonására a tanúsító/registrláló szervezeten belül olyan ismeretszintet és tapasztalatot kell megtestesítsen minden területen, amely elég, hogy kiértékelje az auditfolyamatokat és az auditsoport által tett, ehhez kapcsolódó ajánlásokat.

3.6. Felügyelet és újraminősítési eljárások

3.6.1. A tanúsító/registrláló szervezet végezzen időszakos felügyeletet és újraminősítést eléggé rövid időszakonként annak igazolása céljából, hogy a szervezetei, amelyek ISMS-ét tanúsították/registrláltak folyamatosan megfelelnek a tanúsítási/registrlási követelményeknek.

5. MEGJEGYZÉS: A legtöbb esetben valószínűtlen, hogy egy évnél hosszabb időszakos felügyelet időtartam kielégítené e szakasz követelményeit.

IAF útmutató

- G.3.6.1. A tanúsító/registrláló szervezeteknek legyenek egyértelmű eljárásai, amelyek meghatározzák azokat a követelményeket és feltételeket, amelyek között a tanúsítások/registrlások fenntarthatók. Ha a felügyelet vagy az újraminősítés során a G.1.3.1. szerint meghatározott nemmegfeleléseket találnak, ezeket hatásosan helyesbíteni kell a tanúsító/registrláló szervezettel megállapodott időn belül. Ha a helyesbítést nem végzik el a megállapodott időn belül, a tanúsítást/registrlálást szűkíteni, felfüggeszteni vagy visszavonni kell. A helyesbítő intézkedések elvégzésére megengedett idő legyen összhangban a nemmegfelelés súlyosságával és azzal a kockázattal, hogy biztosítani lehet a termékek vagy szolgáltatások előírt követelményeknek való megfelelését.
- G.3.6.2. A tanúsító/registrláló szervezet által végzett felügyelet biztosítsa, hogy a tanúsított/registrlált szervezetei folyamatosan megfeleljenek a szabvány azon

követelményeinek, amelyek szerint tanúsították/registrlálták azokat. A tanúsító/registrláló szervezetnek legyen meg a felszerelése és eljárásai, hogy lehetővé tegyék ennek elérését.

3.6.2. A felügyeleti és újraminősítési eljárások legyenek összhangban azokkal, amelyek a szervezet ISMS-ének e közleményben leírt minősítésére vonatkoznak.

IAF útmutató

- G.3.6.3. Az ISO/IEC Guide 62 3.6.1. szakasza megkívánja, hogy egy tanúsító/registrláló szervezet egy felügyeleti és újraminősítési programot végezzen eléggé közeli időközökben, hogy igazolja, hogy tanúsított/registrlált szervezetei folyamatosan megfelelnek a tanúsítási/registrlási követelményeknek.
- G.3.6.4. A felügyelet célja, hogy igazolja, hogy a jóváhagyott ISMS továbbra is bevezetett, hogy fontolja meg a változások kihatásait erre a rendszerre, amely a szervezet működésében bekövetkező változások eredményeként indul el és erősítse meg a folyamatos megfelelést a tanúsítási/registrlási követelményeknek. Egy szervezet ISMS-ének felügyelete rendszeresen történjék, rendszeresen évente egyszer célszerű elvégezni. A felügyeleti programok rendszeresen a következőket tartalmazzák:
- a rendszer fenntartási elemeit, amelyek a belső audit, belső biztonsági átvizsgálás, vezetőségi átvizsgálás, megelőző és helyesbítő beavatkozások;
 - a külső felektől érkező kommunikáció, az ISMS szabvány vagy rendelkező dokumentum szerint;
 - a dokumentált rendszer változásai;
 - a változó területek;
 - a tanúsítási/registrlási szabvány vagy rendelkező dokumentum kiválasztott elemei;
 - más kiválasztott területek, szükség esetén.
- G.3.6.5. A felügyeleti tevékenységek külön intézkedést igényelnek, ha egy tanúsított/registrlált ISMS-sel rendelkező szervezet rendszerében nagyobb módosításokat végez vagy más változások történnek, amelyek hatással lehetnek a tanúsítás/registrlálás alapjaira.
- G.3.6.6. Az újraminősítés célja, hogy igazolja a szervezet ISMS-ének átfogó folyamatos megfelelését az ISMS szabvány vagy rendelkező dokumentum követelményeinek valamint, hogy az ISMS-t helyesen vezették be és tartják fenn. Legtöbb esetben valószínűtlen, hogy három évnél hosszabb időszak a szervezet ISMS-ének ismétlődő újravizsgálatára eleget tenne ennek a követelménynek. Az újraminősítés kell gondoskodjon a korábbi bevezetés átvizsgálásáról és a rendszer folyamatos fenntartásáról a tanúsítási/registrlási időszak alatt. Az újraminősítési program figyelembe kell vegye az előbb bemutatott átvizsgálás eredményeit és legalább az ISMS dokumentumok átvizsgálását és egy rendszerauditot (amely

helyettesítheti és/vagy kiterjesztheti a rendszerfelügyeleti auditot). Legalább a következőket biztosítsa:

- az ISMS elemei közti hatásos kölcsönhatást;
- az ISMS átfogó hatásosságát teljes egészében, a tevékenységek változásának fényében;
- kimutatott elkötelezettséget az ISMS hatásossága fenntartására.

G.3.6.7. Ha kivételesen az újraminősítési időszak 3 éven túl terjed, a tanúsító/registrláló szervezet ajánlatos, hogy bemutassa, hogy a teljes ISMS hatásosságát rendszeresen kiértékelték és legyen egy olyan felügyeleti gyakoriság, amely ellensúlyozza ezt, azért, hogy azonos megbízhatósági szintet tartson fenn.

G.3.6.8. A felügyeleti auditok során a tanúsító/registrláló szervezetek ellenőrizzék a tanúsító/registrláló szervezet elé hozott felszólalási, panasz és vitás kérdés feljegyzéseket és ahol bármilyen nemmegfelelés vagy a tanúsítás/registrlálás követelményei teljesülésének hiányossága kiderül, ellenőrizzék, hogy a szervezet megvizsgálta saját ISMS-ét és eljárásait és megfelelő helyesbítő beavatkozást végeztek.

G.3.6.9. A felügyeleti jelentés tartalmazzon a G.3.5.1. útmutató által megkívánt információ kiegészítéseképpen egy beszámolót a korábban feltárt minden nemmegfelelés megszüntetéséről.

ISMS útmutató

IS.14 Felügyeleti auditok és újraminősítések

A tanúsító/registrláló szervezet által végzett évenkénti felügyelet legalább tartalmazza a következő megfontolásokat:

- i) az ISMS hatásossága a szervezet információbiztonsági politikájára, céljainak elérésére tekintettel;
- ii) az időszakos értékelési eljárások és a vonatkozó információbiztonság jogi szabályozásának és szabályzatainak való megfelelés átvizsgálásának működése;
- iii) a legutolsó audit során meghatározott nemmegfelelésekre való beavatkozás;

és legalább tartalmaznia kell a fenti 3.4.2. szakaszban jelentés megtételéhez felsorolt pontokat.

- a) A tanúsító/registrláló szervezet legyen képes alkalmazni felügyeleti programját az információbiztonsági témákra vonatkozó vagyoni fenyegetésekre, sebezhetőségekre és a szervezetre való hatásokra és tudja megindokolni ezt a programot.

- b) A tanúsító/registráló szervezet felügyeleti programját a tanúsító/registráló szervezet kell meghatározza. A látogatások konkrét időpontjaira a tanúsított/registrált szervezettel kell megállapodni.
- c) A felügyeleti auditok végezhetőek közösen más irányítási rendszerek auditjaival. A jelentéstétel egyértelműen kell jelezze az egyes irányítási rendszerekre vonatkozó szempontokat.
- d) A tanúsító/registráló szervezettől megkívánják, hogy a tanúsítvány és jelentés megfelelő alkalmazását felügyelje.
- e) Az újraminősítési audit módszertana célszerűen ugyanaz legyen, mint az audité.

3.7. Tanúsítványok és emblémák alkalmazása

3.7.1. A tanúsító/registráló szervezet gyakoroljon megfelelő ellenőrzést az ISMS tanúsítási/registrálási jel és emblémák tulajdonjoga, alkalmazása és feltüntetése felett.

3.7.2. Ha egy tanúsító/registráló szervezet engedélyezi egy ISMS tanúsítási/registrálási jelölésére egy jel vagy embléma használatát, a szervezet az előírt jelet vagy emblémát csak a tanúsító/registráló szervezet által adott írásbeli meghatalmazásnak megfelelően használhatja. Ezt a jelet vagy emblémát nem szabad terméken vagy olyan módon alkalmazni, hogy azt a termék megfelelőségi jeleként lehessen értelmezni.

3.7.3. A tanúsító/registráló szervezet tegyen megfelelő intézkedéseket, hogy foglalkozzon a tanúsító/registráló rendszerre vonatkozó helytelen hivatkozásokkal vagy a tanúsítványoknak vagy emblémáknak hirdetésekben, katalógusokban és máshol előforduló félrevezető alkalmazásával.

6. MEGJEGYZÉS: Ilyen beavatkozáshoz tartoznak a helyesbítő intézkedés, a tanúsítvány visszavonása, a szabálysértés közzététele és ha szükséges, más jogi beavatkozás.

IAF útmutató

- G.3.7.1. Egy akkreditált tanúsítvány közölje azt a szabvány(oka)t vagy más rendelkező dokumentum(oka)t, amelyek szerint a tanúsítást/registrációt megadják, a tanúsító/registráló szervezet nevét, amely azt kiadta és a vonatkozó akkreditáló testület(ek) nevét. Egyértelművé kell tenni, hogy a tanúsítványt a tanúsító/registráló szervezet akkreditált alkalmazási területén adták ki.
- G.3.7.2. Minden tanúsítvány, amelyet egy akkreditált tanúsító/registráló szervezet adott ki az akkreditált alkalmazási területén belül, viselje a vonatkozó akkreditáló testület jelét. Ha egy szervezet azt kéri, hogy a tanúsítványt akkreditálási jel nélkül adják ki, ahhoz, hogy a tanúsítványt akkreditáltnak lehessen tekinteni, tartalmaznia kell az akkreditáló testület nevét és a registrálási számát.

- G.3.7.3. Azokban az esetekben, amikor a tanúsító/registráló testületet több akkreditáló testület akkreditálta, a tanúsítványon legyen legalább egy akkreditálási jel, a piaci igényeknek megfelelően.
- G.3.7.4. A tanúsító/registráló szervezetnek legyenek dokumentált eljárásai a jelének alkalmazására és azokra az eljárásokra, amelyeket visszaélés esetén követni kell, beleértve tanúsításra/registrálásra vonatkozó meg nem alapozott igényeket és a tanúsító/registráló szervezet jeleinek helytelen alkalmazását.
- G.3.7.5. Ha egy tanúsító/registráló szervezet helytelenül igényli az akkreditált státuszt olyan tanúsítványokra, amelyeket a megfelelő akkreditálás megadása előtt adott ki, az akkreditáló testület kérheti ezt követően azt, hogy vonja vissza azokat.
- G.3.7.6. Az ISO/IEC Guide 62 3.7.1. szakasz rendelkezései, amelyek a „tanúsítási/registrálási jel és embléma”, valamint a 3.7.2. szakasz „jelkép vagy embléma” vonatkozásúak, egyaránt alkalmazhatók a jelekre, emblémákra és jelképekre.
- G.3.7.7. A tanúsító/registráló szervezet kerülje ugyanazon jel alkalmazását különböző megfelelési rendszertanúsításra/registrálásra (pl. terméktanúsítás/registrálás és irányítási rendszer tanúsítás/registrálás) és kerülje a saját jelei értelmezései közötti zavart, ha több jele van.
- G.3.7.8. Egy tanúsító/registráló szervezetnek legyenek eljárásai, hogy biztosítsa, hogy a tanúsított/registrált szervezetek nem engedik jelüknek az alkalmazását oly módon, amely valószínűleg félrevezető vagy zavart okozhat.

3.8. Hozzáférés a szállítókhoz eljuttatott panaszokról készült feljegyzésekhez

A tanúsító/registráló szervezet követelje meg minden szervezettől, amelynek ISMS-ét tanúsította/registrálta, hogy kérésére tegye számára hozzáférhetővé a feljegyzéseket az összes panaszokra és helyesbítő intézkedésekre, amelyeket az ISMS szabványok vagy más rendelkező dokumentumok követelményeivel összhangba tettek.

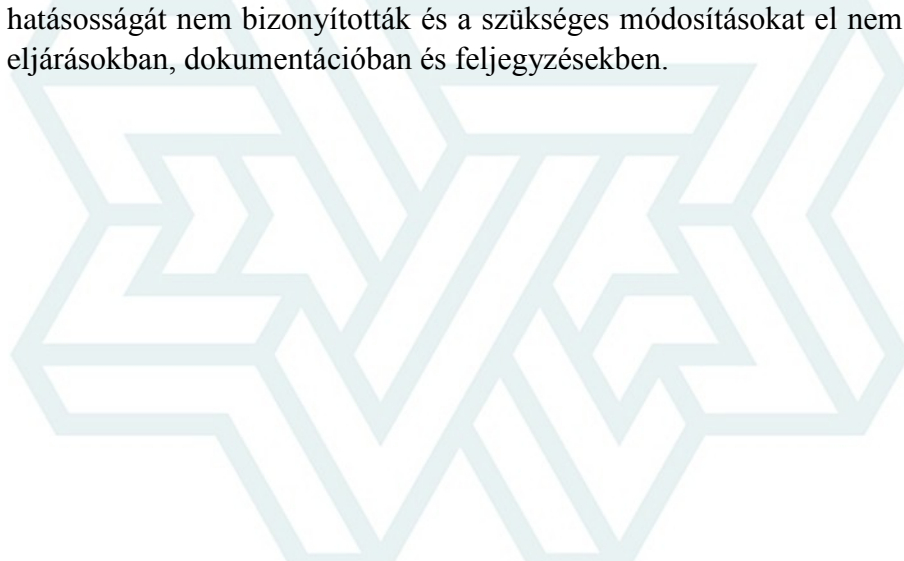
IAF útmutató

- G.3.8.1. Ez a szakasz csak a tanúsított/registrált szervezet által kapott panaszokra vonatkozik, nem a tanúsító/registráló szervezet által kapott panaszokra.
- G.3.8.2. A panaszok egy lehetséges nemmegfelelésre vonatkozó információforrást jelentenek. Egy panasz beérkezésekor a tanúsított/registrált szervezet meg kell állapítsa és ahol helyénvaló tegyen jelentést a nemmegfelelés okáról, beleértve bármilyen előre meghatározó (vagy hajlamosító) tényezőt az ISMS szervezetén belül.
- G.3.8.3. A felügyeleti auditok során a tanúsító/registráló szervezetek ellenőrizték, ahol bármilyen, a szabvány követelményeinek teljesítésére vonatkozó nemmegfelelés vagy hiányosság mutatkozott, hogy a szervezet alaposan megvizsgálta saját rendszereit és eljárásait és megfelelő helyesbítő intézkedéseket tett.

G.3.8.4. A tanúsító/registrláló szervezet meg kell győződjön, hogy a szervezet olyan alapos vizsgálatokat alkalmaz, hogy javító/helyesbítő intézkedést dolgozzon ki, amely tartalmazzon intézkedéseket a következőkre:

- a megfelelő hatóságok értesítése, ha a szabályozás megköveteli;
- a megfelelés lehető leggyorsabb helyreállítása;
- az ismétlődés megakadályozása;
- minden váratlan káros biztonsági esemény kiértékelése és mérséklése, a velük járó hatásokkal együtt;
- az ISMS más összetevőivel való kielégítő kölcsönhatás biztosítása;
- az elfogadott javító/helyesbítő intézkedések hatásosságának minősítése.

G.3.8.5. A javító/helyesbítő intézkedést nem szabad befejezettek tekinteni, míg hatásosságát nem bizonyították és a szükséges módosításokat el nem végezték az eljárásokban, dokumentációban és feljegyzésekben.



1. MELLÉKLET: AZ AKKREDITÁLÁS TÁRGYKÖREI

Jelen akkreditálási terület jegyzék a gazdasági tevékenységek statisztikai nomenklatúrája alapján készült, (NACE Rev. 1.1) 1994; az Európai Közösség Bizottsága kiadásában (Hivatalos Lap, L 083 1993).

Kód	Megnevezés	NACE kód
1	Mezőgazdaság, halászat	A,B
2	Bányászat, kőbányászat	C
3	Élelmiszerek, italok és dohány	DA
4	Textil és textiltermékek	DB
5	Bőr és bőrtermékek	DC
6	Fa és fatermékek	DD
7	Papírpép, papír és papírtermék	DE 21
8	Kiadóvállalatok	DE 22.1
9	Nyomdák	DE 22.2,3
10	Kocsz és finomított olajtermékek gyártása	DF 23.1,2
11	Nukleáris üzemanyag	DF 23.3
12	Vegyszerek, vegyipari termékek és rostok	DG, kivéve 24.4
13	Gyógyszerek	DG 24.4
14	Gumi és műanyag termékek	DH
15	Nemfémes ásványi termékek	DI, kivéve 26.5,6
16	Beton, cement, mész, gipsz, stb.	DI 26.5,6
17	Alapfémek és megmunkált fémtermékek	DJ
18	Gépészet, berendezések	DK
19	Elektromos és optikai berendezés	DL
20	Hajógyártás	DM 35.1
21	Légi és űrjárművek	DM 35.3
22	Egyéb közlekedési eszköz	DM 34,35.2,4,5
23	Máshová nem sorolható gyártás	DN 36
24	Újrahasznosítás	DN 37
25	Elektromos-áramszolgáltatás	E 40.1
26	Gázszolgáltatás	E 40.2
27	Vízellátás	E 41,40.3
28	Építőipar	F
29	Nagykereskedelem és kiskereskedelem Motoros járművek, motorkerékpárok, személyes használatú és háztartási gépek javítása	G
30	Szállodák és éttermek	H
31	Közlekedés (szállítás), raktározás és kommunikáció	I
32	Pénzügyi közvetítés, ingatlan, kölcsönzés	J,K 70,K 71
33	Információs technológia	K 72
34	Műszaki szolgáltatás	K 73, 74.2
35	Egyéb szolgáltatás	K 74 kivéve K 74.2
36	Közigazgatás	L
37	Oktatás	M
38	Egészségügyi és szociális munka	N
39	Egyéb szociális szolgáltatások	O