Deloitte.

7/2017. MNB-rendelet ismertetés

Kofrán László, 2017. október 27.

A Felügyelet 7/2017 (VII.5.) sz. ajánlása

- **A kritikus rendszerek tanúsításáról szóló jogszabályi kiegészítések beemelése**
- **Kétéves felülvizsgálat a felügyeleti gyakorlat fényében**
- **Új technológiák alkalmazása a szektorban**
- **…az abból fakadó kihívásoknak való megfelelés**

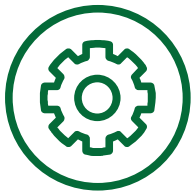
IT eszköz és adatvagyon nyilvántartás

Pontos, folyamatosan aktualizált

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

a) a rendszer legfontosabb **elemeinek** (eszközök, folyamatok, személyek) egyértelmű és visszakereshető **azonosításáról**



5/B. § Az informatikai rendszer megfelel a Hpt. 67/A. § (1) bekezdésében, a Bszt. 12. § (12)-(14) bekezdésében, az Fsztv. 12/A. §-ában és a Bit. 94. § (4)-(6) bekezdésében foglalt, a rendszerelemek zártságával, az informatikai rendszerhez történő jogosulatlan hozzáférés és észrevétlen módosítás megakadályozásával kapcsolatos, valamint az általános információbiztonsági zártsági követelményeknek, ha

a)az élesüzemi rendszer **elemei azonosíthatóak** és dokumentáltak

Szabályozási rendszer

Releváns, testre szabott, betartható és betartatható, kockázatokkal arányos

42/2015 (III. 12.)

2. § (3) Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével az intézmény meghatározza a szervezeti és működési rendeket, a felelősségi, a nyilvántartási és a tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.

3. § (3) Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik

a) informatikai rendszerének **működtetésére** vonatkozó **utasításokkal** és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel,

b) minden olyan **dokumentációval**, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató **informatikai rendszerek folyamatos és biztonságos működését** - még a szállító, valamint a rendszerfejlesztő tevékenységének **megszűnése után is** - **biztosítja**

5/B. § b) az élesüzemi rendszer **üzemeltetési folyamatai szabályozottak**, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek

Tesztelés, változáskezelés

Anonimizálás a tesztelési és fejlesztési környezetben egyaránt, üzemeltető élesít, regressziós teszt

42/2015 (III. 12.)

3. § (3) Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik

d) olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és a tesztelési környezettől, valamint a megfelelő változáskövetés és **változáskezelés** fenntartását

5/B. § *c)* az élesüzemi rendszer **változáskezelési** folyamatai biztosítják, hogy a rendszer paraméterezésében és a szoftverkódban bekövetkező változások csak tesztelt és dokumentált módon valósulhatnak meg

Mentés, visszatöltés - archiválás

Mentés: RTO, RPO, típus, gyakoriság, példányszám, távoli helyszínen is, ellenőrzött módon

Archiválás: min. 5 évig

42/2015 (III. 12.)

3. § (3) Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik

e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan helyreállítási tervekkel, **biztonsági mentésekkel és mentési renddel** (mentések típusa, módja, **visszatöltési** és helyreállítási **tesztek**, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás **kritikus helyreállítási idején belül** lehetővé teszik

f) (…) az archivált anyagokat a jogszabályokban meghatározott ideig, de **legalább öt évig**, bármikor visszakereshetően, helyreállíthatóan megőrizzék

5/B. § *d)* az élesüzemi rendszer **adatmentési és visszaállítási** rendje biztosítja a rendszer biztonságos visszaállítását, továbbá a mentés-visszaállítás a vonatkozó szabályzat szerinti gyakorisággal és dokumentáltan tesztelt

Mentés védelme

Adatvédelem – GDPR megfontolások

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

f) az **adathordozók** szabályozott és biztonságos kezeléséről

(4) A (3) bekezdés *e)* pontja szerinti **mentéseket** kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések **forrásrendszerrel azonos szintű hozzáférési védelméről**.

5/B. § n) az élesüzemi rendszer **adathordozóinak védelme** szabályozott, megfelelően **korlátozott**, és a korlátozásokat rendszeres felülvizsgálatokkal és ellenőrzésekkel is fenntartják

Hozzáférési rend, felhasználói adminisztráció

Magas jogú felhasználók teljes körére (nevesített felelősök technikai usereknél is), nemcsak alkalmazás szintű, hanem alapinfrastruktúra és mappák szintjén is szabályozott hozzáférés-védelem és éves felülvizsgálata, user-friendly módon, a védendő értékkel arányos védelemmel kialakítva

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

c) **a rendszer** szabályozott, ellenőrizhető és rendszeresen **ellenőrzött felhasználói adminisztrációjáról** (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események)

5/A. § c) ca) a jogosult általános (emberek és program entitások) és privilegizált (speciális jogokkal felruházott) felhasználók – így különösen **rendszergazdák** – kizárólag a szigorúan szabályozott **szerepkörüknek megfelelően férhetnek a védendő információkhoz** és az azokat kezelő rendszer elemeihez, kezdeményezhetnek aktivitásokat, valamint kizárólag meghatározott privilegizált felhasználók adhatnak szabályozott szerepkörüknek megfelelően és ellenőrzött módon **hozzáférési jogosultságokat**

5/B. § e) az élesüzemi rendszerhez való **végfelhasználói hozzáférés** mind **alkalmazási,** mind pedig **infrastruktúra szinten** szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal **ellenőrzött**

Hálózati védelem 1.

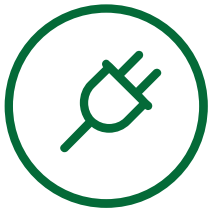
Legalább 2-faktoros hozzáférés (vö. NIST 800-53); ha PKI, kulcskezelési eljárás

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a **naplózás** rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is

e) a **távadatátvitel** bizalmasságáról, sértetlenségéről és hitelességéről

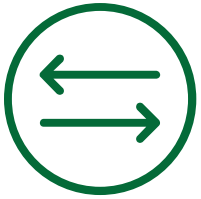


5/B. § h) az élesüzemi rendszerhez történő **távoli hozzáférés** **szabályozott, dokumentált** és a vonatkozó szabályzat szerinti gyakorisággal **ellenőrzött**;

Hálózati védelem 2.

Incidenskezelés csak hálózati védelemre értelmezve (?!)

42/2015 (III. 12.)



3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából **kritikus folyamatok eseményeit naplózza**, alkalmas a **naplózás** rendszeres (esetleg önműködő) és érdemi értékelésére, **valamint lehetőséget nyújt a nem rendszeres események kezelésére is**

5/B. § r) a szervezet detektálja és kezeli az egyes biztonsági eseményeket;

Naplózás 1.

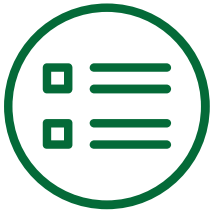
Azonnali, automatikus kiértékelés, kritikus eseményekről alertek (szabályzatban rögzített eseményekre és a szokásostól eltérő esetekre is)

Mit? alkalmazáson belül a tranzakciók, az összes infrastrukturális elemhez való hozzáférésre, rendszer- és hálózati konfiguráció

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a **naplózás** rendszeres (**esetleg önműködő**) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is



5/B. § *f)* az élesüzemi rendszerben felállított végfelhasználói hozzáférések egységes, zárt rendszert alkotnak, melyek biztosítják az üzleti folyamatok megvalósulását, továbbá a **végfelhasználók tevékenysége naplózásra** kerül és a kritikus rendkívüli eseményekről **automatikus figyelmeztetések** generálódnak

Naplózás 2.

Naplófájlok sértetlenségének védelme (magas jogú userek tevékenysége miatt is), naplózás kikapcsolása elleni kontrollok

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a **naplózás** rendszeres (**esetleg önműködő**) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is

5/B. § *g)* az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek, továbbá a **kiemelt jogosultságok**kal elvégzett tevékenység **naplózása** megvalósul, a napló fájlok sérthetetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak

Rosszindulatú kódok elleni védelem

Min. heti 1 full scan, automatikus frissítés, AV beállítások védelme, csak támogatott szoftvert használjunk (biztonsági patchek!)

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

g) a rendszer biztonsági kockázattal arányos **vírus- és más rosszindulatú program** elleni védelméről.

5/B. § i) az élesüzemi rendszer **vírus és más rosszindulatú programok** elleni védelme biztosított;

Adatkommunikációs rendszerek dokumentálása

Friss topológia és topográfia

42/2015 (III. 12.)

3. § (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

e) a **távadatátvitel** bizalmasságáról, sértetlenségéről és hitelességéről

5/B. § j) az élesüzemi rendszer **adatkommunikációs** és rendszerkapcsolatai dokumentáltak és ellenőrzöttek annak érdekében, hogy az adatkommunikáció bizalmassága, sérthetetlensége és hitelessége biztosítható legyen

Szolgáltatásfolytonosság

Új backup site már min. 1000 méterre legyen az éles gépteremtől (régi maradhat 400 m-re), ÉS egyidejű katasztrófa ne érintse mindkettőt
RTO/RPO: csapások, emberi hiba, helyi spec., külső szolgáltatók kiesése is
Oktatni, tesztelni, felülvizsgálni

42/2015 (III. 12.)

3. § (3) Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik

e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan **helyreállítási tervekkel**, biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és **helyreállítási tesztek**, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik,

g) a szolgáltatásai folyamatosságát akadályozó **rendkívüli események** kezelésére szolgáló **terv**vel.

k) a **katasztrófa-helyreállítási** terv rendszeresen **tesztelt**

Beszerzés

Kötelező szerződési elemek, SLA: mérhető (akár maga vagy 3. fél), számonkérhető és szankcionálható szolgáltatás, adatkimentő exit stratégia

Új 5/B. § követelmény!

5/B. § l) a rendszerek és szolgáltatások beszerzése szabályozott, nyomon követett, és megfelel a biztonsági előírásoknak;

Üzemeltetés biztonsága 1.

A kellő szintű védelem, az operatív utasítások rendelkezésre állása (2nd site-on is)

42/2015 (III. 12.)

3. § (3) Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik

a) informatikai **rendszerének működtetésére vonatkozó utasításokkal** és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel,

e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan helyreállítási tervekkel, biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek **az adott rendszer helyreállíthatóságát** a rendszer által nyújtott szolgáltatás **kritikus helyreállítási idején belül** lehetővé teszik

g) a szolgáltatásai folyamatosságát akadályozó **rendkívüli események** kezelésére szolgáló tervvel.

5/B. § *b)* az élesüzemi rendszer **üzemeltetési folyamatai szabályozottak**, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek

m) az élesüzemi rendszer **karbantartása szabályozott**, és megfelel a **rendelkezésre állásra vonatkozó** elvárásoknak

o) az élesüzemi rendszer és az üzemeltetési szabályzatok **gondoskodnak** a rendszerelemek és a kezelt információk **sértetlenségéről**

p) az élesüzemi rendszer és az üzemeltetési szabályzatok gondoskodnak a rendszer és a kommunikáció **kellő szintű védelméről**

Üzemeltetés biztonsága 2.

A feldolgozott és tárolt adatok sértetlenségének védelme – GDPR itt is

42/2015 (III. 12.)

4. § (1) Az intézménynél mindenkor rendelkezésre kell állnia

(2) A szoftvereknek együttesen alkalmasaknak kell lenniük

e) a [**tárolt adatok**] biztonsági kockázattal arányos logikai védelemre és a **sérthetetlenség védelmére**.

5/B. § o) az élesüzemi rendszer és az üzemeltetési szabályzatok gondoskodnak a rendszerelemek és **a kezelt információk sértetlenségéről**

Üzemeltetés biztonsága 3.

Üzemelttetés felügyelete és szabályozottsága

42/2015 (III. 12.)

3. § (1) Az intézmény kiépíti az **informatikai rendszere biztonságos működtetését felügyelő informatikai ellenőrző rendszert** és azt folyamatosan működteti

p) az élesüzemi rendszer és az üzemeltetési szabályzatok gondoskodnak a **rendszer és a kommunikáció** kellő szintű védelméről

Fizikai védelem

Beléptető rendszer, falazat és rácsozat, mozgásérzékelők és környezeti (!) kontrollok a berendezések folyamatos karbantartással

42/2015 (III. 12.)

[számos korábban idézett releváns jogszabályi hely együttesen]

5/B. § q) **megfelelő szintű fizikailag védett környezetet** biztosítanak az élesüzemi rendszer számára

Személy(zet)i biztonság

Külön a felhasználókra, és az üzemeltetőkre (külső képzésekre keretet biztosítani)
A feldolgozott adatok biztonsági besorolása alapján a munkaköröket is besorolják

Új 5/B. § követelmény!

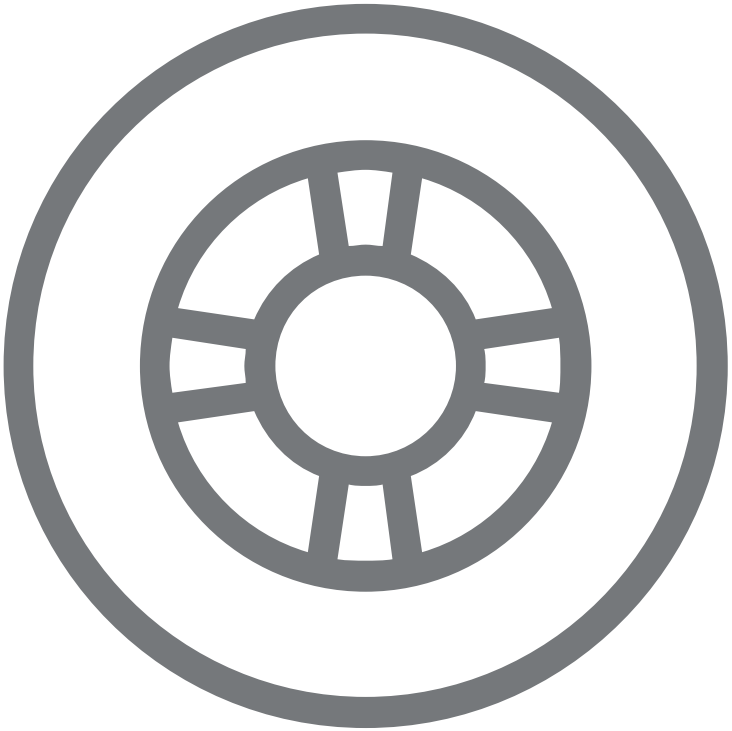
[**5. §** Az intézmény a belső szabályzatában meghatározza **az egyes munkakörök betöltéséhez szükséges informatikai ismeretet**. - 42/2015 (III. 12.) Kr.]

5/B. § s) az élesüzemi rendszer üzemeltetésében és használatában részt vevő személyek rendszeres biztonságtudatossági oktatáson vesznek részt, valamint a szervezet dolgozóinak munkaügyi szabályozása megfelel a biztonsági előírásoknak.

…és ami kimaradt – címszavak a teljesség igénye nélkül

Hogyan tud segíteni a Deloitte?

- **Felügyeleti vizsgálatra való hatékony felkészítés**
- **Azonosítjuk azokat a kontrollhiányosságokat**, amelyek a hazai felügyeleti gyakorlatnak és jogszabályi előírásoknak nem, vagy csak részben felelnek meg
- **Átfogó képet adunk** a kritikus informatikai rendszerek logikai és fizikai kontrolljainak kialakítottságáról, működésük hatékonyságáról
- Javaslatot fogalmazunk meg egy **kockázattudatosabb**, az **üzleti célok és elvárások kiszolgálását jobban szem előtt tartó logikai és fizikai kontrollkörnyezet** kialakítására



Deloitte.

Cyber Security Framework – Bemutató

Szöllősi Zoltán, Deloitte IT Kerekasztal – 2017. október 27.

Cyber Security Framework módszertan

Deloitte’s CSF is built on three foundations

Methodology

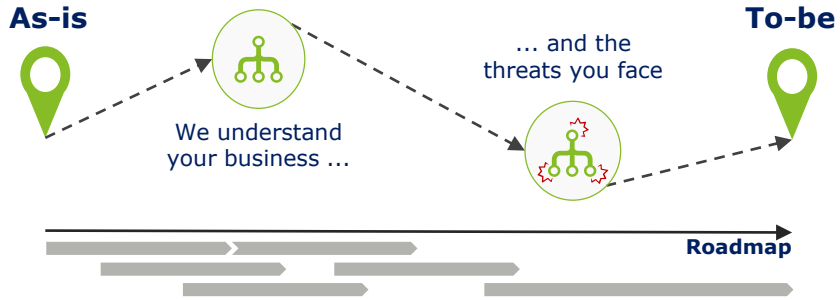
Deloitte’s CSF leverages a proven methodology to assess organization’s current state (as-is) of their security capabilities and to benchmark against a target state (to-be) tailored to the organization’s specific threat landscape.

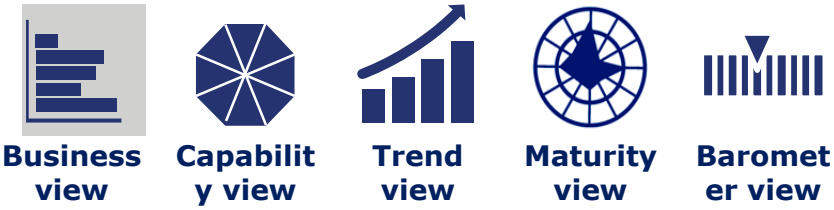
Platform

Deloitte offers clients access to their propriety CSF platform, where data captured during the assessment is analysed. This platform offers a range of clear dashboard views on the data, enabling clients to obtain valuable insight in their security capabilities.

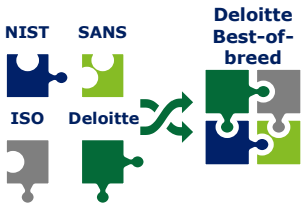
Content Packs

Deloitte's CSF uses extensive content packs encompassing a capability model and best practices, a threat model and a set of benchmark data.





Capability Model Best Practices



Threat Model

Benchmark Data

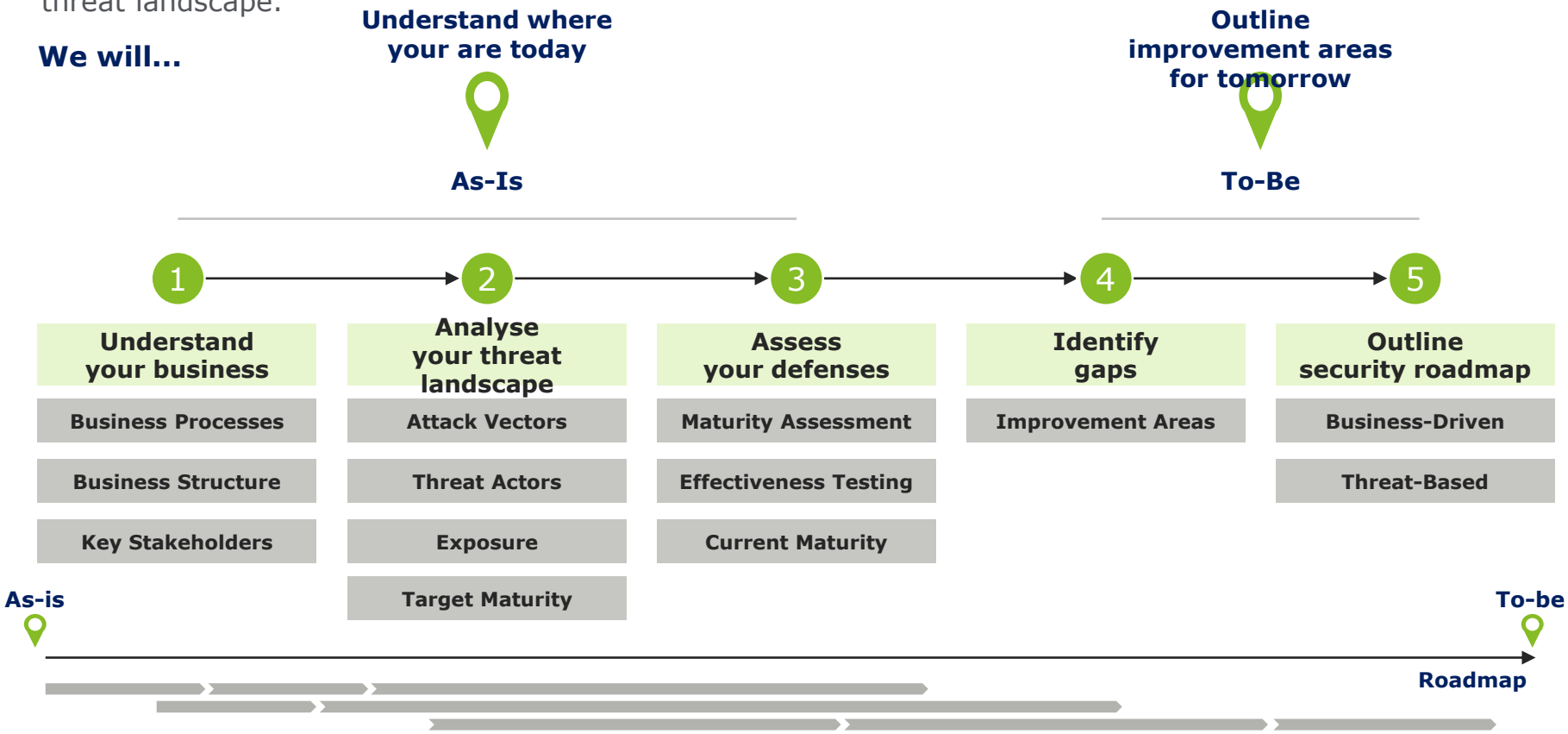
Telco

Financial Services

Follow a proven methodology for cyber strategy

Deloitte's CSF leverages a proven methodology to assess the current state (as-is) of organization's security capabilities and to benchmark against a target state (to-be) tailored to the organization's specific threat landscape.

We will...

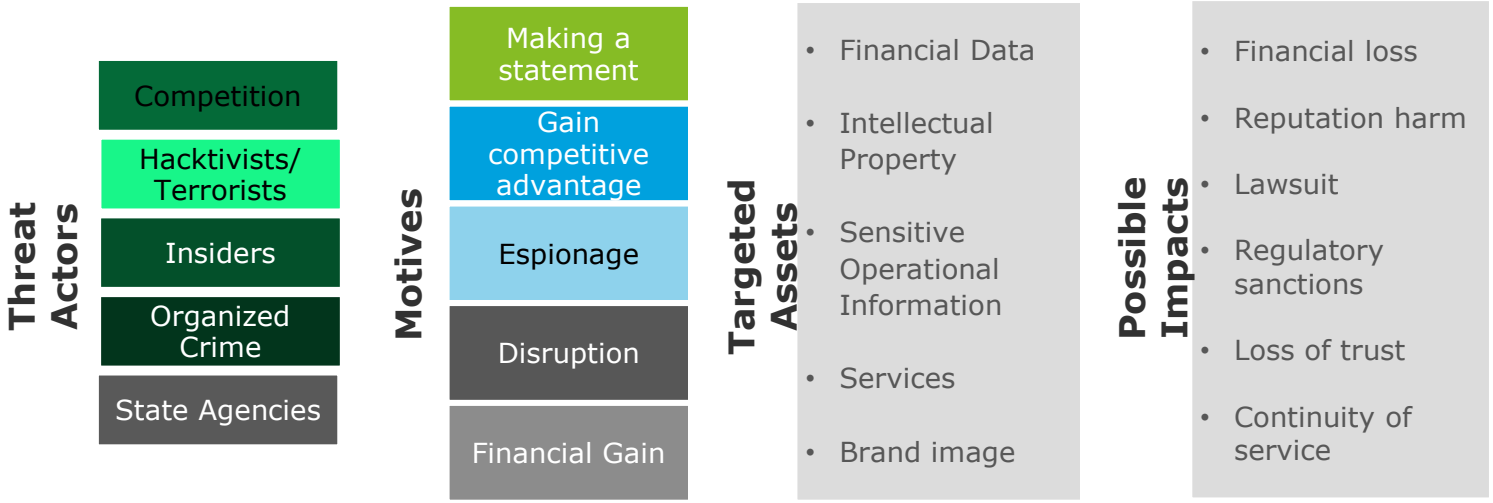


We will help you move from current to target state by designing a the cyber strategy roadmap for the execution of relevant cyber security projects & initiatives

Cyber Strategy Framework Content Packs

Threat Model

Not all cyber threats are equally threatening your business: depending on your Assets, different Threat Actors might be motivated to launch cyber attacks against these assets, which can impact your organisation in different ways (financially, legally etc.).



Cyber Strategy Framework Content Packs

Cyber Security Capability Model

Governance

Ensuring that the necessary structures and rules are in place to maintain and enhance preventative and detective security capabilities.

Secure

Proactive protection against successful cyber attacks before they occur by developing, implementing, and enhancing the controls that safeguard digital assets.

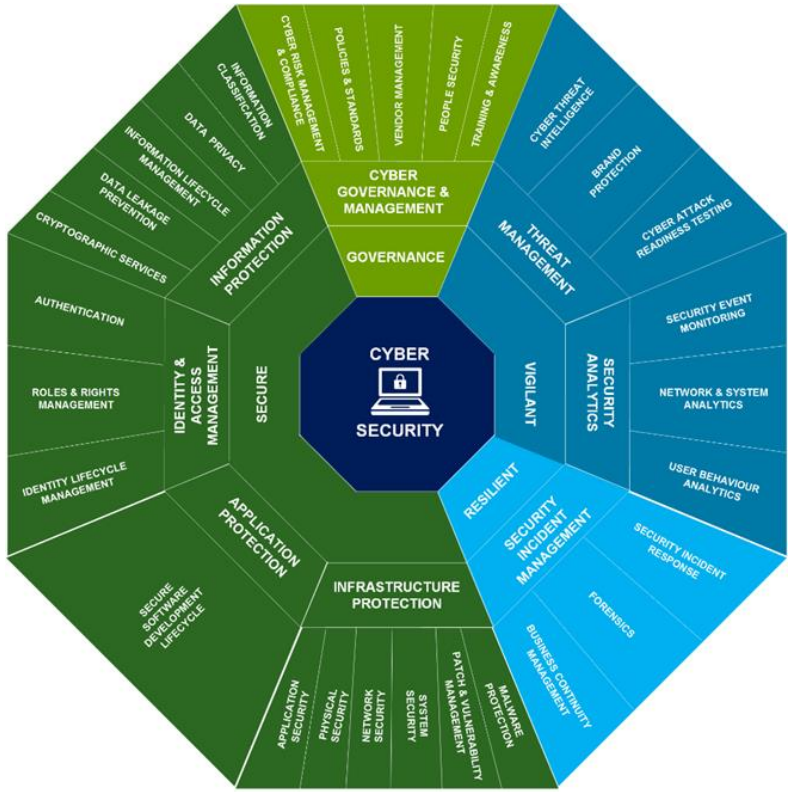
Vigilant

Ability to discover internal and external threats by leveraging the threat intelligence, and pro-actively mitigating them, or minimizing any adverse impacts to the organization.

Resilient

Not a question of whether organizations will be attacked or not, it is a question of when.

These 4 domains are subdivided in 8 capabilities and 29 sub-capabilities.



Deloitte's Cyber Security Capability Model

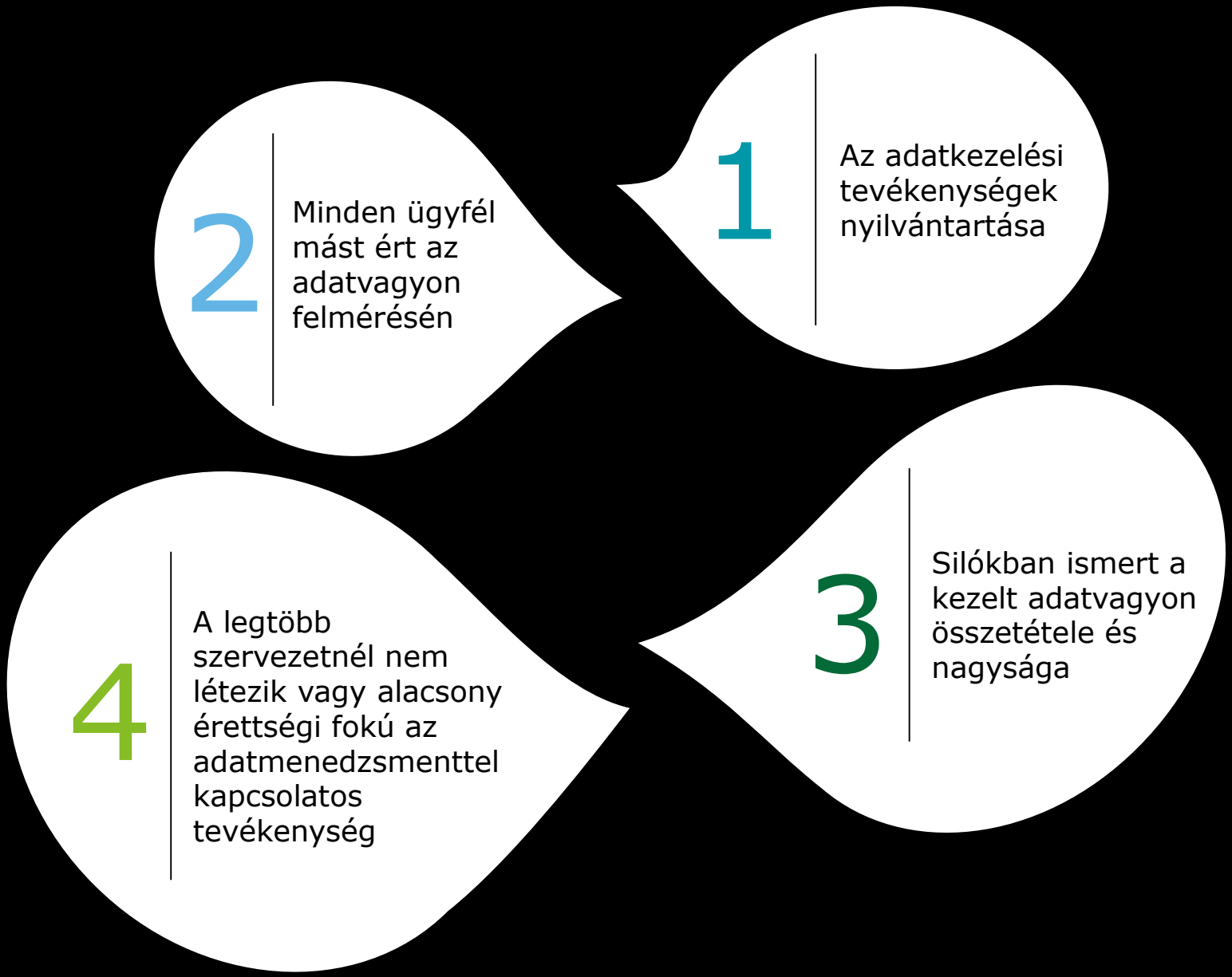
Deloitte.

GDPR – Gyakorlati tapasztalatok

Bereczki Tamás, Deloitte IT Kerekasztal – 2017. október 27.

Az adatvagyon kezelése

Az adatvagyon kezelése



Kihívások az IT környezetekben

Kihívások az IT környezetekben

Teszt- és fejlesztői környezetek

- Élő gyakorlat a teszt- és fejlesztői környezetek éles adatokkal való feltöltése
- A használt anonimizálási technikák nem megfelelőek

Jogosultságkezelés

- Legacy rendszerek
- Szerepkörösítés
- Ellenőrzések – szerepkörök és jogosultságok

Adatbázis replikációk

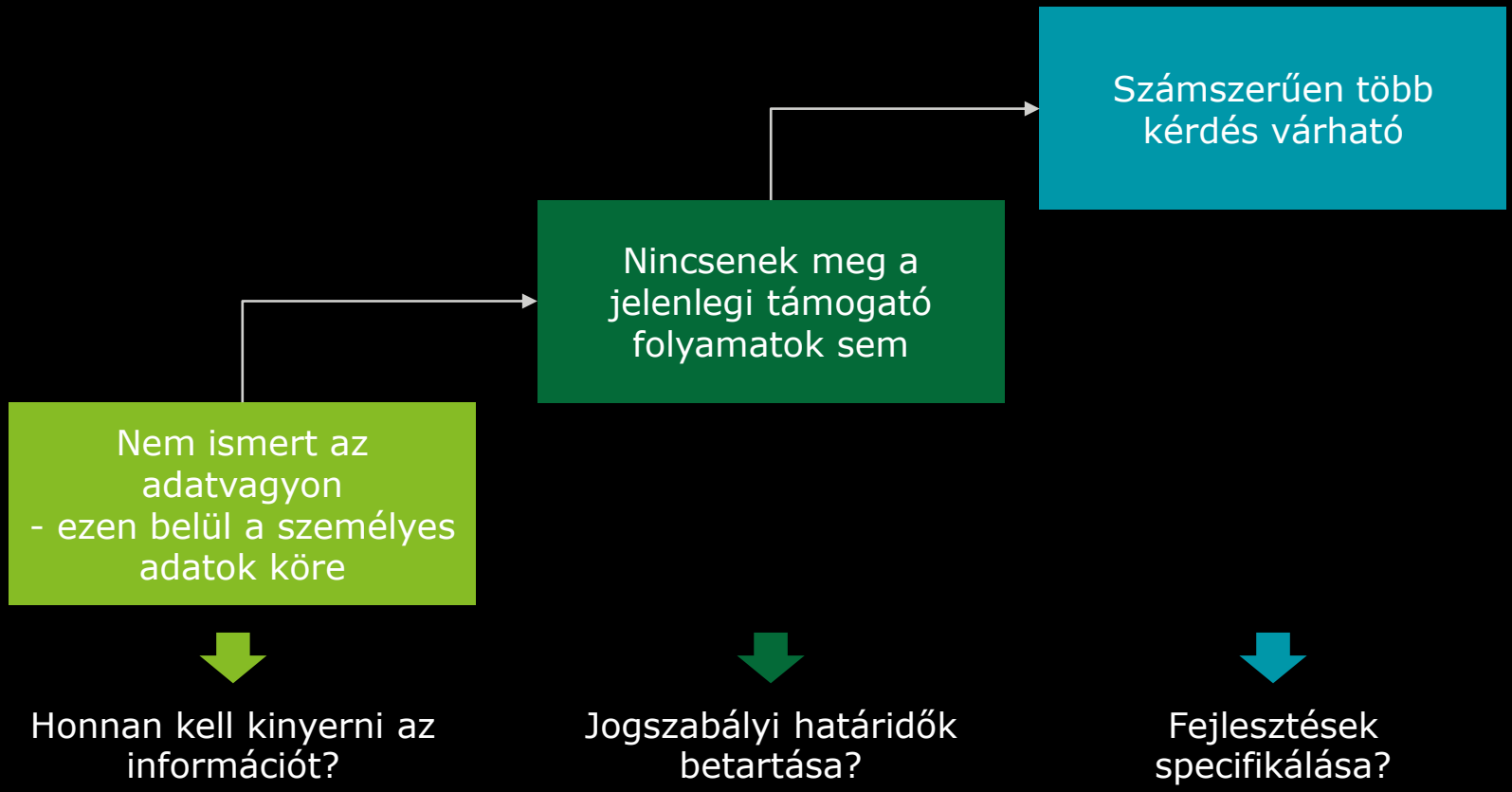
- Adattárházak és CRM rendszerek
- Profilozások, ott is, ahol nem számítunk rá
- Jelenlegi adatkezelési tájékoztatók nem terjednek ki rá

Nem strukturált adatok

- Szkennelt anyagok e-mailben
- Fényképek, fénymásolatok
- Eltérő rendszer kritikussági definíciók

Támogató folyamatok érettsége

Támogató folyamatok érettsége – Szervezési kontrollok




1
Jogosultságkezelés támogatása,
hozzáférés kezelés
2
Incidenskezelés támogatása,
naplózás, egyéb eszközök
3
Privacy-Enhancing Technologies,
titkosítások és adatvesztés
megelőzési képességek

Az adatvédelmi felelős szerepe

Az adatvédelmi felelős szerepe

Az adatvédelmi felelős lehet szervezeten belüli es külsös tanácsadó is. Ennek megállapításához szükséges, hogy a szervezet ismerje a személyes adatkezeléssel érintett folyamatait.

1

Belsős adatvédelmi felelős

választása esetén kívánatos - tekintettel a személyes adatkezelés szervezeten átívelő jellegére - hogy ne egy szervezeti egység alá tartozzon, megosztott feladatkörrel, hanem önálló legyen és a menedzsmentnek közvetlenül jelentsen.

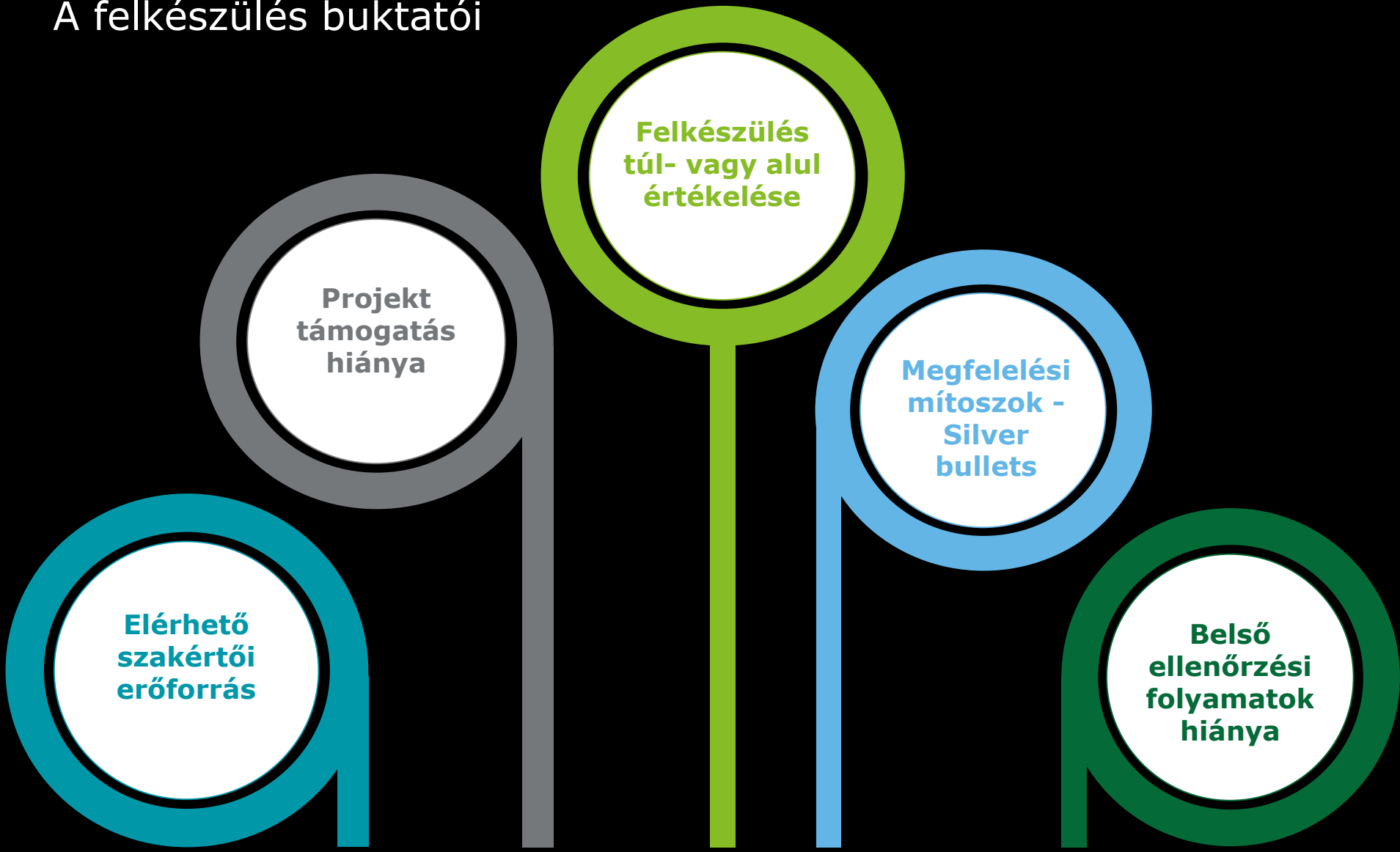
2

Külsös adatvédelmi felelős
feladatkört betöltő személyként akár tanácsadó, ügyvéd, vagy ügyvédi iroda is megbízható.

Az adatvédelmi felelős rendelkezzen adatvédelmi tapasztalattal, értse annak jogi relevanciait, tartsa a kapcsolatot a hatóságokkal, valamint rendelkezzen olyan informatikai alapismeretekkel, hogy a személyes adatoknak ilyen vetületet is számításba tudja venni

A felkészülés buktatói

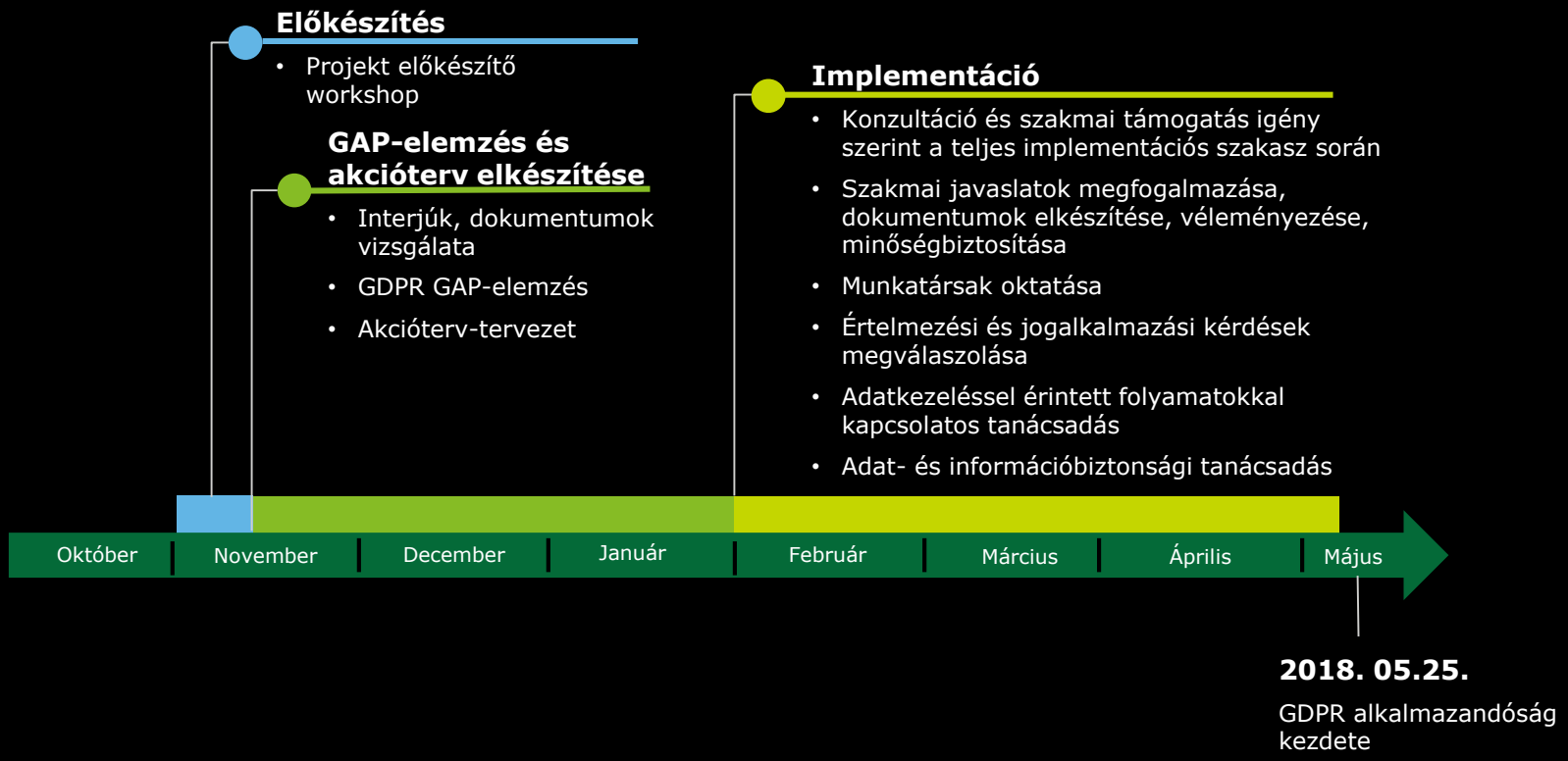
A felkészülés buktatói



Hogyan tud segíteni a Deloitte?

A Projekt időzítése

A projekt várható időzítésének áttekintése



Deloitte.

A Deloitte név az Egyesült Királyságban “company limited by guarantee” formában alapított Deloitte Touche Tohmatsu Limited („DTTL”) társaságra, tagvállalatainak hálózatára és kapcsolt vállalkozásaira utal. A DTTL és valamennyi tagvállalata önálló, egymástól elkülönülő jogi személy. A DTTL (vagy „Deloitte Global”) nem nyújt szolgáltatásokat ügyfelek számára. A DTTL és tagvállalatai jogi struktúrájának részletes bemutatását a következő link alatt találja: www.deloitte.hu/magunkrol.

Magyarországon a szolgáltatásokat a Deloitte Könyvvizsgáló és Tanácsadó Kft. (Deloitte Kft.), a Deloitte Üzletviteli és Vezetési Tanácsadó Zrt. (Deloitte Zrt.) és a Deloitte CRS Kft. nyújtja (melyek közös neve "Deloitte Magyarország"). Mindhárom társaság a Deloitte Central Europe Holdings Limited tagvállalata. A Deloitte Magyarország négy szakmai területen - könyvvizsgálat, tanácsadás, adó- és jogi valamint kockázati tanácsadási területeken - tölt be kiemelkedő szerepet az országban, és kínál szolgáltatásokat több mint 500 hazai és külföldi szakértője segítségével. (Ügyfeleinknek együttműködő ügyvédi irodánk, a Deloitte Legal Szarvas, Erdős és Társai Ügyvédi Iroda nyújtja a jogi tanácsadási szolgáltatásokat.)

A jelen dokumentum és a benne foglalt valamennyi információ a Deloitte Magyarország társaságaitól származik és célja, hogy bizonyos témakör(ök)ben általános információkkal szolgáljon, de nem tárgyalja az adott témakör(öke)t annak teljességében. A jelen dokumentumban megadott információk nem minősülnek számviteli, adóügyi, jogi, befektetési, tanácsadási illetve egyéb szakmai szolgáltatásnak. Ezek az információk nem képezhetik ügyfeleink üzleti döntéseinek kizárólagos alapját. Ügyfeleinket arra kérjük, hogy pénzügyeiket vagy üzletvitelüket befolyásoló bármely döntésük meghozatala, vagy a döntésnek megfelelő magatartás tanúsítása előtt kérjék képzett szakmai tanácsadóink véleményét.

Jelen anyagok és a bennük foglalt információk tájékoztató jellegűek és esetlegesen hibákat is tartalmaznak, amelyekért a Deloitte Magyarország sem kifejezetten, sem hallgatólagosan nem vállal felelősséget, és amelyek nem minősülnek a Deloitte Magyarország állásfoglalásának. Az előzőek érintése nélkül a Deloitte Magyarország nem garantálja az anyagoknak és / vagy a bennük foglalt információknak a hibamentességét, továbbá a teljesítés vagy a minőség valamennyi egyedi kritériumának való megfelelőséget sem. A Deloitte Magyarország cégei nem felelnek a szolgáltatásaik piacképességére, vagy adott célra való alkalmassága, jogtisztasága, versenyképessége, biztonsága és pontossága vonatkozásában.

Ügyfelünk a jelen anyagot és a benne foglalt információkat a saját felelősségére használja, és teljes mértékben felelősséget vállal a jelen dokumentum és a benne foglalt információk használatából eredő következményekért, esetleges veszteségekért. A Deloitte Magyarország cégei nem vonhatók felelősségre jelen dokumentum, vagy a benne foglalt információk felhasználásával kapcsolatosan felmerülő közvetlen, közvetett, járulékos, következményes, büntető jellegű vagy bármilyen egyéb kárért, valamint egyéb veszteségért sem, legyen az szerződéses, jogszabály szerinti vagy magánjogi (például gondatlanságból fakadó).

A fent írtaktól eltérően amennyiben az információk és az anyagok kifejezetten az Ügyfél és a Deloitte Magyarország között létrejött szerződés végleges teljesítéseként kerülnek átadásra, a Deloitte Magyarország felelősséget vállal azért, hogy a szolgáltatásnyújtás és - amennyiben van - az elkészült termék szerződésszerű. A Deloitte Magyarország rögzíti, hogy az anyagok és az információk kizárólag a szerződésben meghatározott személyek / szervezetek számára készülnek és célokra alkalmasak. A Deloitte Magyarország minden felelősséget kizár az Ügyfél által rendelkezésre bocsátott dokumentumokból, anyagokból, információkból és adatokból fakadó vagy azokkal összefüggő károk vonatkozásában. Minden itt nem szabályozott kérdésre a vonatkozó szerződés irányadó.

Ha a fenti rendelkezések bármelyike bármilyen okból nem érvényesíthető, a többi rendelkezés továbbra is hatályban marad és alkalmazandó.