Magyar Rendészet 2026/3. 31–46.
DOI: 10.32577/mr.2026.3.3

INFORMATIKAI BIZTONSÁG

Kiberbiztonsági megfelelés

Fókuszban a sztenderdek

Cybersecurity Compliance

Focus on Standards

BOTTYÁN Béla,[1] BOTTYÁN László[2]

Bevezetés: A kiberbiztonsági fenyegetések száma folyamatos növekedésének és a technológiai környezet változásainak hatására a szervezetek széles körben alkalmaznak különböző sztenderdeket a kockázatok csökkentésére és a megfelelés támogatására. Ugyanakkor kevés olyan, egységes szempontrendszer szerint végzett összehasonlítás áll rendelkezésre, amely kiterjed a megközelítések gyakorlati alkalmazhatóságának és egymáshoz illeszthetőségének értékelésére is. Erre figyelemmel a tanulmány kifejezetten azt vizsgálja, hogy bizonyos sztenderdek milyen környezeti feltételek fennállása esetén adnak hatékony támogatást.

Célkitűzések: A tanulmány célja a COBIT 2019, a NIST CSF, a C2M2 és az ISO/IEC 27001:2022 sztenderdek ismertetése szintetizáló jelleggel, valamint egyes attribútumok mentén azok összehasonlítása, továbbá egy gyakorlati esettanulmányon keresztül a kiválasztás és bevezetés dilemmáinak szemléltetése.

Módszertan: A szerzők mindenekelőtt rögzítik az informatikai biztonság és a kiberbiztonság fogalmi kereteit, kiemelve, hogy a kiberbiztonságnak nem kizárólag technikai okok miatt, hanem a szervezeti és a vezetői felelősség szempontjából is relevanciája van. Ezt követően ismertetik a COBIT 2019 IT-irányítási fókuszú, érettségi szinteket és teljesítménymérést középpontba helyező

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola, e-mail: bela.bottyan@hotmail.com

[2] Doktori hallgató, Pécsi Tudományegyetem Oktatás és Társadalom Neveléstudományi Doktori Iskola, e-mail: laszlo@bottyan.com

megközelítését, illetve kitérnek a NIST CSF kockázatalapú, iparágfüggetlen, moduláris felépítésére, bemutatják továbbá a C2M2 kritikus infrastruktúrákra optimalizált érettségi modelljét, valamint az ISO/IEC 27001:2022 tanúsítható ISMS-követelményeit. A sztenderdek összehasonlításához egyedi szempontrendszert dolgoztak ki, amelynek segítségével értékelik a rendszerek célját, alkalmazhatóságát, tanúsíthatóságát, iparági fókuszát és implementációs összetettségét, rámutatva egyúttal arra is, hogy nem létezik egy valamenynyi szervezet számára egységes „legjobb megoldás", hiszen a választás alkalmával figyelemmel kell lenni többek között a szervezet egyedi céljaira és a kockázati profiljára. A cikk kiegészítő jelleggel tartalmaz egy esettanulmányt, amelyben a szerzők egy ipari nagyvállalat ISO/IEC 27001:2022 szerinti eltéréselemzésén keresztül kívánják szemléltetni a gyakorlati megvalósítással járó kihívásokat, valamint a fejlesztési javaslatok megfogalmazásának szükségességét.

Eredmények: Az összehasonlító elemzés eredményeként a szerzők rávilágítottak, hogy a COBIT 2019 a vállalati IT-irányítás és az üzleti célok összehangolásában képes magas fokú támogatást biztosítani, illetve az érettségi szemlélet is érvényesül, ugyanakkor tanúsításra nincs lehetőség. A NIST CSF moduláris felépítésének és iparágfüggetlen jellegének köszönhetően kifejezetten alkalmas a kiberbiztonsági kockázatok kezelésének elősegítésére. A rendszer érettségalapú megközelítéssel ugyan nem bír, de előnyének tekinthető, hogy más sztenderdekkel együtt is fenntartható. A C2M2 erőssége a kritikus infrastruktúrák érettségi szintjének vizsgálata és a fejlesztési területek egyértelmű azonosítása úgy, hogy az IT mellett az OT-környezetre is ráilleszthető. Az Információbiztonsági Irányítási Rendszer (ISMS) formális követelményei elsődlegesen az ISO/IEC 27001:2022 szabványra épülnek, egy kockázatalapú kontrollrendszert bocsátva az alkalmazó szervezet rendelkezésére. A tanúsíthatósága és széles körű ismertsége miatt bizalomépítő eszközként lehet rá tekinteni az üzleti kapcsolatok létesítése és fenntartása során. Ugyanakkor megállapítható, hogy az implementációja jelentős erőforrás-ráfordítást igényelhet, főként az adminisztratív terhek miatt. Ezt kiegészítve, az esettanulmány rámutatott arra, hogy nagyvállalati IT-környezetben végzett eltéréselemzéshez szükséges a hatókör tudatos megállapítása, valamint a rendszerkritikusságon alapuló priorizálás, ellenkező esetben annak elvégzése aránytalan erőforrás-ráfordítással járhat. A vizsgálat gyakorlati eredményeként létrejött az eltérések strukturált minősítése, ami közvetlenül segítette a magas kockázatok mérséklését, a jelentős fejlesztési potenciállal rendelkező területek azonosítását, valamint egy priorizált intézkedési terv összeállítását.

Konklúzió: A tanulmány legfontosabb tanulsága, hogy a kiberbiztonsági megfelelés tekintetében sem létezik egy valamennyi szervezet számára egységes „legjobb megoldás", hiszen a választás során figyelemmel kell lenni többek között a szervezet egyedi céljaira és a kockázati profiljára, így sok esetben a keretrendszerek együttes vagy kombinált alkalmazása adhatja a legnagyobb értéket. Erre figyelemmel a szerzők jövőbeli kutatási irányként

határozták meg olyan módszertanok kidolgozását, amelyek mérhető módon támogatják a különböző sztenderdek integrációját.

Kulcsszavak: kiberbiztonság, megfelelés, sztenderdek, kockázatok

Introduction: As the number of cybersecurity threats continues to increase and the technological environment evolves, organisations widely adopt various standards to reduce risks and support compliance. However, few comparisons use a uniform set of criteria and also assess the practical applicability of approaches and their ability to align with one another. With this in mind, the study specifically examines under what environmental conditions certain standards provide effective support.

Aim: The objective of the study is to present, in a synthesising manner, the COBIT 2019, NIST CSF, C2M2, and ISO/IEC 27001:2022 standards, to compare them along selected attributes, and to illustrate the dilemmas of selection and implementation through a practical case study.

Methodology: First the authors define the conceptual boundaries of IT security and cybersecurity, emphasising that cybersecurity is relevant not only for technical reasons but also from the perspective of organisational and managerial responsibility. Next, they outline COBIT 2019's IT-governance-focused approach, which centres on maturity levels and performance measurement, and discuss the NIST CSF's risk-based, industry-agnostic, modular structure. They also present the C2M2 maturity model optimised for critical infrastructures, as well as the certifiable ISMS requirements of ISO/IEC 27001:2022. To compare the standards, the authors developed a bespoke evaluation framework, which assesses the objectives, applicability, certifiability, industry focus, and implementation complexity of the systems, while also underscoring that there is no single "best solution" suitable for all organisations, since selection must take into account, among other factors, an organisation's specific goals and risk profile. As a complementary element, the article includes a case study that aims to illustrate the challenges of practical implementation and the need to formulate improvement recommendations through a gap analysis against ISO/IEC 27001:2022 conducted at a large industrial enterprise.

Results: Based on the comparative analysis, the authors highlight that COBIT 2019 can provide a high level of support for aligning corporate IT governance with business objectives and incorporates a maturity perspective; however, it is not certifiable. Owing to its modular structure and industry-agnostic nature, the NIST CSF is particularly well-suited to managing cybersecurity risks. Although it does not rely on a maturity-based approach, it has the advantage of being able to be maintained alongside other standards. The strength of C2M2 lies in assessing the maturity of critical infrastructure and clearly identifying areas for improvement, and it is applicable not only to IT but also to OT environments. The formal requirements of an Information Security Management System (ISMS) are primarily based on ISO/IEC 27001:2022, which provides the implementing organisation with a risk-based control system. Due to its certifiability and wide recognition, it can be regarded as a trust-building instrument in establishing and maintaining business relationships. It should be noted, however, that its implementation may require substantial resources, primarily because of administrative burdens. Complementing these findings, the case study shows that, in a large-enterprise IT environment, a gap analysis requires a deliberate definition of scope and prioritisation based on system criticality; otherwise, conducting it may entail disproportionate resource expenditure. As a practical outcome, a structured classification of gaps was developed, which directly supported mitigating high risks, identifying areas with significant improvement potential, and preparing a prioritised action plan.

Conclusion: The most important conclusion of the study is that, also in the context of cybersecurity compliance, there is no single "best solution" that fits all organisations, since the choice must consider, among other factors, an organisation's specific objectives and risk profile; therefore, in many cases, the parallel or combined application of frameworks may deliver the greatest value. Accordingly, the authors identify, as a direction for future research, the development of methodologies that support, in a measurable way, the integration of different standards.

Keywords: cybersecurity, compliance, standards, risks

Bevezetés

Napjainkra a kiberbiztonsági fenyegetések volumene és összetettsége jelentősen megnövekedett. Emellett azonban kihívást okoz az is, hogy a technológiai változások ütemével az érintetteknek lépést kell tartaniuk. Ezek a körülmények pedig együttesen indokolják a tudatos, egyedi és kockázatarányos védekezési mechanizmusok keresését, fejlesztését és alkalmazását.

E tanulmányban a kiberbiztonsági megfelelést célzó jó gyakorlatokat, valamint azokat a sztenderdeket kívánjuk számba venni, szintetizálni és összehasonlítani, amelyek érdemben elősegíthetik a kiberbiztonsági kockázatok csökkentését.

Mindenekelőtt a a) kapcsolódó fogalmak tisztázását, majd b) az egyes sztenderdek főbb jellemzőit ismertetjük, ezt követően c) saját szempontrendszer segítségével összehasonlítjuk őket, bemutatva az összevetés eredményét, végül d) egy esettanulmány segítségével ismertetünk bizonyos gyakorlati megoldásokat.

Fogalmi alapvetés

Mindenekelőtt az informatikai biztonság és a kiberbiztonság fogalmát szükséges tisztázni. Az elektronikus információs rendszer biztonságának definíciója esetében a kiindulópont az, hogy a védelem alapvető tárgya az adat, de az adatot kezelő rendszerelemek is védendők, hiszen ezek megfelelő állapota szükséges az adat védelméhez (Gyaraki 2023). Az információs rendszer biztonsága

> „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos" (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról).

Az adatot mint a támadások alapvető célját a következő rendszerelemek veszik körül: az információs rendszer fizikai környezete és infrastruktúrája, hardver, a kommunikáció, hálózat, az adathordozók, a szabályozás, a szoftver és a személyi környezet. E rendszerelemekre különböző fenyegetések hatnak, amelyek a rendszerelemek meghatározott láncán keresztül az adatokat veszélyeztetik (Muha 2004).

Ehhez képest a kiberbiztonság

> „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez" (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról).

Ezzel kapcsolatban kiemelendő, hogy a kiberbiztonság megteremtése és fenntartása tehát nemcsak műszaki jellegű probléma, ami az informatikai rendszer működtetését végző személyek feladata, hanem ezzel kapcsolatban a szervezet valamennyi munkatársát és az irányító testület(ek) tagjait is felelősség terheli (Kocziszky–Kardkovács 2020).

COBIT

A COBIT (Control Objectives for Information and related Technology) ajánlást egy amerikai székhelyű szövetség, az ISACA (Information Systems Audit and Control Association) dolgozta ki.

A COBIT keretrendszert az ISACA első ízben 1996-ban tette közzé. A COBIT első verziójának céljaként a vállalati IT-irányítás és a menedzsment támogatása említendő meg, miközben a hangsúly a kontrollcélokon volt. Ezt a változatot 1998-ban a COBIT 2.0 váltotta fel, amely továbbfejlesztés eredményeként kiegészült új kontrollcélokkal és útmutatásokkal. A 2000-ben megjelent COBIT 3.0 már jelentős frissítést hozott, így különösen az IT-folyamatok érettebb menedzselését segítette elő. Ezt követően az ISACA a COBIT 4.0 és 4.1 (2005, 2007) verziókat tette közzé, amelyeknél a hangsúly a vállalatirányítási szempontok integrálására, valamint a kockázat- és teljesítménymenedzsment támogatására helyeződött át. A keretrendszer fejlődése 2012-ben érkezett újabb mérföldkőhöz a COBIT 5 változat megjelenésével. Ez a verzió a korábbiakhoz képest egy még átfogóbb, stratégiai szempontokat is tartalmazó keretrendszerré vált, amely az egész vállalatirányítást le kívánta fedni. Ez megnyilvánult többek között abban is, hogy a teljesítménymenedzsment, a kockázatkezelés és megfelelés *(compliance)* integrációjára is nagy figyelmet fordított (Kő 2014). A legfrissebb verzióként a COBIT 2019-et tartjuk számon, amely tovább finomította a COBIT 5-öt, és rugalmasabb keretrendszert kínál a modern IT-irányítási és menedzsmentkövetelményekhez, különösen a digitális transzformációt támogató folyamatokhoz.

A COBIT egy irányítási eszköz, alkalmazása elősegíti az információval, valamint az információtechnológiával kapcsolatos kockázatok és előnyök megértését, kezelését. Elsősorban üzleti vállalkozások számára készült, nemzetközileg elfogadott és fejlesztett „keretrendszer", amelynek célja az információtechnológiai szolgáltatások és a szervezet működési folyamatainak egymással való összehangba hozatala, az informatikai kockázatok kezelése, informatikai jellegű jogszabályoknak, szabványoknak való megfelelés, továbbá az informatikai szolgáltatások meghatározott szempontok szerinti mérése azok biztonsági és irányítási jellemzői útján (Michelberger 2024).

A COBIT keretrendszer 6 irányelvet jelöl ki, nevezetesen (a) az értékteremtést, (b) a holisztikus megközelítést, (c) a dinamikus irányítási rendszert, (d) az irányítási és menedzsmentfolyamatok elkülönítése, (e) a vállalati igényekhez való igazítást, valamint (f) az *end-to-end* megoldásokat (Harisaiprasad 2020).

A COBIT 2019 öt területre osztva irányítási és menedzsment-célkitűzéseket vázol fel (1. táblázat).

1. táblázat: A COBIT 2019 irányítási és menedzsment-célkitűzései

Irányítási és menedzsmentterület	Leírás
Összehangolás, tervezés és szervezés (*align, pland and organise,* APO)	Magában foglalja a biztonság és a kockázatok kezelését
Fejlesztés, beszerzés és bevezetés (*build, acquire and implement,* BAI)	A változások és a kérések kezelésére összpontosít
Szolgáltatásnyújtás és támogatás (*deliver, service and support,* DSS)	Hatékony szolgáltatásnyújtást és incidenskezelést biztosít
Felügyelet, értékelés és vizsgálat (*monitor, evaluate and assess,* MEA)	Az informatikai folyamatok felügyeletére, teljesítményük értékelésére és a szabályozásoknak való megfelelés biztosítására összpontosít (Putra–Wahyuningtyas 2023)
Értékelés, irányítás és monitorozás (*evaluate, direct and monitor,* EDM)	Biztosítja a kockázatok optimalizálását és a szervezeti célokhoz való igazítását

Forrás: a szerzők szerkesztése

Minden terület konkrét folyamatokat – összesen negyvenet – tartalmaz, amelyeket a szervezetek végrehajthatnak az informatikai irányítás javítása érdekében (Beato–Indah Fianty 2024).

A COBIT 2019 egyik fontos jellemzője, hogy a teljesítmény mérését és a folyamatos fejlesztést helyezi a középpontba, hangsúlyozza a teljesítménymutatók fontosságát az informatikai irányítás hatékonyságának értékelésében (Indah Fianty – Brian 2023). Ezenkívül a keretrendszer 0-tól (nem létező) 5-ig (optimalizált) terjedő skálán érettségi szinteket határoz meg, lehetővé téve a szervezetek számára, hogy felmérjék jelenlegi érettségüket és azonosítsák a fejlesztésre szoruló területeket. A gyakorlatban a szervezetek gyakran a 2. szinten helyezkednek el, és a 3. szint elérését tűzik ki célul, jelezve, hogy továbbfejlesztett gyakorlatokra van szükség. Mindez arra vezethető vissza, hogy az érettségi szintek és a teljesítménymenedzsment közötti kölcsönhatás elősegíti a folyamatos fejlesztés kultúráját. A szervezetek rendszeresen értékelhetik folyamataikat, és teljesítménymutatók alapján korrekciós és fejlesztési intézkedéseket hajthatnak végre, ezáltal javítva általános informatikai irányításukat.

A COBIT 2019 megalkotásánál törekedtek arra, hogy az egyes komponensek egymással összhangban működjenek, elősegítve ezzel az informatikai megoldások interoperabilitását, valamint az üzleti célok támogatását. Ennek egyik példája, hogy az APO-terület a kapcsolatok és kockázatok kezelésére összpontosít, amelyek elengedhetetlenek a stratégiai célok eléréséhez.

Megjegyzendő, hogy a COBIT-nek nem kifejezett célja más szabványokba való beépülés, ugyanakkor több megfeleltetés is készült az ISACA szervezésében, például az ITIL, ISO/IEC 27002 és PMBOK szabványokkal való összeegyeztethetőség biztosítása érdekében (Szádeczky 2014).

NIST Security Framework

A National Institute of Standards and Technology (NIST) első Kiberbiztonsági Keretrendszere (Framework for Improving Critical Infrastructure Cybersecurity) 2014 februárjában látott napvilágot többéves közös munka eredményeként, az iparág, az akadémiai tagok, illetve a kormányzat képviselőinek bevonásával. Az első verzió elsődlegesen azokat a szervezeteket célozta, amelyek az amerikai kritikus infrastruktúra részének tekintendők. Az 1.1-es változatot 2018-ban jelentették be egy olyan többéves felülvizsgálat eredményeként, amelynek keretében figyelemmel voltak a keretrendszer implementálásának egyszerűsítésére, valamint a tartalom aktualizálására is, nevezetesen a hitelesítés és azonosítás, a kockázatelemzés, a kiberbiztonság és az ellátási láncok összefüggései, továbbá a biztonsági rések tárgykörébe tartozó normák módosítására. Újdonságként értékelhető az is, hogy egy külön fejezet rendelkezett az önértékelésről, amely a kiberbiztonsági kockázatértékelés lebonyolítását segíti elő. A CSF 2.0 előkészítése során azt célozták, hogy a sztenderd még általánosabban alkalmazható legyen függetlenül az adott szervezet által foglalkoztatott munkavállalók számától, a tevékenységét meghatározó ágazat jellegétől, valamint a biztonsági fejlettségének szintjétől (Nemzeti Kibervédelmi Intézet 2024).

A sztenderd céljai között szerepel a kockázatok kezelése, a folyamatok javítása, illetve a jó gyakorlat kialakítása, valamint a kiberbiztonsági tárgykörben folytatott kommunikáció egységesítése. A NIST CSF három pillérre épül: a) *core* (mag); b) *implementation tiers* (megvalósítási szintek) és c) *profile* (profil) (NIST 2024).

A keretrendszer magja hat fő funkciót jelöl ki, nevezetesen az azonosítást, a védelmet, az észlelést (detektálást), a reagálást, a helyreállítást és az irányítást (NIST 2024). Az azonosítás a szervezet informatikai és üzleti környezetének megértése, beleértve az eszközöket, adatokat, szoftvereket és a hozzájuk kapcsolódó kockázatokat. A védelem a kiberbiztonsági kockázatok megelőzését szolgáló intézkedések bevezetését foglalja magában, például a hozzáférés-kezelést, az adatvédelmet, a tréningeket és a megfelelő biztonsági rendszerek kialakítását. A detektálás a fenyegetések észlelését és az informatikai rendszerek folyamatos figyelemmel kísérését jelenti. A reagálás célja a kiberbiztonsági események kezelésére alkalmas eljárások kidolgozása és végrehajtása, ideértve a gyökérokok elemzését, az incidensek kategorizálását, illetve az információk gyűjtését és továbbítását. A helyreállításhoz a szolgáltatások és rendszerek – kiberbiztonsági események bekövetkezését követő – visszaállítása, valamint a gyakorlati tapasztalatok hasznosítása tartozik. Az irányítás 2024-ben került be a felsorolásba, amellyel a keretrendszer egy korábban hiányzó, a kockázatkezelés szempontjából alapvető irányítási elemmel egészíti ki a NIST keretrendszerét (Nemzeti Kibervédelmi Intézet 2024).

A megvalósíthatósági szintek az érettségi szintet jelzik, amely alapján a szervezetek értékelhetik a kiberbiztonsági képességeiket. Az első szint az úgynevezett részleges *(partial),* miszerint nincs formalizált kiberbiztonsági megközelítés, a biztonsági tevékenységek *ad hoc* módon zajlanak. A következő szint a kockázattudatos *(risk informed),* ami azt jelenti, hogy a kiberbiztonsági tevékenységek nemzeti szinten következetesek, de a kockázatok kezeléséhez kapcsolódóan részleges rendszerek állnak rendelkezésre. Harmadik fokozat az ismételhető *(repeatable),* vagyis a szervezeten belüli folyamatok szabályozottak, ismételhetők, és rendszeresen végrehajtják azokat (NIST 2024). A sztenderd besorolása szerint a legmagasabb szint az adaptív *(adaptive):* a szervezet a legjobb gyakorlatokat alkalmazza, és képes dinamikusan reagálni a változó kockázati környezetre.

A profil abban segíti a szervezeteket, hogy azonosítsák és összehangolják a kiberbiztonsági céljaikat az üzleti céljaikkal, valamint azonosítsák a jelenlegi kiberbiztonsági érettségi szintjüket és a kívánt jövőbeli állapotot. A profil megmutatja, hogy a szervezet milyen helyzetben van jelenleg (jelenlegi profil) és hova szeretne eljutni (célprofil).

C2M2

A C2M2-t az Egyesült Államok Energiaügyi Minisztériuma (DOE), magán- és közszféra szakértői, valamint az energiaszektoron belüli eszköztulajdonosok és üzemeltetők képviselői közösen fejlesztették ki. 2012-es megjelenése óta széles körben használják önértékelések támogatására az energiaszektorban és más ágazatokban. Az 1.1-es verzió 2014-ben, a 2.0-s verzió 2021-ben, a 2.1-es verzió pedig 2022-ben jelent meg (U.S. Department of Energy 2021). A C2M2 egy érettségi modellt követ, amely lehetőséget ad a szervezetek számára, hogy felmérjék jelenlegi kiberbiztonsági érettségüket, és tervet készítsenek annak fejlesztésére (Sri et al. 2019).

A modell 10 különböző kiberbiztonsági területre oszlik, amelyek lefedik a kiberbiztonság egyes részeit: a) az informatikai eszközök, rendszerek változás- és konfigurációmenedzsmentje; b) kockázatok azonosítása, elemzése és mérséklése; c) fenyegetések és sérülékenységek felismerése és kezelése; d) identitás- és hozzáférés-kezelés (IAM); e) incidenskezelés és üzletmenet-folytonosság biztosítása; f) harmadik személyekkel (külső partnerekkel) összefüggésben felmerülő kockázatok kezelése; g) kiberbiztonsági szakértelem és tudatosság biztosítása; h) kiberbiztonsági program tervezése, irányítása és működtetése; i) erőforrás-menedzsment; j) kiberbiztonsági architektúra (U.S. Department of Energy 2021).

A modell valamennyi területhez érettségi szinteket rendel, amelyek a következők lehetnek: a) nincs kialakított gyakorlat (MIL0); b) van gyakorlat, de *ad hoc* jellegű (MIL1); c) a folyamatokat dokumentált módon hajtják végre (MIL2); d) a tevékenységek szabályozva vannak (MIL3). A sztenderd szerint „MIL2” szintként értékelhető az, ha dokumentáltság mellett már megfelelő erőforrásokat biztosítanak a végrehajtáshoz és a gyakorlat kiforrottabb, mint a „MIL1”-nél. A legmagasabb szint esetében a felelősségi körök tisztázottak, az elszámoltathatóság biztosított, illetve általánosságban rendelkezésre állnak a szükséges felhatalmazások a folyamatok végrehajtásához amellett, hogy a tevékenységek hatékonyságát folyamatosan mérik és értékelik.

Noha a C2M2 modellt elsősorban az energiaszektor és a kritikus infrastruktúrák védelmére fejlesztették ki, más iparágakban is alkalmazható, például a pénzügyi szektorban, a közlekedésben vagy az egészségügyben. A modellt széles körben vezetik be közép- és nagyvállalatok, valamint a kormányzati szervezetek körében, amelyek kritikus rendszereket és szolgáltatásokat üzemeltetnek.

A modell elsődleges célja tehát, hogy értékelés útján átfogó képet adjon a szervezeteknek arról, milyen szinten állnak kiberbiztonsági érettségükben. Emellett a sztenderd segítséget nyújt abban is, hogy ezek az entitások a hiányosságaikat azonosítsák és megfogalmazzák a biztonsági képességek fejlesztésére irányuló intézkedéseket.

ISO 27001

Az ISO 27001 egy nemzetközi szabvány, amely az információbiztonság irányítási rendszerének (Information Security Management System, ISMS) követelményeit határozza meg. Célja, hogy segítse a szervezeteket az információik védelmében az adatvesztés, adatszivárgás, illetéktelen hozzáférés vagy bármilyen egyéb biztonsági incidens ellen.

A 27000-es szabványcsalád alapjai a brit BS 7799 szabványhoz nyúlnak vissza, amelyet az Egyesült Királyságban 1995-ben publikáltak, elérhetővé téve ezzel az első átfogó információbiztonsági irányítási keretrendszert. A szabvány két részből állt, a BS 7799-1 az információbiztonsági kontrollokra és legjobb gyakorlatokra vonatkozott, míg a BS 7799-2 az információbiztonsági irányítási rendszer (ISMS) követelményeit fogalmazta meg. A BS 7799-1 szabványt az ISO 2000-ben átvette, és ISO/IEC 17799 néven publikálta. Ez a szabvány globális keretrendszert hozott létre a biztonsági kontrollok számára, és hamar elismertté vált világszerte. Az ISO/IEC 27001 szabvány 2005-ben jelent meg, amely a BS 7799-2 átdolgozott változata volt, és az információbiztonsági irányítási rendszer követelményeit határozta meg. Ezzel egy időben döntés született a 27000-es szabványcsalád létrehozásáról, amely a különböző aspektusokra és szakterületekre szabott további szabványokat foglalta volna magában. Az ISO folyamatosan újabb és újabb szabványokat adott ki, hogy kiterjessze a 27000-es szabványcsaládot az információbiztonság speciális területeire. 2022-ben megjelent az ISO/IEC 27001 legújabb változata, amely új kontrollokat és modernizált követelményeket vezetett be. Szintén 2022-ben frissült az ISO/IEC

27002, amely a kontrollok végrehajtását támogató legjobb gyakorlatokat tartalmazza, így még inkább igazodik a mai információbiztonsági környezethez.

Az ISO 27001:2022 szabvány rendeltetése, hogy az alkalmazása során biztosítsa az adatok bizalmasságát, sértetlenségét és rendelkezésre állását, valamint a működést fenyegető kockázatok kezelését és csökkentését, többek között incidenskezelési és üzletmenet-folytonossági eljárások javítása, illetve biztonságtudatos vállalati kultúra kiépítése útján.

Az ISO/IEC 27001:2022 szabvány három fő részre bontható: a) az ISMS kialakítása és működtetése (fő szabvány); b) melléklet (Annex A) biztonsági kontrollok listája; c) PDCA-ciklus *(plan-do-check-act)*.

A szabvány az első részében az információbiztonsági irányítási rendszer követelményeit definiálja, amit a szervezetek az ISMS létrehozásához és fenntartásához követhetnek. A szabvány előrebocsátja a szabvány általános célját és alkalmazási területét, valamint azt, hogy az ISMS tervezése során figyelembe kell venni a szervezet környezetét mind a külső, mind a belső tényezőket, ideértve az érdekelt felek elvárásait is. A dokumentum rögzíti, hogy a felső vezetésnek támogatnia kell és aktívan részt kell vennie az ISMS bevezetésében, különben az implementálás nem lesz sikeres. A szabvány ezt követően rendelkezik a kockázatelemzésről és a kockázatkezelési folyamatokról, az információbiztonsági célok meghatározásáról, az ISMS fenntartásához szükséges erőforrások biztosításáról és a szükséges képzésről, de külön-külön fejezetet szentel a működtetésnek, a teljesítményértékelésnek és a fejlesztésnek is.

Az Annex A rész tartalmazza a 93 kontrollt, amelyeket a szervezet kockázatelemzés alapján alkalmazhat. A kontrollok négy fő kategóriája a szervezeti kontrollok, az emberi erőforráshoz kapcsolódó kontrollok, a fizikai és környezeti kontrollok és a technológiai kontrollok. A kontrollok tehát különböző területeken és szinteken építendők be a működésbe.[3] Az új kontrollok a modern kiberbiztonsági igényekhez illeszkednek, így például nagyobb hangsúlyt fektetnek a felhőalapú rendszerek védelmére, a végpontbiztonságra és az adatvédelemre. A kontrollok célja az, hogy segítsenek a szervezeteknek az információbiztonság különböző aspektusainak figyelembevétele során.

A szabvány a PDCA-ciklust használja az ISMS folyamatos fejlesztéséhez.[4] A tervezés keretében az információbiztonsági célok és kockázatkezelési intézkedések meghatározását, a végrehajtás során az ISMS tervezett elemeinek bevezetését, az ellenőrzés a teljesítményértékelést és az esetleges problémák feltárását jelenti, míg az intézkedés a rendszer fejlesztését foglalja magában a folyamatos javítás érdekében (Vértesy 2012).

---

[3] Például vezetői támogatás, kockázatkezelési eljárások, alkalmazottak felvétele és elbocsátása, a helyiségek és létesítmények fizikai védelme, hozzáférés-kezelés, vírusvédelem, titkosítás stb.

[4] Vértesy 2014: 148–149.

Összehasonlítás

Az egyes sztenderdeket egyedi szempontrendszer alapján érdemes összehasonlítani. A komparatív megközelítés alapjául a sztenderdek főbb elemei, az alkalmazhatóságuk, valamint a bevezetéssel összefüggő gyakorlati tapasztalatok szolgáltak (2. táblázat).

2. táblázat: A sztenderdek összehasonlítása

Jellemző *(Attribute)*	COBIT	NIST CSF	C2M2	ISO/IEC 27001:2022
Elsődleges cél *(primary objective)*	IT-irányítás és -menedzsment biztosítása	Kiberbiztonsági kockázatok kezelése	Érettségi szint meghatározása	Információbiztonság növelése
Alkalmazási terület *(scope of application)*	IT- és üzleti folyamatok	Kiberbiztonság bármely területe	Kritikus infrastruktúra	Valamennyi iparág
Tanúsíthatóság *(certifiability)*	Nem	Nem	Nem	Igen
Érettségi modell *(maturity model)*	Igen	Nem	Igen	Nem
Specifikus iparági fókusz *(industry-specific focus)*	Nem	Nem	Igen	Nem
Nemzetközi alkalmazás *(international adoption)*	Igen	Igen	Korlátozott	Igen
Integrált jelleg mértéke *(level of integration)*	Magas	Közepes	Közepes	Magas
Implementálás összetettségének mértéke *(implementation complexity)*	Közepes	Alacsony	Alacsony	Magas

Forrás: a szerzők szerkesztése

A COBIT előnye, hogy a megfelelő implementálás és fenntartás esetén elérhető az IT-stratégia és az üzleti stratégia összehangolása, valamint részletes, érettségi modelleket is tartalmaz *(capability maturity model)*. Tanúsítani nem lehet, de az alkalmazhatósága rendkívül széles körű. A NIST CSF kockázatalapú megközelítésből indul ki, amely hosszú távú megoldást nyújt a folyamatos fejlesztés biztosításához. Amellett, hogy rugalmas, moduláris felépítésének köszönhetően könnyen alkalmazható bármely iparágban és integrálható más szabványokkal. A C2M2 legfőbb célja, hogy a kritikus infrastruktúrák kiberbiztonsági érettségi szintjét felmérje és javítsa 10 terület lefedésén keresztül. Előnyei között megemlítendő az is, hogy nem kizárólag az IT-ra, hanem az operációs technológiákra (OT) is vonatkozik. Az ISO 27001 rendeltetése az információbiztonsági irányítási rendszerek (ISMS) szabványosítása, amely bármely iparágban implementálható. Követelményeket határoz meg az információbiztonsági rendszerek kiépítéséhez, működtetéséhez, fenntartásához és folyamatos javításához úgy, hogy egyúttal a kockázatértékelésre és kontrollintézkedésekre helyezi a hangsúlyt. Egyedisége abban áll, hogy tanúsítható sztenderd, emiatt nemzetközileg is széles körben elismert.

Esettanulmány

Egy ipari szektorban tevékenykedő nagyvállalat célul tűzte ki, hogy megvizsgálja a jelenleg alkalmazott információbiztonsági irányítási rendszerét és eltéréselemzést készítsen a jelenlegi kontrollkörnyezetre az ISO/IEC 27001:2022 szabvány szerint. Az eltéréselemzés elvégzésével az IBIR adott időállapotban meglévő gyengeségeket és hiányosságokat kívánta azonosítani annak érdekében, hogy az erőforrásokat a legkritikusabb területekre összpontosítsa.

Az alkalmazandó szabvány kiválasztásánál a cég több szempont alapján mérlegelt. Egyrészt az ISO 27001 tanúsítható, azaz a szervezet hivatalosan is igazolhatja az információbiztonság iránti elkötelezettségét az üzleti partnerei és az ügyfelei felé. Ez különösen fontos a hasonló nemzetközi piacokon működő vállalatok számára, mivel ez erősítheti a bizalmat és növelheti a versenyelőnyt. Másrészt ugyanezen nagyvállalat több eltérő méretű és tevékenységű leányvállalatai révén az európai és Európán kívüli piacon is jelen van, és a különböző országokban egységes információbiztonsági keretrendszert kívánt alkalmazni. A szabvány olyan rugalmas kereteket biztosít, amellyel a szervezeten belül csak egy konkrét altevékenységre, üzleti egységre, vagy akár egy adott termékre is alkalmazható a tanúsítás anélkül, hogy az egész vállalatcsoportnak tanúsítottnak kellene lennie. Ez a megoldás lehetőséget biztosít a menedzsment számára, hogy ütemezetten határozza meg és döntsön az alkalmazási területről. Ebben az esetben ugyanakkor alapvető követelmény annak egyértelmű meghatározása, hogy a tanúsítás pontosan melyik területre vonatkozik, amit feltüntetnek a tanúsítványon is.

Az elemzés szempontjából lényeges körülmény, hogy az említett nagyvállalat informatikai architektúrája rendkívül heterogén, ugyanakkor a legfontosabb üzleti folyamatok és a hozzájuk kapcsolódó informatikai rendszerek jellemzően központosítottak, azok száma több százra tehető. Az informatikai szervezet legnagyobb része a központban helyezkedik el, és üzemeltetésre, infrastruktúrára, IT-projektmenedzsmentre, architektúrára, fejlesztésre és információbiztonságra oszlik. A fent említett körülmények miatt a szakértők az eltéréselemzést nem terjesztették ki valamennyi rendszerre, mivel sem az ehhez szükséges erőforrás nem állt rendelkezésre, sem a várható eredmény nem állt volna arányban a szükséges erőforrás-ráfordítással. Ezért a vállalat úgy döntött, hogy a) tovább szűkíti az alkalmazási területet, valamint b) egy rendszerkritikusság-elemzést folytat le.

A szűkítés eredményeként csak a központi informatikai rendszerelemek kerültek be a leltárba, valamint a termelési és egyéb automatizálási (*operation technology,* OT) rendszereket kizárták, az alkalmazási terület tehát csak az irodai és gyártástámogatási informatikára (IT) terjedt ki.

A rendszerkritikusság-elemzéshez meg kellett határozni a szempontokat, amelyek fontossági sorrend felállítását képezik. Ennek fontosabb kritériumai a 3. táblázatban láthatók. A rendszerkritikusság-elemzés elvégzése során a vállalat szakértői – valamennyi releváns körülmény értékelése alapján – az öt legfontosabb rendszerként a következőket azonosították:

- az integrált üzleti folyamat kezelő rendszer (ERP);

- a felhasználók, csoportok és erőforrások központosított kezelésére szolgáló tartományvezérlő rendszer *(active directory)* és annak elemei;
- a munkavállalók időgazdálkodására, személyügyi adminisztrációjára, kommunikációjára, kompetenciamérésére szolgáló HR-rendszer;
- a gyártási folyamatok digitális felügyeletéért, támogatásáért és irányításáért felelős gyártási kivitelezési rendszer (MES);
- az üzleti tevékenységéhez szükséges napi pénzügyi műveletek végzéséért felelős kincstári *(treasury)* rendszer.

3. táblázat: A rendszerkritikussági szempontrendszer

Kritikusság *(criticality)*	Adatosztály *(data class)*	Adatvédelem / GDPR *(privacy/* GDPR)	Üzletmenet-folytonosság / rendelkezésre állás (BCP/*availability*)	Pénzügyi hatás *(financial)*	Stratégiai hatás *(strategy)*	Jogi/hatósági kitettség *(legal)*	Reputációs hatás *(reputational)*
Magas *(high)*	Bizalmas / szigorúan bizalmas adat érintett	Nagy mennyiségű személyes adat érintett, vagy egyéb GDPR-megállapítás magas bírságot eredményezhet	A rendszernek elérhetőnek kell lennie < 4 órán belül	Pénzügyi veszteség > 1 000 000 EUR	Az éves üzleti stratégia jelentős/mérvadó módosulása várható	Hatósági megállapítás és/vagy bírság nemmegfelelőség miatt	Nemzetközi és hazai médiafigyelem
Közepes *(medium)*	Belső adat érintett	Személyes adat szivárog ki, vagy GDPR-sértés történik	A rendszernek elérhetőnek kell lennie < 24 órán belül	Pénzügyi veszteség < 1 000 000 EUR, de > 500 000 EUR	Az éves üzleti stratégia mérsékelt módosulása várható	Hatósági jelentéstétel / észrevétel nemmegfelelőség miatt	Helyi médiafigyelem
Alacsony *(low)*	Jelentéktelen belső adat vagy nyilvános adat érintett	Csekély mennyiségű vagy jellegű személyes adat érintett; nem valószínű GDPR-sértés	A rendszer elérhetősége > 1 nap	Pénzügyi veszteség < 500 000 EUR	Az éves üzleti stratégia nem vagy nem jelentősen módosul	Nincs jelentős nemmegfelelőség; legfeljebb belső szabályzatok megsértése	Nincs jelentős figyelem; legfeljebb egy szűk ügyfélkör érintett

Forrás: a szerzők szerkesztése

Az alkalmazási terület meghatározása után szisztematikus információgyűjtés következett; a szakértők többek között áttanulmányozták a vizsgált rendszerek szempontjából releváns informatikai és biztonsági szabályzatokban és eljárásrendekben foglaltakat, és vizsgálták a folyamatokat, valamint mélyinterjúkat készítettek az egyes rendszerek, illetve rendszerelemek működéséért felelős informatikai és biztonsági személyzet tagjaival.

Az elemzés keretében az interjúk során elhangzott információk, illetve az azok alapján készült és ellenőrzött leiratok tartalmát összevetették az ISO 27001 szabvány követelményeivel, ideértve az információbiztonsági irányítási rendszerre (IBIR) vonatkozó és az ISO/IEC 27002 kontroll-listában szereplő elvárásokat is. A jelenlegi helyzetnek a szabvány egyes követelményeivel való összevetése mutatott rá a tényleges eltérésekre. Noha a szabvány nem határoz meg külön skálát a nemmegfelelőségek mértékének kimutatására, az eltérések azonosítása érdekében – összhangban a piaci gyakorlattal – az eltérés szignifikanciáját négyfokú skálán jelölték:

- megfelel a szabvány szerint;
- jelentős *(major)* nemmegfelelőség;
- kisebb *(minor)* nemmegfelelőség;
- fejlesztési javaslat *(observation)*.

A szakértők az eltéréselemzés segítségével különböző fejlesztési lehetőségeket azonosítottak, többek között az üzletfolytonosság, mentéskezelés, IT-katasztrófa-helyreállítás (5.29; 5.30; 8.13; 8.14), az ellátási lánc és külső szolgáltatók (5.19; 5.20; 5.21; 5.22; 5.23), valamint alkalmazásbiztonság és biztonságos szoftverfejlesztés (8.25; 8.26; 8.27; 8.28; 8.29; 8.30) területén.

Összegzés

A jelen tanulmányban részletezett sztenderdek mindegyikének számos előnyös tulajdonsága van. A COBIT az IT-irányításra és az üzleti célok támogatására fókuszál, a NIST CSF kiberbiztonsági keretrendszer rugalmas és iparágfüggetlen. A C2M2 kritikus infrastruktúrákra specializált, érettségi modelleket kínál, míg az ISO/IEC 27001 nemzetközi információbiztonsági szabvány tanúsítható. Az adott szervezetnek az azonosított kockázatok figyelembevételével, valamint a saját kitűzött célja és az iparági követelmények alapján érdemes mérlegelnie a sztenderdek tulajdonságait, és kiválasztani a számára megfelelőnek tartott keretrendszert, illetve ezek valamilyen kombinációját.

Az elmúlt években növekvő gyakorisággal megjelenő fenyegetések, mint például a *ransomware* vagy a DDoS-támadások jelentős működési zavarokat okozhatnak a szervezetek életében (ENISA 2024), ezért az üzletmenet-folytonosság *(business continuity)* napjainkra szorosan kapcsolódik az információbiztonsághoz. Az üzletmenet-folytonosság nem csak az esettanulmányban említett nagyvállalatnál jelentkezett hiányosságként, mindez összhangban áll a piaci tapasztalatokkal. A KPMG tanácsadó cég által készített körkép alapján 2017-ben a válaszadók 22%-a, 2018-ban 20%-a nem rendelkezett üzletfolytonossági programmal, közel egyharmaduk esetében a program még kezdeti szakaszban volt (KPMG 2013). Az információbiztonság kérdésköre az ellátási láncokban különösen aktuális napjainkban, tekintettel arra, hogy a modern gazdaságban az ellátási láncok összetettsége és globális jellege jelentős kockázatokat hordoz. A hálózatba kapcsolt vállalatok esetében kiemelten fontos annak meghatározása is, hogy mely személyek, milyen időpontban és módon férhetnek hozzá a szükséges információkhoz, illetve mikor kezdeményezhetnek vagy módosíthatnak egy belső vagy vállalatok közötti üzleti tranzakciót (Michelberger–Lábodi 2009).

Az eltérések feltérképezése során problémát jelentett, hogy az ellátási láncban részt vevő beszállítók, illetve partnerek eltérő biztonsági szintekkel rendelkeznek, és sok esetben a szerződések sem elég átláthatók a biztonsági követelményekre vonatkozóan. A biztonságos szoftverfejlesztés integrálása az alkalmazások tervezésébe és megvalósításába segít abban, hogy az információs rendszerek ne csak funkcionalitásban, hanem biztonság terén is megfeleljenek a kor kihívásainak, például rosszindulatú kódok beágyazásának, SQL-injekciónak vagy egyéb adatszivárgásnak. A 8.28 biztonságos kódolás *(secure coding)* egy teljesen új kontroll, amelyet az ISO szabvány 2022-es verziójában vezettek be. Ez a kontroll lehetővé teszi a szervezetek számára, hogy megelőző intézkedéssel csökkentsék a keletkező biztonsági kockázatokat és sebezhetőségeket, amelyek a rossz szoftverkódolási gyakorlatból eredhetnek.

Összességében az esettanulmány alátámasztotta, hogy a megfelelő sztenderd kiválasztása mellett fontos az adott szervezeti igényekhez és problémákhoz illeszkedő eszközök tudatos kiválasztása és alkalmazása. A vizsgált esetben az eltéréselemzésnek nélkülözhetetlen szerepe volt egy intézkedési terv kidolgozásában és jóváhagyásában, amelyek megvalósítása érdemben hozzájárult a kockázatok csökkentéséhez.

Felhasznált irodalom

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Online: https://njt.hu/jogszabaly/2013-50-00-00

Beato, Jonathan – Indah Fianty, Melissa (2024): COBIT 2019 Framework: Evaluating Knowledge and Quality Management Capabilities in a Printing Machine Distributor. *Journal of Information Systems and Informatics,* 6(1), 1–12. Online: https://doi.org/10.51519/journalisi.v6i1.638

European Union Agency for Cybersecurity (ENISA) (2024): *ENISA Threat Landscape 2024*. Heraklion: ENISA. Online: https://doi.org/10.2824/0710888

Gourisetti, S. N. G. et al. (2019): Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2): Next-Generation Cyber Resilience by Design. *NCS'19: Proceedings of the Northwest Cybersecurity Symposium,* 1–9. Online: https://doi.org/10.1145/3332448.3332461

Gyaraki Réka szerk. (2023): *Az információbiztonság alapjai*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://doi.org/10.37372/mrttvpt.2023.3

Harisaiprasad, Kumaragunta (2020): *COBIT 2019 and COBIT 5 comparison*. ISACA. Online: www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

Indah Fianty, Melissa – Brian, Maximillian (2023): Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company. *Journal of Information Systems and Informatics,* 5(2). Online: https://doi.org/10.51519/journalisi.v5i2.492

Kocziszky György – Kardkovács Kolos (2020): *A compliance szerepe a közösségi értékek és érdekek védelmében*. Budapest: Akadémiai. Online: https://doi.org/10.1556/9789634545972

Kő Andrea szerk. (2014): *Informatikai irányítás és menedzsment*. Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/20.500.12944/10377

KPMG (2013): *BCM körkép. Tanulmány az üzletfolytonosság-menedzsment magyarországi helyzetéről*. Budapest: KPMG. Online: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/20130911-BCM-korkep.pdf

Michelberger Pál (2024): *Fejezetek a vállalati biztonságmenedzsmentből*. Budapest: Akadémiai. Online: https://doi.org/10.1556/9789634549376

Michelberger Pál – Lábodi Csaba (2009): Információbiztonság az ellátási láncokban. *MEB 2009 – 7th International Conference on Management, Enterprise and Benchmarking*. Budapest. Online: https://bit.ly/4wQnA5k

Muha Lajos (2004): A terrorizmus és az informatikai biztonság. *HISEC 2004 Nemzeti adatvédelmi és adatbiztonsági konferencia*. Budapest.

National Institute of Standards and Technology (NIST) (2024): *NIST Cybersecurity Framework 2.0*. Online: https://doi.org/10.6028/NIST.CSWP.29

Nemzeti Kibervédelmi Intézet (2024): *Megjelent a NIST Cybersecurity Framework 2.0*. Online: https://nki.gov.hu/it-biztonsag/hirek/megjelent-a-nist-cybersecurity-framework-2-0/

Putra, Kevin – Wahyuningtyas, Emmy (2023): E-Learning System Audit at ABC University Using COBIT 5 Framework–MEA (Monitoring, Evaluate and Assess) Domain. *Melek IT,* 9(2). Online: https://doi.org/10.30742/melekitjournal.v9i2.261

Szádeczky Tamás (2014): *Információbiztonsági szabványok*. Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/20.500.12944/14304

U.S. Department of Energy (2021): *Cybersecurity Capability Maturity Model (C2M2) (Version 2.0)*. Washington, DC: U.S. Department of Energy. Online: https://c2m2.doe.gov/

Vértesy László (2012): A közigazgatás ellenőrzése és a közreműködő szervek. In *Közigazgatás, ellenőrzés, gazdálkodás*. Budapest: Nemzeti Közszolgálati Egyetem, 39–60. Online: https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/vertesy-laszlo-kozigazgatas-ellenorzes-gazdalkodas.original.pdf

Vértesy László (2014): *Az állami beavatkozás joga és hatékonysága*. Budapest: Nemzeti Közszolgálati Egyetem.