# Kiberbiztonsági auditjelentés gépi feldolgozásra alkalmas formátuma

## Bevezetés

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 16. § alapján végrehajtott audit eredményeit a Kiberbiztonsági tv. 22. § (2) bekezdés alapján az auditor az SZTFH és a szervezet részére az audit befejezését követően haladéktalanul megküldi. A kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I. 31.) SZTFH rendelet 5. § (8) bekezdése alapján az adatszolgáltatást gépi feldolgozást biztosító specifikáció szerinti változatban is meg kell küldeni.

A Hatóság által elvárt OSCAL (Open Security Controls Assessment Language) nyílt szabványú leíró nyelv, amelynek célja, hogy egységes, gépi feldolgozásra alkalmas formában támogassa a követelmények dokumentálását, értékelését és megosztását.

## Az OSCAL komponensei

Az OSCAL nyelv több fő sémát tartalmaz, amelyek különböző szintű dokumentálási és értékelési igényeket elégítenek ki:

1. Catalog: A biztonsági kontrollok katalógusa, amely meghatározza a megfelelőségi elvárásokat.
2. Profile: A katalógus testreszabott részhalmaza, amely az adott szervezet vagy projekt specifikus igényeit tükrözi.
3. System Security Plan (SSP): A rendszer biztonsági architektúrájának és kontrolljainak dokumentálása.
4. Assessment Plan (AP): Az audit és értékelés tervezése.
5. Assessment Results (AR): Az audit során gyűjtött megfigyelések, megállapítások, eredmények strukturált összefoglalása.
6. Plan of Action and Milestones (POA&M): Az észlelt hiányosságok és azok javítási tervének dokumentuma.

## Az Assessment Results szerepe és előnyei

Az Assessment Results az OSCAL egyik kulcseleme, amely az audit során keletkező tényleges eredményeket foglalja össze. Ez a struktúra biztosítja, hogy az auditorok egységes és összehasonlítható formában tudjanak jelentéseket készíteni és feldolgozni.

Az Assessment Results szerkezete logikus, hierarchikus formában tartalmaz minden releváns információt:

- az auditban érintett elektronikus információs rendszerek jellemzőit (pl. komponensek, kockázati szintek);
- a dokumentumvizsgálat, az interjú és a tesztelés eredményeit;
- az észlelt kockázatokat, és azok jellemzőit;
- a vizsgált követelmények állapotát, valamint
- minden az audit során keletkezett bizonyítékot, amelyek alátámasztják az auditjelentésben szereplő értékelést.

## Miért ezt a struktúrát kell használni az auditoroknak?

A kiberbiztonsági auditjelentések esetében elengedhetetlen, hogy az adatok átláthatóan, strukturáltan és automatizálható módon álljanak rendelkezésre. Az OSCAL Assessment Results séma ezt ténylegesen biztosítja. A formátum támogatja az:

- egységes riportkészítést, ahol az auditorok jelentései összehasonlíthatók;
- a gépi feldolgozhatóságot, ami kulcsfontosságú az elemzések és a hatósági feldolgozás szempontjából;
- a verziók követhetőségét és a jelentések digitális aláírhatóságát.

# Formátum

Az OSCAL Assessment Results séma több kulcselemre tagolódik:

- metadata: tartalmazza a jelentés alapinformációit (cím, kiadás dátuma, változat, verzió, közreműködő szerepkörök és helyszínek, érintettek adatai).
- import-ap: az audit alapjául szolgáló auditálási terv referenciája.
- results: egy tömb, amely a konkrét audit során gyűjtött információkat tartalmazza. Ebben szerepel:
    - local-definitions: az auditban használt komponensek, eszközök, címek, szereplők.

    - reviewed-controls: a megvizsgált követelmények leírása, beleértve az esetleges kizárásokat, hozzárendelt komponenseket.
    - attestations: az auditban részt vevő értékelők által aláírt, pontozással vagy megállapításokkal kiegészített értékelések.
    - observations: olyan egyedi megfigyelések, amelyek segítik az értékelést. Minden megfigyelés tartalmazhat leírást, módszert, érintett komponenst vagy személyt.
    - risks: az értékelt elektronikus információs rendszerekre vonatkozó, az audit során azonosított kockázatok leírása és kategorizálása (súlyosság, hatás, állapot).
    - findings: a követelménycsoportokra vonatkozó megállapítások. Ezek a biztonsági osztályokhoz kapcsolódnak, és hivatkozhatnak megfigyelésekre és kockázatokra is.
- back-matter: mellékletek, hivatkozott források (pl. PDF dokumentumok, szoftverek kimenetei, weboldalak).

Az alábbi táblázat a gépi feldolgozásra alkalmas auditjelentés struktúráját (sémáját) és az ahhoz kapcsolódó magyarázatokat tartalmazza. Minden elem esetén szögletes zárójelben a kötelező vagy megengedett darabszám, kerek zárójelben pedig az adott elem típusa kerül megjelenítésre.

| JSON OSCAL elem | Magyarázat |
|---|---|
| assessment-results (object) [1] | Kötelező gyökér elem, amelyből pontosan egy darab kell, hogy legyen a jelentésben. |
| ├── uuid (string) [1] | Egyedi UUD4 azonosító. |
| ├── metadata (object) [1] | A jelentésben pontosan egy darab metadata elemnek kell szerepelnie. |
| │ ├── title (string) [1] | A title mezőnek az Audit jelentés címét kell tartalmaznia. |
| │ ├── published (string) [1] | A jelentés kiadásának, elkészítésének időpontja. Ez a dátum- és időérték az RFC3339 által meghatározott „date-time” szerint van formázva. |
| │ ├── last-modified (string) [1] | A dokumentum utolsó módosításának időpontja, ami jellemzően megegyezik a kiadás dátumával. Ez a dátum- és időérték az RFC3339 által meghatározott „date-time” szerint van formázva. |
| │ ├── version (string) [1] | Az auditjelentés verziója |
| │ ├── oscal-version (string) [1] | Értéke kötelezően: 1.1.3 |

| | |
|---|---|
| ├── props (array of object) [1 … ∞] | Tetszőleges számú egyedi információs mezőt tartalmazhat, amely a jelentés tulajdonságait írja le. Minimálisan azonban a 7/2024. (VI. 24.) MK rendeletre való hivatkozásnak szerepelnie kell. Valamint egy egyedi projekt / audit azonosítót tartalmazó tulajdonságnak is, amely alapján az audit utólag bármikor beazonosítható. Lásd 1. kiegészítés. |
| ├── name (string) [1] | Egyedi, auditor specifikus tulajdonság mezők esetén az ns (namspace) mezőnek az auditor szervezet által kiadott namespace-nek kell lennie. |
| ├── ns (string) [1] | |
| └── value (string) [1] | |
| ├── roles (array of object) [6 … ∞] | Az auditálási folyamatban részt vevő személyek szerepköreit tartalmazó felsorolás. Kötelezően az alábbi szerepköröknek kell szerepelnie benne:<br>authority, assessor, assessment-team, assessment-lead, organization, organization-team.<br>Lásd 2. kiegészítés.<br>Emellett tetszőleges számú, az audit szempontjából releváns szerepkört is definiálhat az auditor (pl vulnerability-test-team, vulnerability-test-lead). |
| ├── id (string) [1] | Minden mező megadása kötelező minden szerepkör esetén. |
| ├── title (string) [1] | |
| └── description (string) [1] | |
| ├── locations (array of object) [2 … ∞] | Az audit szempontjából releváns, összes fizikai helyszín megadása kötelező. Minimálisan meg kell adni az alábbi kettőt: Auditor székhelye vagy telephelye, az auditált szervezet székhelye vagy telephelye. Emellett, az összes auditált fizikai helyszínt is szerepeltetni kell (pl. szerverterem, ügyfélszolgálati iroda stb.) |
| ├── uuid (string) [1] | Minden helyszínre egyedi UUID. |
| ├── title (string) [1] | A helyszín megnevezése. (pl. “Auditor székhelye”) |
| ├── address (object) [1] | Az adott helyszín címe. |
| ├── type (string) [1] | Az értéke kötelezően “work”. |
| ├── addr-lines (array of string) [1 … ∞] | A helyszín címe egy vagy több sorba rendezve. |
| ├── city (string) [1] | Város |

| | |
|---|---|
| ├── postal-code (string) [1] | Irányítószám |
| └── country (string) [1] | Ország kód. Jelen esetben “HU” |
| └── props (array of object) [0 ... ∞] | A helyszínhez kapcsolódó egyéb, egyedileg definiált tulajdonságok listája. Adatközpont esetén opcionálisan megadható az erre vonatkozó jelzés. |
| ├── name (string) [1] | Adatközpont esetén az értéke “type”. |
| ├── ns (string) [1] | |
| ├── class (string) [1] | Adatközpont esetén az értéke "data-center". |
| └── value (string) [1] | Adatközpont esetén az értéke lehet “primary” vagy “alternative”. |
| ├── parties (array of object) [5 ... ∞] | Az audit szempontjából releváns összes szereplő megadása. Ezek között lehetnek cégek (szervezetek) illetve személyek is. Minimálisan a következők megadása szükséges: auditor cég, az auditált szervezet, SZTFH, az auditban résztvevő auditor személyek (minimum egy), az auditált szervezet oldaláról az auditban résztvevő személyek (minimum egy). Lásd 3. kiegészítés. |
| ├── uuid (string) [1] | Egyedi UUID azonosító. |
| ├── type (string) [1] | Szervezet esetén: “organization”, személy esetén “person”. |
| ├── name (string) [1] | A szervezet vagy személy neve |
| ├── short-name (string) [0 .. 1] | Szervezet esetén opcionálisan a szervezet rövid neve. |
| ├── links (array of object) [0 ... ∞] | Opcionális, az auditált szervezet honlapjára mutató link. |
| ├── href (string) [1] | A honlap címe. |
| └── rel (string) [1] | Értéke kötelezően: “home-page” |
| ├── email-addresses [1 ... ∞] | Szervezet és személy esetén is kötelező egy email elérhetőség megadása. |
| ├── telephone-numbers (array of object) [1 ... ∞] | Auditor és auditált szervezet esetén kötelezően megadandó a szervezet elérhetőségi telefonszáma. Személyek esetén nem kötelező megadni. |
| └── number (string) [1] | Telefonszám. |
| ├── member-of-organizations (array of string) [0 ... 1] | Személy esetén kötelező megadni, hogy mely szervezet tagja. A lista egyetlen eleme a megadott szervezet egyedi UUID azonosítója. |
| └── location-uuids (array of string) [1 ... ∞] | Szervezet esetén az összes releváns “location” (helszín) egyedi UUID |

| | |
|---|---|
| | azonosítója (székhely, telephely, adatközpont stb.), személy esetén a személy munkavégzése szempontjából releváns helyszín egyedi UUID azonosítója. Minimum egy megadása kötelező. |
| └── responsible-parties (array of object) [6 ... ∞] | Ez a lista rendeli össze egymással a szerepköröket (“roles”) és az egyes résztvevőket (“parties”). A roles-ban szereplő összes szerepkörre (minumum 6) meg kell adni, hogy ki vagy kik töltik be ezt a szerepet. |
| ├── role-id (string) [1] | A szerepkör azonosítója (neve), ahogy a roles struktúrában meg lett adva. (pl. “authority”) |
| └── party-uuids (array of string) [1 ... ∞] | Az audit során szerepet betöltő személyek vagy szervezetek egyedi UUID azonosítója, ahogyan a parties listában meg lett adva. |
| ├── import-ap (object) [1] | Kötelező elem, az auditálási tervre vonatkozó egyedi hivatkozás. |
| ├── href (string) [1] | Az auditálási terv elérhetősége. Ennek a hivatkozásnak a back-matter resources listájának egyik elemére kell mutatnia. |
| └── remarks (string) [0 .. 1] | Opcionális megjegyzés az auditálási tervvel kapcsolatosan. |
| ├── results (array of object) [1] | A results lista tartalmazza az audit eredményeit. Kötelezően egy elemű lista, amely az aktuális audit eredményeit ismerteti. Az előzmény vagy ismételt auditok eredményeit a lista nem tartalmazza jelen formátum szerint. |
| ├── uuid (string) [1] | Egyedi UUID azonosító. |
| ├── title (string) [1] | Egyedi cím a jelentéshez, amely jelen esetben megegyezhet a metadata-ban megadott title értékével, vagy hivatkozhat arra is, hogy ez a szervezet első vagy akár megismételt auditja. |
| ├── description (string) [1] | Az auditjelentéssel kapcsolatos rövid leírás a jelentés céljáról, felépítéséről, vagy egyéb, az auditor által relevánsnak ítélt információkról. |
| ├── start (string) [1] | Az audit kezdésének időpontja. Ez a dátum- és időérték az RFC3339 által meghatározott „date-time” szerint van formázva. |

| | |
|---|---|
| ├── end (string) [1] | Az audit befejezésének időpontja. Ez a dátum- és időérték az RFC3339 által meghatározott „date-time“ szerint van formázva. |
| ├── local-definitions (object) [1] | Kötelező elem, amely az audit szempontjából fontos alábbi két elemet kell minimálisan tartalmaznia: components,, inventory-items. |
| ├── components (array of object) [1 ... ∞] | Az audit során vizsgált EIR-eket tartalmazó lista. Minimum 1 megadása kötelező. Egyéb komponens megadása is lehetséges, de az EIR-eken kívül más nem kötelező. |
| ├── uuid (string) [1] | Az EIR egyedi UUID azonosítója. |
| ├── title (string) [1] | Az EIR neve. |
| ├── description (string) [1] | Az EIR leírása, az EIR által támogatott üzleti cél. |
| ├── type (string) [1] | Értéke kötelezően “system” az EIR-ek esetében. |
| ├── status (object) [1] | A status megadása kötelező. |
| └── (string) [1] | Értéke kötelezően “operational”. |
| └── props (array of object) [3 ... ∞] | Az EIR-re vonatkozó információkat tartalmazó lista. Minimálisan tartalmaznia kell az auditált szervezet által megadott alábbi információk mindegyikét:<br>risk-level: Az EIR biztonsági osztályba sorolása<br>assessment-catalog: Az audit során használt követelmény katalógus azonosítóját.<br>assessment-profile: Az audit során használt követelmény profil azonosítóját.<br>business-domain: Az EIR által támogatott üzleti cél.<br>reasoning: Az EIR biztonsági osztályba sorolásának indoklása<br>Az egyes kritériumokra vonatkozó indoklás, pl.: 2.2.2.1.reasoning: A 2.2.2.1. kritérium indoklása<br>Minden a biztonsági osztály szempontjából elvárt kritérium indoklásának szerepelnie kell. |
| ├── name (string) [1] | A tulajdonság neve. (pl. “risk-level”) |

| | |
|---|---|
| ├── ns (string) [1] | Az auditor által megadott egyedi namespace. |
| └── value (string) [1] | Szöveges információ (pl. indoklás), risk-level esetén az értéke az alábbiak közül egy lehet: “alap”, “jelentős”, “magas”. assessment-catalog esetén az értéke kötelezően “7/2024. (VI. 24.) MK rendelet katalógus” assessment-profil esetén az értéke a risk-level függvényében kötelezően az alábbi három egyike lehet “7/2024. (VI. 24.) MK rendelet alap profil”, “7/2024. (VI. 24.) MK rendelet jelentős profil”, “7/2024. (VI. 24.) MK rendelet magas profil” |
| └── inventory-items (array of object) [1 ... ∞] | A vizsgált EIR-ek egyes vizsgálati elemeit tartalmazó lista. Jellemzően a sérülékenységvizsgálat során érintett IP címek, web címek, a vizsgált szerverek, munkaállomások, adatbáziskezelők, alkalmazás szerverek stb. listája. Minden olyan munkaállomást, szervert, vagy egyéb informatikai elemet szerepeltetni kell itt, amelyeket a vizsgálat (jellemzően a TESZT típusú) ellenőrzött. |
| ├── uuid (string) [1] | A vizsgált elem egyedi UUID azonosítója. |
| ├── description (string) [1] | A vizsgált elem leírása. |
| └── props (array of object) [1 ... ∞] | A vizsgált elem azonosításához szükséges tulajdonságok megadása. Pl. IP cím, URL, szerver neve, adatbázis neve, stb. Kötelező legalább egy megadása. |
| ├── name (string) [1] | A tulajdonság neve, pl.: ipv4-address, host-name |
| ├── ns (string) [1] | Az auditor által meghatározott egyedi namespace. |
| └── value (string) [1] | Az azonosításhoz szükséges érték. |
| ├── reviewed-controls (object) [1] | Kötelező elem, az audit során ellenőrzött követelménycsoportok meghatározása. |
| ├── control-selections (array of object) [1 ... ∞] | Minden auditált EIR esetén kötelező pontosan egy ilyen elem megadása, amely az adott EIR vonatkozásában |

| | |
|---|---|
| | meghatározza a vizsgált követelménycsoportokat. |
| ├── description (string) [1] | Általános leírás, amely indokolja a követelménycsoport kiválasztását. Alap esetben ez az EIR biztonsági osztályba sorolásából következik, de amennyiben kizárásra kerül védelmi intézkedés, amit az auditor elfogad, azt az indoklásban jelezni kell. |
| ├── include-all (object) [1] | Szerepelnie kell és értéke kötelezően {}. Ez jelzi, hogy minden követelménycsoport auditálása kötelező a lent kizártakat kivéve. |
| ├── exclude-controls (array of object) [0 ... ∞] | Amennyiben az auditor által elfogadott indoklás alapján kizárásra kerülnek bizonyos követelménycsoportok, azokat itt kell megadni. |
| └── control-id (string) [1] | A kizárt követelménycsoport egyedi azonosítója (pl. “4.6.”) |
| └── props (array of object) [1 ... ∞] | A tulajdonság listának minimum egy eleműnek kell lennie, és minimálisan tartalmaznia kell az EIR-re (mint component) való hivatkozást.<br>Emellett amennyiben követelménycsoport kizárás történt, minden egyes követelménycsoport kizárásának indoklása is egy-egy önálló tulajdonság mezőben kell, hogy megjelenjen. |
| ├── name (string) [1] | EIR hivatkozás esetén “component”, kizárás esetén “exclusion”. |
| ├── ns (string) [1] | A namespace értéke az auditor által egyedileg meghatározott. |
| ├── class (string) [0 ... 1] | Csak “exclusion” esetén kell megadni. A class értéke tartalmazza az adott követelménycsoport azonosítóját. (Pl. “4.6.”) |
| └── value (string) [1] | EIR megadására vonatkozó tulajdonság esetén az értéke az EIR egyedi UUID azonosítója (lásd. components). Kizárás esetén a kizárás indoklása. |
| └── control-objective-selections (array of object) [1] | Kötelező elem, amely jelzi, hogy a nem kizárt követelménycsoportok |

| | |
|---|---|
| | esetén minden elemi követelmény auditálása kötelezően megtörténik. |
| └── include-all (object) [1] | Kötelező elem, értéke {}, amely jelzi, hogy a nem kizárt követelménycsoportok esetén minden elemi követelmény auditálása kötelezően megtörténik. |
| ├── attestations (array of object) [1 ... ∞] | Minimum egy elemet tartalmazó lista. Kötelező eleme egy olyan igazolás megadása, amely tartalmazza a szervezetre vonatkozó SZEKI és az egyes EIR-ekre vonatkozó VMI értékeket. |
| └── parts (array of object) [1 ... ∞] | Minimálisan egy ilyen elem kell a SZEKI és VMI értékekhez kapcsolódó információk megadásához. |
| ├── name (string) [1] | A kötelező elem esetében ennek az értéke “audit-scores”. Amennyiben az auditor további part elemet akar hozzáadni a listához, azok esetében az auditor határozza meg a nevet. |
| └── parts (array of object) [2 ... ∞] | Minden egyes index értékhez egy önálló part megadása kell. A SZEKI-nek kötelezően van egy part eleme, ezen kívül kötelező minden auditált EIR-hez egy-egy part elem megadása. |
| ├── name (string) [1] | A SZEKI esetén a név kötelezően “szeki”. VMI esetén a név kötelezően “vmi”. |
| ├── props (array of object) [2 ... ∞] | SZEKI esetén minimum két elemet kell tartalmazzon, az egyik a SZEKI index értékét mutatja be, a másik pedig a szervezetre (mint “party”) vonatkozó egyértelmű hivatkozást ad meg. VMI esetén legalább két elemet kell, hogy tartalmazzon, amiből az egyik a VMI értékét tartalmazza, a másik tulajdonság pedig az adott EIR-re való egyértelmű hivatkozás. |
| ├── name (string) [1] | A SZEKI és a VMI értékét tartalmazó tulajdonság esetén az értéke “score“, az EIR-re való hivatkozás esetén az értéke “component”. Szervezetre való hivatkozás esetén “party”. |
| ├── ns (string) [1] | Egyedi, auditor által definiált tulajdonságok esetén az auditor |

| | |
|---|---|
| | saját namespace-e. |
| └── value (string) [1] | SZEKI és VMI esetén az adott index értéke (mint egész szám) szövegként tárolva. EIR hivatkozás esetén az EIR egyedi UUID azonosítója a “components”-ben megadott szerint. Szervezet hivatkozás esetén a szervezet egyedi UUID azonosítója. |
| └── prose (string) [1] | Az adott index megnevezése és magyarázata. |
| ├── observations (array of object) [4 ... ∞] | Ez a lista tartalmazza az összes olyan auditori tevékenységet, amely során az auditor meggyőződött az EIR-ek megfelelőségéről. Minimum négy elemnek meg kell jelennie azonban: az auditált szervezet által átadott EIR biztonsági osztályba sorolásának átvizsgálása, dokumentumvizsgálat, interjú, teszt (pl helyszín audit). Az auditor döntése, hogy például a szabályzatokat minden EIR esetében közösen vizsgálja át, és ebben az esetben erre vonatkozóan csak egy “observation” jelenik meg, vagy ezeket EIR-enként külön-külön vizsgálja avagy akár követelmény családonként szétdarabolva végzi a vizsgálatot. Szintén az auditor folyamatán múlik, hogy hány interjút folytat (de ezek mindegyikének meg kell jelennie, mint observation), hány helyszíni auditot folytat. Itt kell megjelennie annak is, mint önálló observation-nek, ha az auditor sérülékenység vizsgálatot folytat.<br>Minden önállóan értelmezhető auditori “megfigyelés” önálló observation-be kell, hogy kerüljön. |
| ├── uuid (string) [1] | Egyedi UUId azonosító. |
| ├── title (string) [1] | Az auditori vizsgálati módszer meegnevezése. |
| ├── description (string) [1] | Az auditori vizsgálati módszer leírása |
| ├── methods (array of string) [1 ... ∞] | Jellemzően egy elemű lista, amelynek az értéke lehet “EXAMINE” (átvizsgálás), “INTERVIEW” (interjú) vagy “TEST” (teszt). Előfordulhat, hogy az |

| | |
|---|---|
| │ │ │ | auditor egy interjút és egy auditot (teszt) összevon, ez esetben mind a két vizsgálati módszer szerepel a listában. |
| │ │ ├── types (array of string) [1] | Az EIR biztonsági osztályba sorolásának auditori értékelése esetén az értéke "risk-adjustment", minden más esetben "control-objective". |
| │ │ ├── origins (array of object) [1] | A megfigyelést végző entitás (“party”) megadása kötelező. Ez lehet egy auditor személy, az auditori csapat, illetve maga az auditor szervezet is. |
| │ │ │ └── actors (array of object) [1 ... ∞] | Legalább egy felelős szereplő megadása kötelező a vizsgálat módszer forrásaként. |
| │ │ │ ├── type (string) [1] | Személy vagy szervezet esetén az értéke “party”. |
| │ │ │ └── actor-uuid (string) [1] | A “parties” listában szereplő entitás egyedi UUID azonosítója. |
| │ │ ├── subjects (array of object) [1 ... ∞] | EIR biztonsági osztályba sorolásának esetén nem kötelező, egyéb esetben legalább egy olyan elem megadása kötelező, amely meghatározza, hogy a vizsgálati módszer mire vonatkozik. Ez az alábbiak közül lehet egy vagy több is akár: “component” (maga az EIR), “location” (fizikai helyszín), “party” (interjún résztvevő személy vagy a szervezet maga), “inventory-item” (pl. IP cím, vizsgált adatbázis szerver). |
| │ │ │ ├── subject-uuid (string) [1] | EIR esetén a components-ben szereplő EIR egyedi UUID azonosítója.<br>Személy esetén a parties-ban szereplő személy egyedi UUID azonosítója.<br>Inventory elem esetén az inventory-items-ben megadott elem egyedi UUID azonosítója.<br>Helyszín esetén a locations-ben megadott helyszín egyedi UUID azonosítója. |
| │ │ │ ├── type (string) [1] | “component“ (maga az EIR), “location” (fizikai helyszín), “party” (interjún résztvevő személy vagy a szervezet maga), “inventory-item” (pl. IP cím, vizsgált adatbázis |

| | |
|---|---|
| | szerver) |
| └── title (string) [0 ... 1] | Opcionális rövid leírás (pl. “Az XY EIR szabályzatai”, vagy “Az interjún résztvevő CISO a szervezet részéről”) |
| ├── relevant-evidence (array of object) [1 ... ∞] | Az összes olyan evidenciát fel kell sorolni, amiket az adott megfigyelési tevékenység során az auditor vizsgált, vagy ami a tevékenység során keletkezett. Legalább egy bizonyítéknak szerepelnie kell. Itt kell, hogy megjelenjenek (a megfelelő observation alatt) a szervezet által készített EIR biztonsági osztályba sorolások, az összes szabályzat, audit és interjú jegyzőkönyv, sérülékenység vizsgálati jegyzőkönyv, screenshot-ok, napló bejegyzések, egyéb audit evidenciák. |
| ├── description (string) [1] | Az adott evidencia rövid megnevezése |
| └── links (array of object) [1 ... ∞] | Minimum egy “back-matters” ”resources” listaelemre való hivatkozás megadása kötelező, ami egyértelműen megadja, hogy hol érhető el az adott audit bizonyíték. |
| └── href (string) [1] | A back-matters resources listaelemben található dokumentum egyedi azonosítójára vonatkozó hivatkozás. |
| └── collected (string) [1] | A bizonyíték begyűjtésének időpontja. Ez a dátum- és időérték az RFC3339 által meghatározott „date-time” szerint van formázva. |
| ├── risks (array of object) [0 ... ∞] | Az egyes követelménycsoportokra vonatkozó eltéréseket tartalmazó lista. Minden egyes követelménycsoportra, ahol valamelyik elemi követelmény esetén az auditor nem teljesülést állapít meg, ezen listában szerepeltetni kell egy kockázatot, amely ismerteti az eltérés mértékét és hatását. |
| ├── uuid (string) [1] | A kockázat egyedi UUID azonosítója. |
| ├── title (string) [1] | A kockázat (eltérés) rövid megnevezése, pl.: “EIR 1 - 2.2. eltérés”. Kötelező mező. |

| | |
|---|---|
| description (string) [1] | A kockázat (eltérés) részletes leírása. Kötelező mező. |
| statement (string) [1] | Az eltérés által a rendszer biztonságára gyakorolt hatás megfogalmazása. Kötelező mező. |
| status (string) [1] | Az auditjelentésben elegendő csak a nyitott (azaz élő) eltéréseket bemutatni. Az audit során feltárt és közben javított eltéréseket nem kell szerepeltetni. A nyitott eltérések esetén ennek a mezőnek az értéke “open”. De ha az auditor a lezárt (javított) eltéréseket is be akarja mutatni, akkor “closed” státusz is alkalmazható. |
| characterizations (array of object) [1] | Kötelező pontosan egy elemet megadni az eltérés leírásával. |
| facets (array of object) [1] | Kötelező pontosan egy elemet megadni az eltérés leírásával. |
| name (string) [1] | Értéke kötelezően “severity”. |
| system (string) [1] | |
| value (string) [1] | Az értéke az alábbiak közül kerülhet ki: „elhanyagolható mértékű eltérés”, „kismértékű eltérés”, „kiemelt mértékű eltérés”, „kritikus mértékű eltérés”. |
| origin (object) [1] | Kötelező pontosan egy elemet megadni, ami a kockázat forrását jelöli. |
| actors (array of object) [1] | Legalább egy elemű lista, amely a megfelelő party-ra (személy vagy szervezet) mutat, aki az eltérést megállapította. |
| type (string) [1] | Értéke kötelezően "party". |
| actor-uuid (string) [1] | Az értéke a megfelelő auditor személy, csoport vagy szervezet egyedi UUID azonosítója. |
| findings (array of object) [1 ... ∞] | Ennek a listának minden EIR esetén minden elemi követelményre vonatkozóan tartalmaznia kell legalább egy elemet, amely az adott EIR esetén az adott elemi követelmény vizsgálati megállapításait tartalmazza. Ha egy elemi követelmény több “observation” részeként is |

| | |
|---|---|
| | vizsgálatra került, több elem is szerepelhet ugyanarra. Sem EIR-eket, sem vizsgálatokat, sem elemi követelményeket nem lehet ebben a listában összevonni egymással. Ha például az EIR 1 esetén egy elemi követelmény például dokumentumvizsgálattal és interjúval is ellenőrzésre került, úgy legalább kettő “finding” elem kell, hogy szerepeljen rávonatkozva. Ez a lista maximális részletezettséggel tartalmazza az elemi követelmények teljesülését és az auditor által elvégzett auditori tevékenységeket is.<br>Emellett a listának minden EIR esetében minden követelménycsoportra is tartalmaznia kell egy-egy elemet, amely az adott követelménycsoportra vonatkozó összefoglaló megállapítást tartalmazza. |
| ├── uuid (string) [1] | A megállapítás egyedi UUID azonosítója. |
| ├── title (string) [1] | A megállapítás rövid szöveges megnevezése. Pl.: “EIR 1 K02.002_O.2.2.1.(a) (átvizsgálás)” vagy “EIR 1 2.2. követelménycsoport megállapítás” |
| ├── description (string) [1] | A megállapítás leírása. Pl.: “A K02.002_O.2.2.1.(a) elemi követelmény nem teljesülés az EIR 1 esetében a dokumentumvizsgálat alapján, mert a szabályzat nem tartalmazza a … részeket”. Amennyiben a megállapítás az, hogy “teljesül”, az auditornak nem kell részletes indoklást adnia ebben a mezőben, mert a hivatkozott bizonyítékok önmagukban elegendőek. Amennyiben azonban a döntés “nem megfelelt”, ebben a mezőben részletes indoklás kell, amely a nem megfelelést ismerteti. |
| ├── target (object) [1] | Kötelező elem, amely az elemi követelmény és az EIR hivatkozást megadja. |
| │ ├── type (string) [1] | Elemi követelmények esetén ennek értéke kötelezően "objective-id". A teljes követelménycsoportra |

| | |
|---|---|
| | vonatkozó megállapítás esetén az értéke “statement-id”. |
| ├── target-id (string) [1] | Elemi követelmény esetén az elemi követelmény (objective) egyedi azonosítója, pl.: "K02.002_O.2.2.1.(a)". Követelménycsoport esetén a követelménycsoport azonosítója, pl.: “2.2.”. |
| ├── props (array of object) [1 ... ∞] | Minimum egy elemű lista. Az egyetlen kötelező elem az EIR-re vonatkozó hivatkozás. Emellett az auditor szabadon megadhat egyéb tulajdonságokat is, de azokhoz saját namespace-t kell definiálnia. |
| ├── name (string) [1] | EIR hivatkozás esetén az értéke kötelezően “component”. |
| ├── ns (string) [1] | |
| └── value (string) [1] | EIR hivatkozás esetén az értéke a “components”-ben megadott EIR egyedi UUID azonosítója. |
| └── status (object) [1] | Kötelező elem, amely tartalmazza az adott EIR, adott elemi követelményére vagy követelménycsoportjára az adott vizsgálat során tett megállapítását. |
| └── state (string) [1] | Értéke két féle lehet: “satisfied” (az elemi követelmény vagy követelménycsoport “megfelelt”) vagy “not-satisfied” (az elemi követelmény vagy követelménycsoport “nem megfelelt”) az adott vizsgálat alapján. |
| ├── related-observations (array of object) [1 ... ∞] | Kötelezően meg kell adni annak a vizsgálati módszernek a hivatkozását, amely alapján a megállapítás született. Elemi követelmények esetén jellemzően ez egy egyelemű lista lesz. Követelménycsoport esetén pedig az összes alá tartozó elemi követelmény összes “observation” hivatkozását tartalmazni fogja. |
| └── observation-uuid (string) [1] | Annak a vizsgálati módszernek (“observation”) az egyedi UUID azonosítója, amelynek során a megállapítás született. |
| └── related-risks (array of object) [0 ... ∞] | Amennyiben a döntés “nem |

| | |
|---|---|
| | megfelelt”, kötelező megadni egy kockázatot (eltérést), amely a nem teljesülésből adódó kockázatokat és hatást ismerteti. Ha a döntés “megfelelt” volt, nem szabad kockázatot megadni itt. “Nem megfelelt” elemi követelmény esetén jellemzően egy kockázat lesz megadva itt, követelménycsoport esetén pedig az összes alá tartozó “nem megfelelt” elemi követelmény összes kockázatának a felsorolása. |
| └── risk-uuid (string) [1] | A “risks” szekcióban megadott releváns kockázat egyedi UUID azonosítója. |
| └── back-matter (object) [1] | Kötelező elem, amely a hivatkozott dokumentumokat és evidenciákat gyűjti össze. Az audit során felhasznált összes evidenciát, jegyzőkönyvet, dokumentumot kötelező tételesen felsorolni. |
| └── resources (array of object) [2 … ∞] | Az egyes külső hivatkozásokat felsoroló lista. Legalább két jogszabályi hivatkozás kötelező. Lásd 5. kiegészítés. |
| ├── uuid (string) [1] | Egyedi UUID azonosító. |
| ├── title (string) [1] | A dokumentum vagy evidencia megnevezése. Dokumentum jellegű forrás (pl. szabályzat, jegyzőkönyv) esetén a dokumentum címe. |
| ├── props (array of object) [1 … ∞] | Legalább egy tulajdonság megadása kötelező, amely a dokumentum / evidencia típusát adja meg. |
| ├── name (string) [1] | A típust meghatározó kötelező tulajdonság esetén ennek a mezőnek az értéke “type”. |
| ├── ns (string) [1] | |
| ├── class (string) [0 … 1] | Amennyiben “evidence” típusú a tulajdonság szerint meghatározott forrás, akkor a class mező kitöltése kötelező, és ez mondja meg, milyen típusú bizonyítékról van szó. Az értéke szabadon választható, de az alábbi bizonyíték típusok esetében ezeket az értékeket kell használni: “policy”, “document”, “screenshot”, “memo”, “minutes”, “image”, “log”, “configuration”, “scan-report”, |

| | |
|---|---|
| | "script".<br>Amennyiben a forrás nem bizonyíték típusú (pl. jogszabály), akkor a class mező nem kötelező. |
| └── value (string) [1] | Szabadon megadható az értéke, de jogszabály esetén kötelezően "regulation", illetve minden bizonyíték esetén "evidence". |
| └── rlinks (array of object) [1] | Kötelező megadni minden bizonyíték esetén a forrás elérhetőségére vonatkozó információkat. |
| ├── href (string) [1] | Az auditor rendszerében a forrást egyértelműen azonosító hivatkozás (path, documentum azonosító, stb.) |
| ├── media-type (string) [0 ... 1] | Az Internet Assigned Numbers Authority (IANA) Media Types Registry 'Ital meghatározott médiatípus. |
| └── hashes (array of object) [0 ... ∞] | Legalább egy elemű lista, amely tartalmazza minimálisan az evidencia SHA256 lenyomatát. |
| ├── algorithm (string) [1] | Kötelezően „SHA-256" vagy „SHA-512". |
| └── value (string) [1] | A hivatkozott dokumentum lenyomata. |

## Kiegészítések

### 1. kiegészítés


```
{
   "id": "authority",
   "title": "Kiberbiztonsági felügyelet",
   "description": "Az SZTFH, mint Kiberbiztonsági Felügyelet"
},
{
   "id": "assessor",
   "title": "Auditor szervezet",
   "description": "Az auditot végrehajtó szervezet."
},
{
   "id": "assessment-team",
   "title": "Auditor csapat",
   "description": "Az auditot végrehajtó személyek csoportja."
},
{
   "id": "assessment-lead",
   "title": "Audit vezető",
   "description": "Az auditot lefolytató csapat vezetője."
},
{
   "id": "organization",
   "title": "Az auditált szervezet",
   "description": "Az auditot megrendelő szervezet."
},
{
   "id": "organization-team",
   "title": "A szervezet audit felelősei",
   "description": "A szervezet részéről az auditban részt vevő személyek."
}
```

**2. kiegészítés**


```
{
   "uuid": "abaf3529-cd59-4445-ae88-870695605675",
   "type": "organization",
   "name": "Szabályozott Tevékenységek Felügyeleti Hatósága",
   "short-name": "SZTFH",
   "links": [
      {
         "href": "https://sztfh.hu",
         "rel": "homepage"
      }
   ],
   "email-addresses": [
      "sztfh@sztfh.hu"
   ],
   "addresses": [
      {
         "type": "work",
         "addr-lines": [
            "Alkotás utca 50."
         ],
         "city": "Budapest",
         "postal-code": "1123",
         "country": "HU"
      }
   ],
   "remarks": "Kiberbiztonsági Igazgatóság"
}
```


**3. kiegészítés**


```
{
   "name": "state",
   "value": "initial"
}
```

## Megjegyzések

A jelentésben szereplő minden UUID egyedi azonosítónak meg kell felelnie az UUID version 4 formátumnak (RFC4122) és egyedileg generáltnak kell lennie. Az UUID-t újra használni nem megengedett az egyedi azonosítás érdekében.

Megtörténhet, hogy egy EIR esetén egy elemi követelmény a dokumentumvizsgálat során “megfelelt” (és ennek megfelelően egy ilyen “finding” rögzítésre kerül a jelentésben), majd az interjú során olyan információ merül fel, ami alapján “nem megfelelt” (és ekkor egy ilyen tartalmú “finding” is rögzítésre kerül). Ilyen esetben minden “megfelelt” és “nem megfelelt” megállapítást külön-külön rögzíteni kell. Az auditornak minden EIR esetben az adott követelménycsoport alá tartozó összes elemi követelményére tett összes megállapítás együtteséből kell meghatároznia az adott követelménycsoport teljesülését és az esetleges eltérések mértékét.

Fontos, hogy a jelentésben minden EIR minden elemi követelményének a teljesülését, és minden EIR minden követelménycsoportjának a teljesülését is szerepeltetni kell.