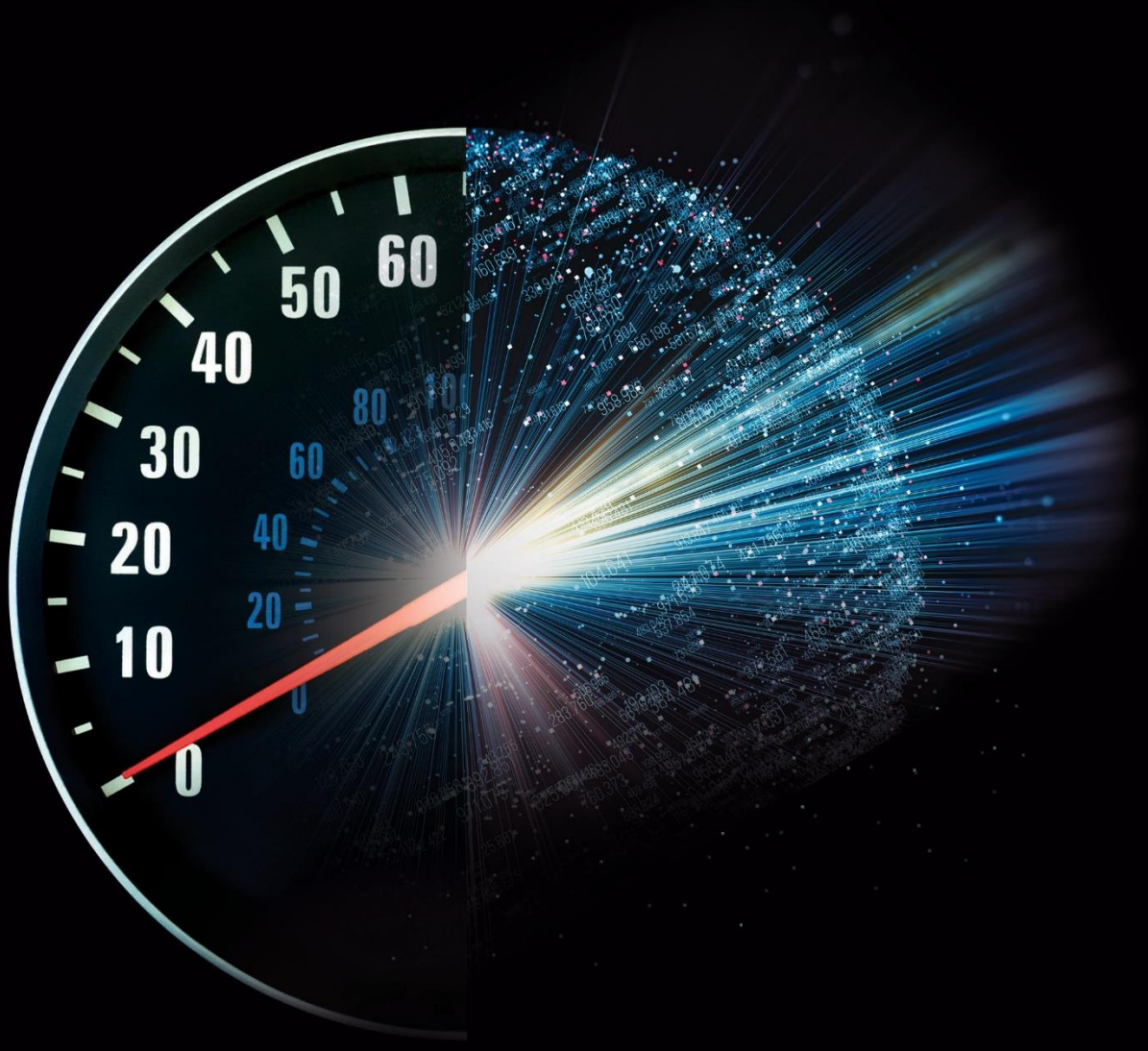
Deloitte.



Új technológiákhoz kapcsolódó kockázatok

Belső ellenőrzés a digitalizáció korában

Digitalizáció kora

Izgalmas átalakulás korát éljük. A technológiai haladás és a fejlett analitika, robotizált folyamatautomatizálás (RPA) és kognitív intelligencia terén (CI) elért eredmények nagy ütemben alakítják az üzleti modelleket, növelve a termelékenységet és innovatív megoldásokat kínálva a termékek és szolgáltatások egyes vevőkhöz kapcsolására. Az újdonságok széleskörű elterjedését nevezzük Ipar 4.0-nak, vagy a Negyedik ipari forradalomnak (lásd 1. ábra).

Részletes koordinációra van szükség. Ahogy a vállalatok egyre inkább alkalmazzák az új technológiákat, a belső ellenőrzésnek proaktívan fel kell ismernie és értékelnie az ezekkel járó kockázatokat. Ennek segítségével a belső ellenőrzés felméri, hogy megfelelőek-e a bevezetett kontrollok az új és még ezután felmerülő kockázatok megelőzésére és észlelésére.

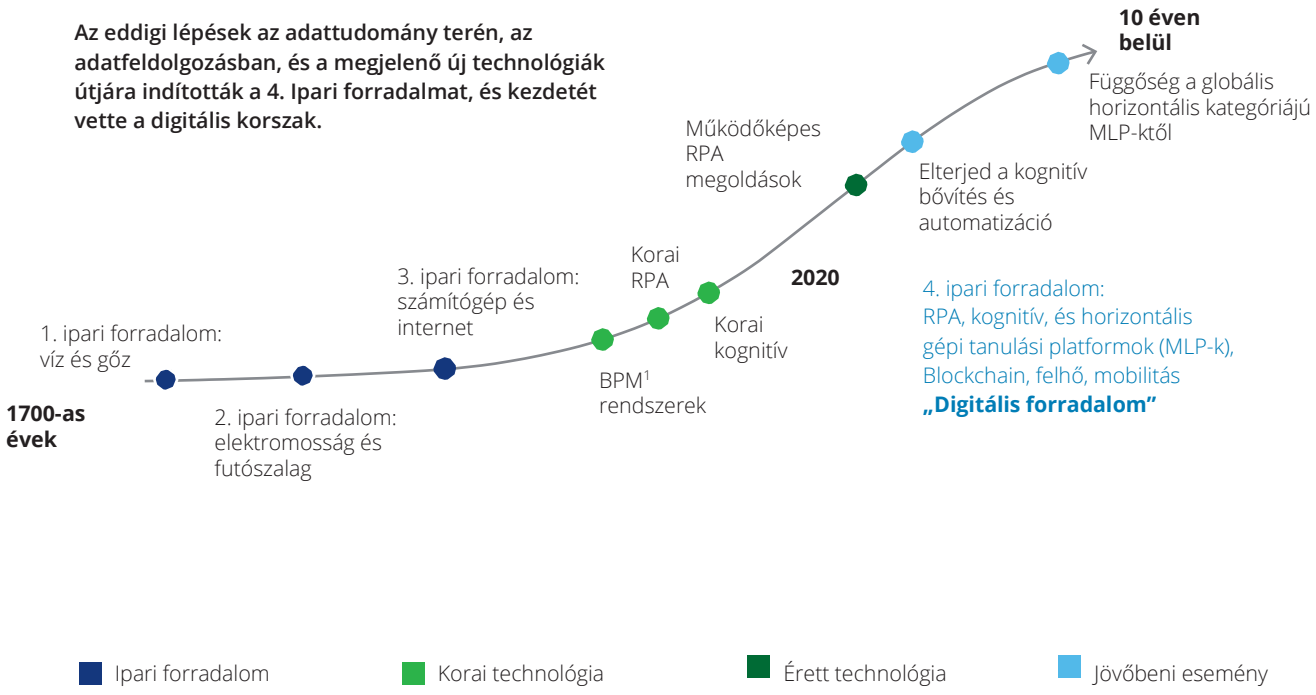
Számos belső ellenőrzési osztály tett lépéseket a változások kezelése terén. Jóllehet egyesek érettebb megoldásokkal rendelkeznek, a legtöbb belső ellenőrzési osztály még csak az út kezdeti szakaszánál tart. Ezen túlmenően, fejlett technológiákat akarnak alkalmazni a programok modernizálása és hatékonyságának javítása érdekében, ami azonban a kapcsolódó kockázatok kezelését is szükségessé teszi.

Jelenleg rengeteg új technológia lendíti előre az Ipar 4.0 fejlődését, beleértve az egymáshoz kapcsolódó és nagy teljesítményű hálózatokat és számítógépeket, digitális eszközöket, adatelemző, RPA és CI eszközöket. Együttesen ezek a technológiák alapvetően változtatják meg az üzleti tevékenységet.

Ennek a tanulmánynak a digitalizáció áll a középpontjában. A következőkben közelebbről megvizsgáljuk az új digitális technológiákkal együtt járó kockázatokat, és javaslatokat teszünk arra, hogy a belső ellenőrzési osztályok hogyan kezelhetik azokat.

1. ábra Ipar 4.0

Az eddigi lépések az adattudomány terén, az adatfeldolgozásban, és a megjelenő új technológiák útjára indították a 4. Ipari forradalmat, és kezdetét vette a digitális korszak.



Forrás: Ipar 4.0: Kihívások és megoldások - digitális átalakulás és az exponenciális technológiák, Deloitte kutatás 2015

[1]BPN: Business process Management - Üzleti folyamatok kezelése

Diszruptív digitalizáció

A diszruptív digitális technológiák olyan új megoldásokat kínálnak, melyek gyökeresen megváltoztatják az életünket, felforgatják a piacot, az erősorrendet gyökeresen megváltoztatják rendkívül rövid idő alatt. Új automatizációs képességek bevezetésével az RPA és a CI segítségével, a diszruptív digitális technológiák a belső ellenőrzés hatékonyságát és eredményességét is képesek növelni. Számos vezető vállalat alkalmazott egy vagy több technológiát a 2-es ábrán láthatóak közül a napi működésük biztosítására. Éppen ezért, ezen szervezetek belső ellenőrzési részlegeinek is fontos ezzel lépést tartania.

2. ábra A digitalizációs spektrum

Az automatizáció mértéke

Kapcsolódó technológiák

Alapok

Adatintegráció

Az integrált adatok konzisztens információs alapokat biztosítanak (pl. megfelelőségi kockázat és felügyeleti adattárház)

Analitika

Prediktív analitika

Prediktív modelleket felhasználó szoftvermegoldások (pl. megfelelősségi kockázati modellek)

Adatvizualizáció

Az adatokat vizuális kontextusba helyező szoftver (pl. GRC dashboards)

Robotika

Robotikus folyamatautomatizálás

Szabályok irányította rendszerek, melyek az emberi viselkedést utánozzák, hogy automatizálhatóvá tegyenek ismétlődő folyamatokat

Kognitív intelligencia

Természetes nyelv generálása (NLG)

Alkalmazások, melyek képesek strukturált adatok befogadására (Excel-szerű sorok és oszlopok) látszatra struktúra nélküli narratívák generálásához.

Természetes nyelv feldolgozása (NLP)

A nem strukturált adatokat (pl. egyszerű szöveg) feldolgozó alkalmazások, amelyek lehetővé teszik strukturált adatok lekérdezését és generálását.

Gépi tanulás (ML)

A kiszámíthatóságot és a működést javító, a huzamosabb időn keresztül fogadott adatokon alapuló alkalmazások

Mesterséges intelligencia (AI)

Az emberi viselkedést utánozni képes alkalmazások, mint a vizuális észlelés, beszédfelismerés, döntéshozatal és nyelvek közötti fordítás

A belső ellenőrzés áttekintése - múlt, jelen és jövő

Ahol minden kezdődött: Adatintegráció

A vállalatoknak képesnek kell lenniük a gyors és konzisztens adatelemzésre annak érdekében, hogy szervezeti szinten, valós időben, gyorsan meg tudjanak valósítani fejlesztéseket. Ez az elvárás motiváló környezetet teremtett az innovatív növekedéshez, a sikeres automatizálás alapjául szolgáló adatintegritással.

A közelmúlt történései: Analitika

Az elmúlt években egyre több vállalat alkalmazza az analitika módszereit, hogy megvilágítsanak trendeket, problémákat és lehetőségeket, melyek a folyamatosan növekvő adattárak mélyén rejtőznek. Az analitikában rejlő lehetőségek száma végtelen – a jelen adatainak, a jövő trendjeinek és kockázatainak elemzése mellett a szervezetek adatvizualizációval érdemi és átfogó vizuális kontextust hozhatnak létre.

Hol tartunk most: Automatizáció

A robotizált folyamatautomatizálás (RPA) olyan szoftverfelhasználást jelent, ahol szabályalapú feladatok végrehajtásával utánozzák a felhasználói aktivitást az interfészen, gyakran egyszerre több rendszeren is dolgozva. A vállalatok fokozottan érdeklődnek az RPA alkalmazásának lehetősége iránt, mivel az időigényes tevékenységek automatizálása nagyobb hatékonyságot eredményezhet, és így az alkalmazottak magasabb hozzáadott értékű feladatokra fókuszálhatnak. Egy másik előny a méretezhetőség, amely javíthatja a kereslet és az elérhető erőforrás között mutatkozó ingadozásra adott reakciót.

A következő lépés CI

A fejlett kognitív intelligencia (CI) alapú technológiák, mint a természetes nyelvfeldolgozás és a gépi tanulás, a következő feladatokra használnak algoritmusokat:

- Összefüggések és kapcsolatok kinyerése adatokból
- Jelentésük "megértése"
- Adatminták és korábbi tapasztalatok alapján bővítik az önálló emberi és gépi tevékenységeket

A vállalatok egyre több automatizációs kezdeményezéseket adoptálnak, új technológiákat integrálnak. Ezek az új technológiák ugyanakkor új kockázatokat is jelentenek a meglévő irányítási környezetre.
Ha a három védelmi vonalon át nincsenek megfelelően kezelve, ezeknek a kockázatoknak értékcsökkentő- vagy megsemmisítő hatásuk is lehet.

Az kiadványunk hátralevő részében az RPA és a CI specifikus kockázatairól lesz szó. A belső ellenőrzési funkcióknak hatnia kell az érdekelt felekre, hogy azok mérjék fel az automatizációs technológiák bevezetésével kapcsolatos kockázatokat. Ez a kockázatfelmérés a következő kérdésekkel indulhat el:

- Hogyan biztosítható, hogy ezek a botok* megfeleljenek az irányelveknek?
- Létezik-e incidens kezelési keretrendszer, amely a botokat ellenőrzi?
- Hogyan akadályozható meg a botok hiba halmozása?
- Hogyan kerülhetők el a visszaélések a rendszer-hozzáférési jogosultságok kapcsán?
- Hogy néz ki a botok változáskezelési folyamata?
- Az érintett felek hogyan fognak oktatást kapni a robotikáról?
- Melyek a botokat ellenőrző menedzserek feladatai?

*Ezekben a kérdésekben a bot kifejezés olyan okos automatizációs technológiára vonatkozik, melyeket szabályalapú vagy kognitív intelligencia alapú algoritmusok működtetnek.

A létező digitalizációs környezet vizsgálata

Az automatizáció kapcsán felmerülő legfontosabb kockázatok

Ezeknek az RPA és CI technológiáknak az ökoszisztémájukba történő bevezetésével a vállalkozások potenciális kockázatoknak teszik ki magukat. Ezeket a kockázatokat öt fő kategóriába sorolhatjuk (lásd 3. ábra):

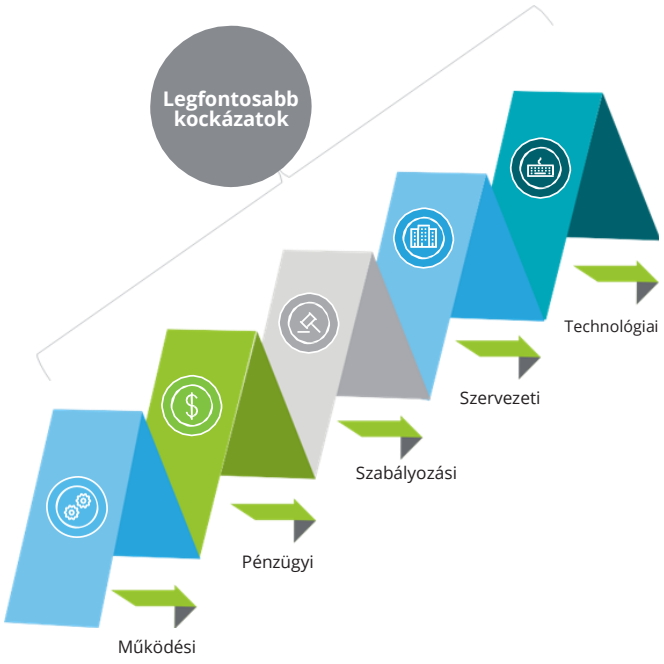
Működési kockázatok:

- A rosszul megtervezett RPA és CI technológiák a botok nagy végrehajtási sebességével kombinálva megsokszorozhatják a feldolgozási hibák számát.
- A botok nem megfelelően kialakított ellenőrzési folyamatai nagy hatásfokú működési hibákat eredményezhetnek.
- Az RPA és CI technológiák különböző üzleti problémákra történő nem egységes alkalmazása nem standardizált környezethez vezethet és növelheti a botok ellenőrzésével kapcsolatos komplexitást.
- A fejlesztők által a CI technológiákhoz használt algoritmusok tanításához biztosított bemeneti adatok hiányosak, elavultak, vagy részrehajlóak lehetnek.
  Előfordulhat, hogy túlságosan nagy és sokrétű a minta mérete. Ezen kívül a nem megfelelő adatgyűjtési módszerek eltérést eredményezhetnek az algoritmus tanításához használt adatok és a működéshez használt konkrét bemeneti adatok között.
- A hibás feltételezések, a nem megfelelő modellezési technikák, illetve a kódolási hibák további működési kockázatot eredményezhetnek.
- Számos RPA és CI technológiai szolgáltató új a piacon és még nem kellően érett, ami harmadik felekhez kapcsolódó beszállítói, illetve pénzügyi kockázatot jelent.

Pénzügyi kockázatok:

- Az RPA és CI technológiák nem megfelelő implementációja pénzügyi veszteségekhez és a vállalkozás jó hírnevének romlásához vezethet.
- Az RPA és CI technológiák nem megfelelő konfigurációjából vagy helytelen beállításaiból eredő hibás pénzügyi állítások jelentős hiányosságokhoz vagy lényeges gyengeségekhez vezethetnek a pénzügyi beszámoláshoz kapcsolódó belső kontrollok esetében (ICFR).

3. ábra Az automatizálással kapcsolatos öt legfőbb kockázat



Szabályozási kockázatok:

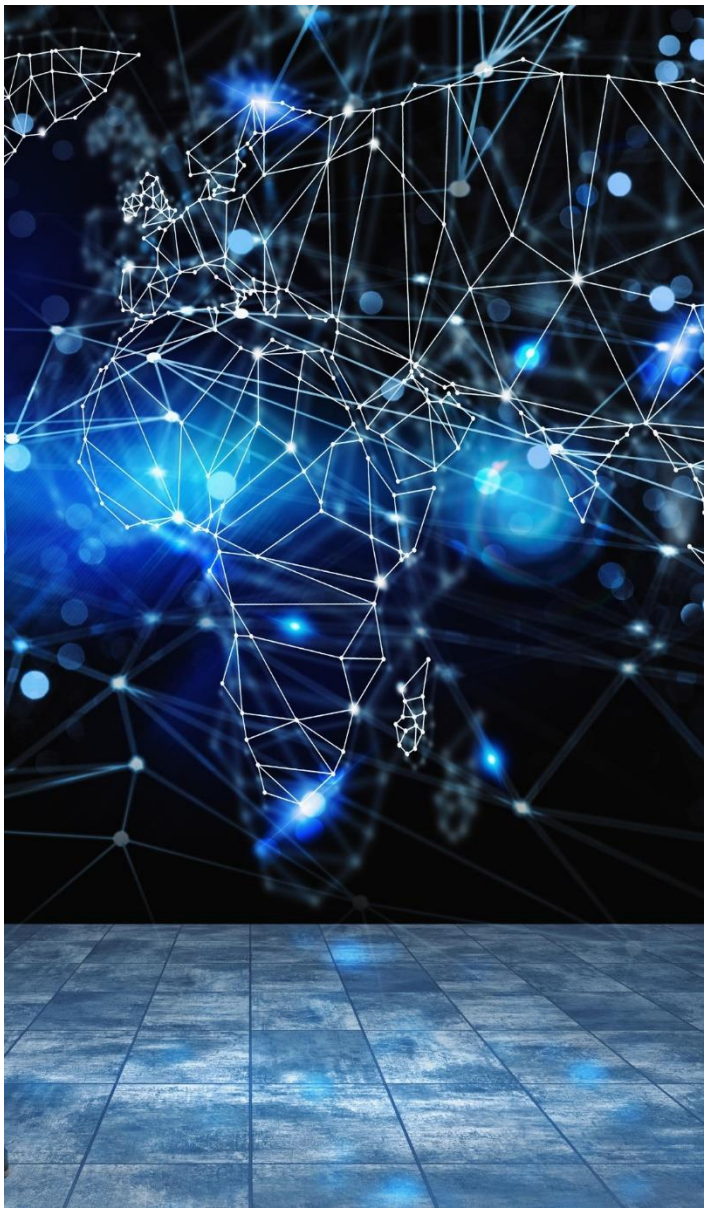
- Egy törvény vagy szabályozás változása lényeges hatással lehet az RPA és a CI technológiák korai alkalmazóira.
- Egyes nagy mértékben szabályozott folyamatok (pl.: adatvédelem) esetében nem mindenhol engedélyezett a botokkal történő automatizáció.
- Az RPA vagy CI segítségével létrehozott hibás és/vagy hiányos, szabályozó számára készített jelentések szabályozói problémákat és magas bírságokat eredményezhetnek.
- A botok magatartása szembe mehet a hatályos törvényekkel (pl.: az algoritmusok megtanulása a kisebbségek jogellenes megkülönböztetéséhez vezethet).
- Amennyiben a bizalmas vagy korlátozás alá eső információk gyűjtésére használt szoftverbotokat nem a szigorú kontrollokkal együtt implementálják, az az adatvédelmi standardokkal és szabályozásokkal szembeni nem-megfelelést vonhat maga után.

Szervezeti kockázatok:

- A teljes munkaidős alkalmazottnak megfelelő munkaerő (FTE) cseréje vagy új munkakörben történő alkalmazása negatívan hathat a dolgozói morálra.
- A csoportok közötti nem megfelelő egyeztetés hiányosságokhoz vezethet a feladatok és felelősségek terén.
- A botokkal kapcsolatos változások végrehajtásával kapcsolatos standardok hiánya hátrányosan hathat a változáskezelési folyamatokra.
- Egyetlen bot több FTE-t is kiválthat, ami koncentrációs kockázatot eredményezhet.
- A botok újketetű alkalmazása képzési kihívásokat eredményezhet az érintett felek körében.

Technológiai kockázatok:

- A létező IT platformon végzett rutin karbantartási változtatások hatásait az érintett robot rendszereknél szükséges lehet regressziós teszteléssel megvizsgálni.
- Az automatizációs algoritmus "fekete dobozos" valósága behatárolja a technológia működésére vonatkozó átláthatóságot.
- A szoftveres botnak szüksége van megfelelő hozzáférésre, hogy adatokat, rendszereket és alkalmazásokat érjen el. Mint minden rendszerhasználó, egy bot is jelenthet információbiztonsági és hozzáférési kontrollal kapcsolatos kihívásokat.
- A botokat szabálytalanul is felhasználhatják feladatok végrehajtására vagy adatgyűjtésre. Különböző kibertámadási módokra is fogékonyabbak hardver-es, firmware-es illetve alkalmazási szinteken.
- Az üzletmenet-folytonosság és katasztrófa-helyreállítási programoknak számolnia kell a kockázatokkal, amelyeket a fejlett analitika, az RPA és a CI technológiák jelentenek.
- A bot betanítására használt adat lehet hiányos, elavult vagy irreleváns, ami hibás végkimenetelt eredményezhet.
- A rosszul megtervezett botok, melyek gyorsabban működnek mint ahogy az a megállapodásokban (SLA-kban) elvárt, túlterhelhetik a létező IT rendszereket.



A digitalizációból fakadó kockázatok ellenőrzésének tudománya

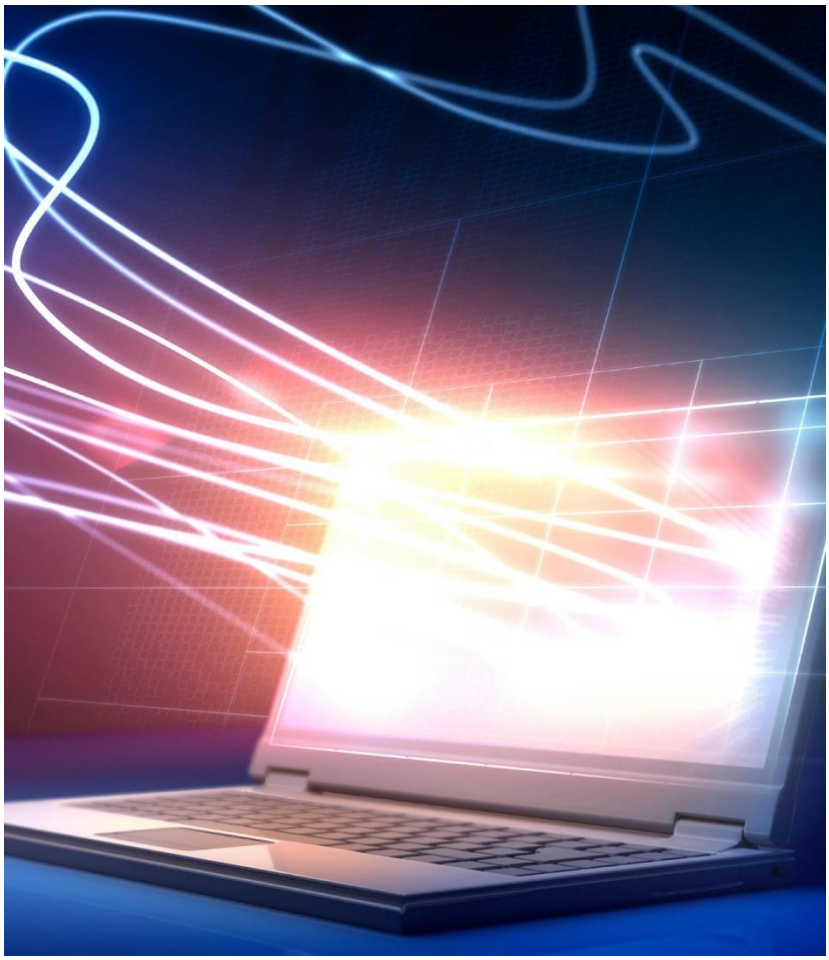
Az RPA és CI technológiák meglévő kontrollkörnyezetre gyakorolt hatásának felmérése, beleértve az új kockázatokat is, elengedhetetlen a legkorszerűbb technológiák sikeres alkalmazásához. Azért a spanyol viaszt nem kell felfedeznünk! Elegendő a létező módszerek kiterjesztése a vállalati kockázatokra.
A technológiák értékelése során a belső ellenőrzésnek meg kell találnia a hangsúlyt a következő feladatok között:

Bizonyosság nyújtás: Hagyományos bizonyossági szolgáltatások nyújtása

Tanácsadás: Megbízható tanácsadói tevékenység

Előrejelzés: Felkészülés új kockázatokra

Ez az egyensúly a szervezet alkalmazkodási szintjének érettségétől és a belső ellenőrzési osztály stratégiai célkitűzéseitől egyaránt függ.



Lépjen túl az egyszerű ellenőrzések és megfelelés fogalmán! Építsen egy ellenálló, értékteremtésen alapuló, előremutató belső ellenőrzési funkciót.

+ Bizonyosság
Magabiztosság

+ Előrejelzés
Előre tekintés

+ Tanácsadás
Betekintés

Bizonyosság nyújtás

A bot fejlesztési életciklusa során felmerült kockázatok (lásd. 4. ábra) nem feltétlenül újkeletűek. Pusztán a jellemző IT kockázatkezelési keretrendszer kiterjesztéséről van szó. Mialatt a második védelmi vonal (pl. compliance és működési kockázat kezeléséért felelős osztályok) a kontrollok tesztelésének modernizálását sürgeti, és számos szervezet a hatékonyság növelésére kombinált bizonyossági modell felé fordul, nagyon fontos, hogy a belső ellenőrzési osztályok időben bekapcsolódjanak a munkába. Így a belső ellenőrzés hatékony és értékes bizonyosságot szerez dupla munka nélkül.

Néhány gyakorlati szempont, hogy a belső ellenőrzés a bizonyossági szolgáltatás során értéket is hozzáadjon a folyamathoz:

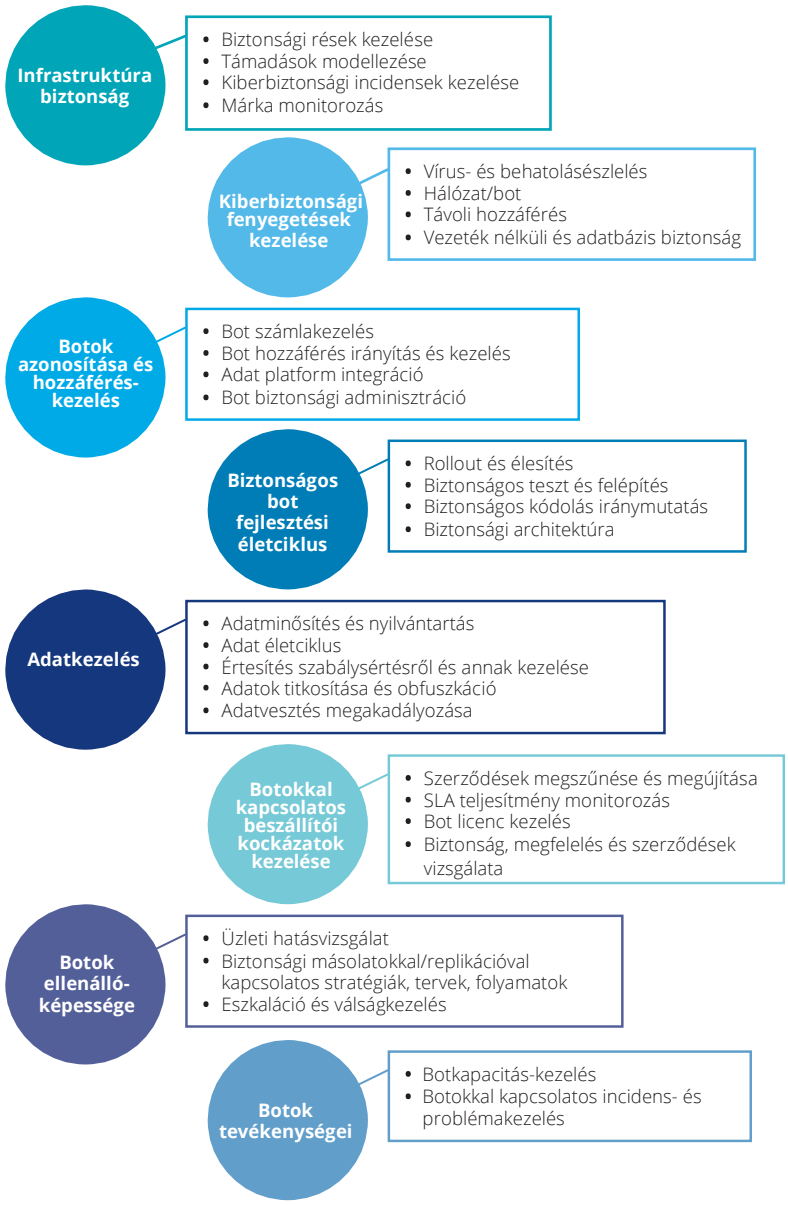
Tesztelés: A belső ellenőrzési osztályoknak hozzáférést kellene kapniuk a tesztelési dokumentációkhoz, és független vizsgálatokat végezniük mintavételek, eredmények és naplózott problémák alapján.

Kivételek kezelése és nyomon követés: Olyan keretrendszert és folyamatot érdemes tervezni, amely nyomon követi a botokat a tesztelési és gyártási környezetben, és osztályozza a felmerülő kérdéseket. A belső ellenőrzés a következő elemeket veheti sorra a botok kialakítási és működési hatékonysága kapcsán nyújtott bizonyossági szolgáltatásoknál:

- **Botok problémáinak azonosítása és megoldása:** Léteznek a vállalatnál eszközök és folyamatok a bot teljesítmények minőségének nyomon követésére, értesülnek-e a dolgozók a kivételekről, és létezik-e előre meghatározott cselekvési terv a szolgáltatások helyreállítására arra az esetre, ha a bot tevékenysége kudarcot vall?
- **Bot változásmenedzsment:** Van olyan standard folyamat, amely a meglévő botok változtatására szolgál, beleértve az érdekelt felek tájékoztatását, valamint az eljárások és bot konfigurációk frissítését?
- **Külső felekkel kapcsolatos kockázatkezelés:** Az automatizálási szoftverek szállítói szerződései megfelelnek az érvényben lévő, külső felekre vonatkozó szabályzatoknak?
- **Üzletfolytonosság:** A továbbfejlesztett üzletfolytonossági és IT katasztrófa elhárítási terv tartalmaz-e olyan lépéseket, amelyek a bot alapú digitális munkaerő működését állítja helyre?
- **Bot felügyelet és compliance:** A botok tevékenységét felügyelő felelősök és compliance munkatársak hogyan biztosítják, hogy a botok megfelelnek a jogszabályi előírásoknak és céges szabályzatoknak?

Újratanúsítási folyamat: A belső ellenőrzésnek az üzleti és technológiai felelősöket arra kell ösztönöznie, hogy az RPA és CI okos automatizációs technológiák kialakítását, implementációját évente újratanúsíttassák. Amennyiben szükséges, az objektív bizonyosság érdekében a folyamatot is tesztelni kell, hogy az a leírtaknak megfelelően kerül kivitelezésre.

4. ábra Reprezentatív bot életcikluskezelési események és altevékenységek[2]



[2]A további, algoritmusokhoz kötődő kockázatokkal kapcsolatos információkért lásd: "Managing algorithmic risks: Safeguarding the use of complex algorithms and machine learning," Deloitte Development LLC, 2017. https://www2.deloitte.com/us/en/pages/risk/articles/algorithmic-machine-learning-risk-management.html

Tanácsadás

Ha egy szervezet az RPA és CI technológiák terén még csak a felfedező szakaszban jár, a belső ellenőrzési osztálynak részt kell vennie az RPA és CI automatizáció pre-implementációs szakaszában. Néhány javaslat, amelyet a belső ellenőrzési osztály felvethet:

- Tanácsadás a szervezetnek a kapcsolódó kockázati tényezők számbavételével kapcsolatban
- Útmutatás jobb teljesítményt és nagyobb értéket teremtő vezető gyakorlatokkal kapcsolatban
- A belső ellenőrzési osztály profiljának javítása, a szaktudás bemutatása az objektivitás megtartása mellett

Néhány gyakorlati javaslat, amellyel a belső ellenőrzés javíthatja megbízható tanácsadói szerepét:

Folyamatok dokumentációja: A belső ellenőrzés biztassa az egyes üzletágakat arra, hogy hozzanak létre és tartsanak fenn könnyen auditálható pre-implementációs dokumentációt. Példák a folyamatok dokumentációjára:

- **Automatizálási stratégia:** Általános üzleti értékkel kapcsolatos célok, hatókör, források (költségek, munkaerő) racionalizálása, a megtérülés és az érték mérésére használt mérési és értékelési rendszer
- **Az automatizálási folyamat dokumentálása**: Részletes folyamatleírások, a mintavételtől a beszámolásig, az automatizálási folyamat kódkezelésének segítése érdekében
- **Automatizálási folyamatleírás**: A robotikai folyamat egészének vizuális megjelenítése
- **RPA programozás, mint az automatizálás eszköze:** A teljes RPA-t lefedő részletes kódolási forgatókönyv minden teszt esetén
- **Munkalapok vizsgálata**: Ideértve a minta kiválasztást, a kivételek jelentését, a teszteredményeket, és a végső teszteredmények összefoglalóját.

A változások átültetése a kockázatfelmérési folyamatba: A belső ellenőrzésnek be kell vezetnie egy folyamatos kockázatértékelési folyamatot, hogy időben tudja minősíteni a különböző innovációk hatását. Ennek érdekében a belső ellenőrzésnek figyelembe kell vennie és integrálnia kell a technológiai változásokat a kockázatelemzési folyamatba.

Dinamikus könyvvizsgálati eljárások végrehajtása: A belső ellenőrzésnek fel kell készülnie arra, hogy gyakrabban hajtson végre dinamikus és hatékony vizsgálatokat, különösen ott, ahol nagy mértékben, sokféle felhasználási módra alkalmaznak botokat.
A belső ellenőrzésnek érdemes megfontolnia, hogy agilis keretrendszer segítségével végez vizsgálatokat. Amennyiben megfelelően alkalmazzák, az agilis belső ellenőrzési keretrendszer a kisebb adagokban, rövid időtartamok alatt történő munkavégzést támogatja, és a kollaborációra összpontosít, beépítve a gyakori visszajelzést és iteratív módon javítva a vizsgálat minőségét.

A jelentéstétel frissítése: A belső ellenőrzésnek fel kell ismernie az RPA és CI automatizációk ellenőrzéséhez szükséges jelentéstételi szintet és struktúrát (pl.: technológiai szint versus üzleti funkció szintje, vagy bizonyosság-alapú versus tanácsadás-alapú).

Előrejelzés

Függetlenül attól, hogy mennyire érett az adott szervezet a diszruptív digitalizáció bevezetése terén, a belső ellenőrzési osztálynak mindenképpen előre kell látnia és összehangoltan monitoroznia kell a felmerülő kockázatokat, stratégiákat kell kidolgoznia, és a kockázatokat ellensúlyozó technikákat kell végrehajtania.
A belső ellenőrzési osztályok az analitika és az új technológiák segítségével hasznosabb, proaktívabb, és a jövőre összpontosító felismerésekre juthatnak.

A tanácsadás és a bizonyossági szolgáltatás mellett a belső ellenőrzésnek előre kell jeleznie az RPA és CI automatizációs technológiákhoz kapcsolódó felmerülő kockázatokat.

A határok feszegetése és a kockázatvállalási hajlandóság közötti egyensúly: Ahhoz, hogy a belső ellenőrzési osztály helyet kapjon a tárgyalóasztalnál és véleményt formálhasson a diszruptív technológiákkal kapcsolatos kockázati stratégiáról, proaktívan meg kell értenie minden egyes RPA és CI automatizált megoldás felhasználási módját. A belső ellenőrzésnek prioritási keretrendszert kell kidolgoznia a legfontosabb kockázatok, például a harmadik felektől származó kockázatok vizsgálatához, amelyek a diszruptív technológiák implementációjából erednek.

Kockázatérzékelés és analitika: Az RPA és CI technológiák implementására való felkészülés során a belső ellenőrzési osztályoknak érdemes adatelemző és kockázatokat felismerő eszközöket használniuk, hogy proaktívan azonosíthassák a felmerülő kockázatokat és megtalálhassák az új technológiák vizsgálatához szükséges legjobb megközelítést.

Válságszimuláció és előrejelző rendszerek: Egy rosszul sikerült szoftverbot-implementációt imitáló, megrendezett krízisforgatókönyvek alapján végzett szimuláció során a belső ellenőrzés valós időben kipróbálhatja magát a szerepében.
Ezzel a módszerrel több szinten: stratégiai, magatartási és taktikai szinten is azonosíthatóak a szervezet reakcióképességében rejlő gyengeségek.

A belső ellenőrzésnek tartania kell a lépést

Ahogy a vállalatok továbbra is diszruptív technológiák bevezetésével törekednek a kézzelfogható működési hatékonyság elérésére, a belső ellenőrzési osztályoknak is tartaniuk kell a lépést. Íme néhány gyakorlati tanács a belső ellenőrzési osztályok számára, hogy hogyan tudják kivenni a részüket a folyamatból:

Stratégiai tervezés és harmonizáció
A belső ellenőrzési osztályoknak meg kell alkotniuk azt a stratégiai víziót, célokat és ütemtervet, amelyek alapján az RPA és CI, technológiákon, illetve a fejlett analitikán keresztül automatizált folyamatok vizsgálatát tervezik. Ennek a megközelítésnek kell meghatároznia a fenti folyamatok vizsgálatának módszertanát (magas kockázat, gyakoriság), a mintavételi módszert, a munkalap-mintákat, valamint a problémamegoldási folyamatokat. Ezen kívül a víziónak összhangban kell lennie a meglévő vállalati kockázatkezelési (ERM) keretrendszerrel és tartalmaznia kell a szervezet általános stratégiai vízióját.

Kockázatelemzés: A belső ellenőrzési osztályoknak a lehető leghamarabb el kell kezdeniük az RPA és CI automatizáció kockázatelemzését. A végzett értékelés alapján a belső ellenőrzési osztályok jobban fel tudják mérni a sérülékeny, illetve a végzett vizsgálatok szempontjából prioritást élvező területeket. A technológiai fejlesztések és az adaptáció mértéke miatt elengedhetetlen, hogy a belső ellenőrzés folyamatosan vizsgálja a digitalizációval járó kockázatokat (lásd 5. ábra).

Analitika és összefoglaló grafikonok (dashboard-ok):
Az analitika segítségével létrehozott, az RPA és CI technológiák állapotát részletesen bemutató összefoglaló grafikonok segítenek abban, hogy a belső ellenőrzés lépést tarthasson a változásokkal.

Továbbképzés és toborzás:
A belső ellenőrzési osztály munkatársainak el kell fogadnia a küszöbön álló automatizálási változást és alkalmazkodnia kell hozzá. Ahhoz, hogy ezek az automatizációs technológiák valóban hatékonyabbá tegyék a munkavégzést, az auditoroknak részleteiben meg kell érteniük azok működését.

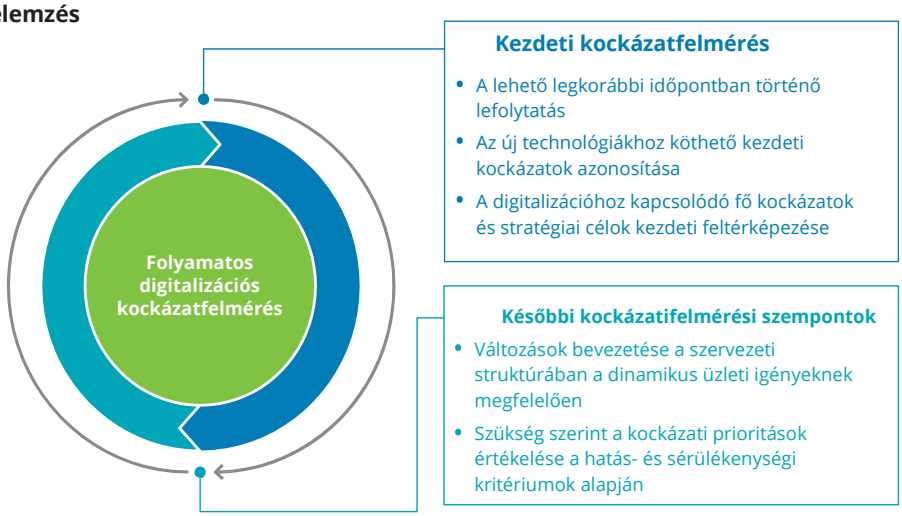
A fentiek mellett a felső vezetés más osztályokon vagy vállalatoknál dolgozó szakértők toborzásával új perspektívákat és tudást hozhat a céghez. Fontos, hogy a belső ellenőrzés munkatársai nem csupán az általuk vizsgált technológiákkal kapcsolatban rendelkezzenek technikai tudással, de az általuk alkalmazott belső ellenőrzési módszertanról is legyenek átfogó ismereteik.

Az automatizáció ereje: Végül, de nem utolsó sorban, a belső ellenőrzésnek érdemes kihasználnia a fejlett analitikában, illetve az RPA és CI technológiákban rejlő lehetőségeket az audit életciklus terén, beleértve a kockázatelemzést, az audit tervezést, a helyszíni vizsgálatot, a munkalapok dokumentációját, valamint a jelentéstételt.Ez nem csak azt teszi lehetővé a belső ellenőrzés számára, hogy modernizálja a vizsgálatok végrehajtására irányuló megközelítést, de kulcsfontosságú tapasztalatokkal szolgálhat az ilyen diszruptív technológiák bevezetésével járó kihívásokkal és kockázatokkal kapcsolatban.

5. ábra Folyamatos digitalizációs kockázat elemzés

A belső ellenőrzés folyamatos feladatai:

- A fő információforrásokból érkező adatok nyomonkövetése és frissítése
- Az alábbi fő kockázati területekhez kapcsolódó kockázatok értékelése és felmerülő fenyegetések azonosítása: kiberbiztonság, szabályozás, adatvédelem, pénzügy, jóhírnév, sikertelen bevezetés
- Az RPA hatásának értékelése a szervezet, a folyamatok, az erőforrások, a régió, a szabályozási környezet, a kiber- és harmadik felek felügyelete, stb. szempontjából



Lépést tartani a fejlődéssel

Az újabbnál újabb digitalizációs technológiák bevezetése vállalkozásonként eltérő. Így a belső ellenőrzés felkészültsége is változó lehet a kockázatokra adott reakció szempontjából. Az általános kihívás azonban ugyanaz: meg kell szokni a kényelmetlenséget, valamint meg kell fogalmazni, hogy hogyan őrizheti meg a belső ellenőrzés a bizonyosság és a tanácsadási szolgáltatások színvonalát a digitalizáció korában.

A Deloitte világszerte elismert tanácsadási üzletága segíthet Önnek kezelni a helyzetet és felkészülni a változásokra. Szakembereink, eszközeink és folyamataink stratégiai megoldásokat kínálnak, hogy segítsenek Önnek megérteni és megvizsgálni az RPA és CI technológiákhoz, valamint a prediktív adatelemzéshez kapcsolódó kockázatokat. Az új diszruptív technológiák egész biztosan egyre növekvő szerepet fognak játszani a vállalatok életében – tapasztalatunk segíthet tartani a lépést!

Kapcsolattartók

A digitalizációhoz, diszruptív technológiákhoz kapcsolódó kockázatok ellenőrzéséről további információt kaphat a Deloitte csapatától:

Szöllősi Zoltán
Director, Risk Advisory
IT kockázatkezelési szakértő
zszollosi@deloittece.com

György Adél Virág
Senior Manager, Assurance
Belső Ellenőrzési Szakértő
agyorgy@deloittece.com

Barta Gergő
Manager, Risk Advisory
Mesterséges Intelligencia Szakértő
gbarta@deloittece.com

Deloitte.