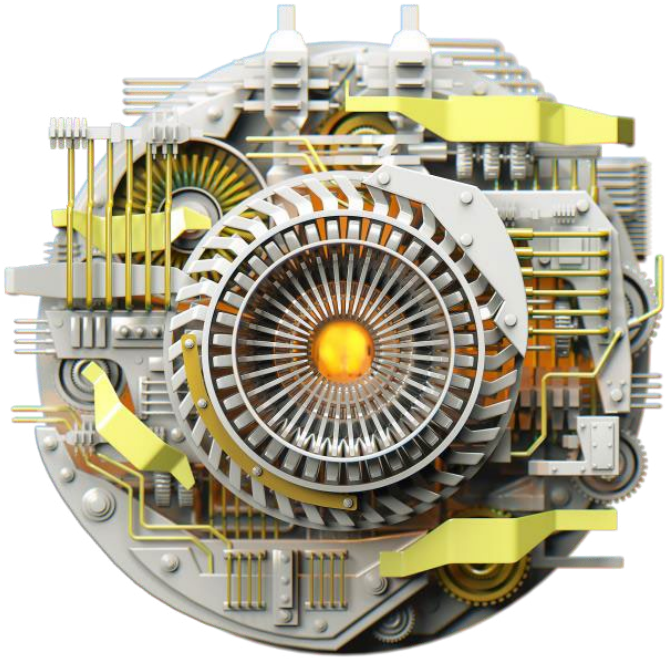
Deloitte.



Správa dát:

Prečo je preverovanie účinnosti sankcií dôležité.

1. Čo je to preverovanie sankcií a kto ho vykonáva?

V roku 2019 viedli donucovacie opatrenia a vyšetrovanie porušovania sankcií k pokutám vo výške 8,14 miliárd USD (celosvetovo) za nedodržanie predpisov AML, KYC a sankčných predpisov.[1]

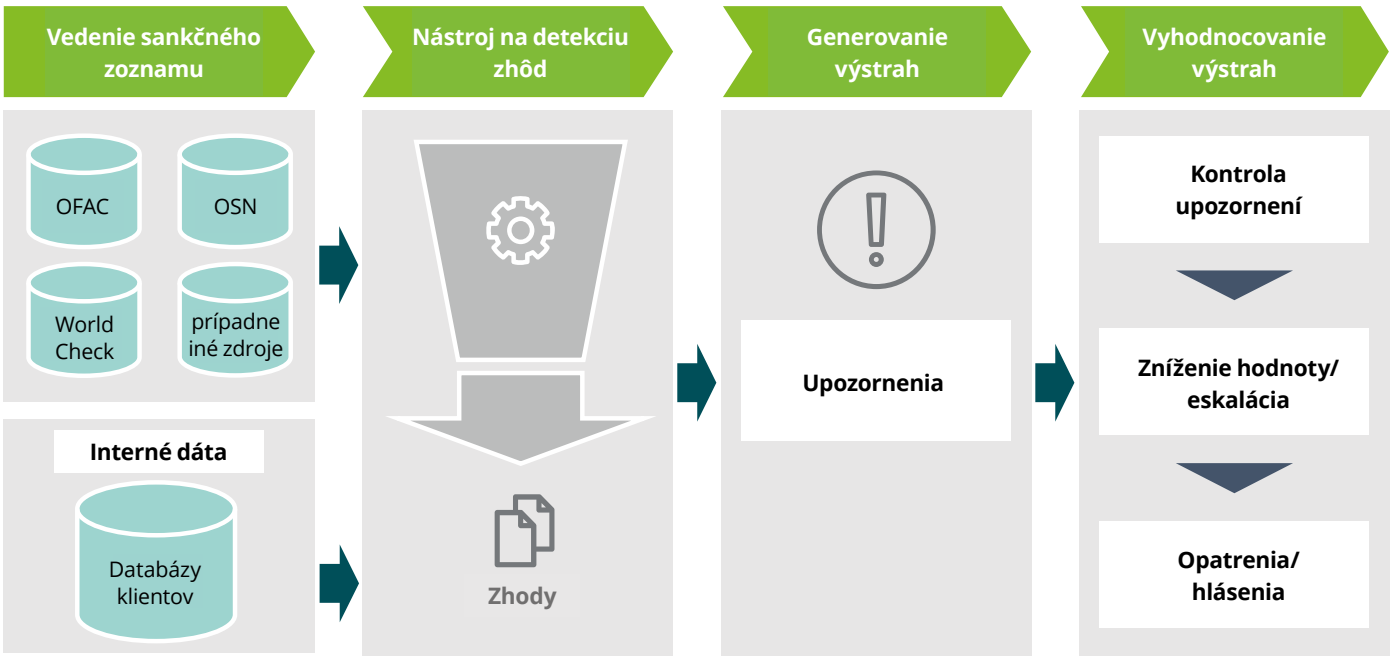
Jedným z príkladov vysokých pokút je napr. pokuta vo výške 8,9 miliardy USD, ktorú zaplatila banka BNP Paribas v roku 2014 americkým úradom za porušenie obchodných sankcií USA. Ďalší prípad je z roku 2020, keď bola Standard Chartered Bank pokutovaná sumou 24,9 mil. USD za vážne porušenie sankcií, t. j. poskytnutie úveru vo výške približne 119,1 mil. USD ruskej banke na Ukrajine. A tretí príklad je z roku 2018, keď Société Générale súhlasila s tým, že americkým úradom zaplatí 1,3 miliardy USD za urovnanie prípadu zahŕňajúceho spracovanie dolárových transakcií v rozpore s americkými sankciami.[2,3] Spojenie so sankcionovanou osobou, subjektom alebo krajinou môže tiež viesť k významnému poškodeniu dobrého mena finančnej inštitúcie.

Vo Wolfsbergských odporúčaniach na preverovanie sankcií sa uvádza, že by finančné inštitúcie mali „udržiavať účinný a efektívny proces preverovania sankcií". Očakáva sa, že väčšie finančné inštitúcie budú na zaistenie súladu s predpismi a na zvládnutie čoraz väčšej zložitosti v oblasti sankcií využívať technológie. Technológie môžu pomôcť vykonať požadovanú analýzu a tiež nevyhnutné kontroly. Použitie vhodných technologických riešení a automatizácie môže zvýšiť efektivitu. Posledné technologické trendy nielenže uľahčili inštitúciám prehľadávanie obrovského množstva dát, ale zvýšili aj očakávania týkajúce sa procesu Due Diligence a štandardov v odvetví.

Sankcie sú hlavnou súčasťou celosvetového úsilia v boji proti finančnej kriminalite. Sú zamerané na štáty, fyzické alebo právnické osoby, ktoré sú zapojené do nezákonných činností alebo sú z nich podozrivé. Vlády a organizácie ako OSN, OFAC a EÚ uvaľujú sankcie a obmedzenia, ale ich uplatňovanie je úlohou finančných inštitúcií. Tie sú povinné prehľadávať svoje klientske databázy a údaje o transakciách, aby odhalili akékoľvek potenciálne porušenia. Niektoré z organizácií, ktoré vydávajú sankčný zoznam, však nemajú právomoc vymáhať tresty, napr. OSN. Na druhej strane existujú vnútroštátne orgány, ako je FINMA vo Švajčiarsku, ktoré presadzujú platné sankčné predpisy. Na dodržiavanie sankcií neexistuje žiadny model „jedno pravidlo pre všetkých", ktorý by bol vhodný pre všetky inštitúcie. Model by mal byť navrhnutý tak, aby zohľadňoval faktory, ako je charakter podnikania inštitúcie, zahrnuté krajiny a používané meny. Aby inštitúcie zaviedli účinný program dodržiavania sankcií, musia najprv určiť rozsah relevantných sankčných predpisov. Program dodržiavania sankcií zahŕňa dva typy preverovacej kontroly: preverovanie transakcií a preverovanie klientov.

Oba typy kontrol závisia od spoľahlivého mechanizmu, ktorý je založený na hľadaní zhody. Ten vzájomne porovnáva dáta z interných a externých zdrojov, aby sa zistili podobnosti naznačujúce možnú zhodu. Len čo je identifikovaná možná zhoda, vygeneruje sa upozornenie. Potom dôjde k presmerovaniu ku kontrolórovi zhody, aby posúdil, či výstraha označuje zhodu „skutočnú" alebo „falošnú". Pri identifikácii skutočnej zhody s dostatočnou istotou musí inštitúcia uplatniť nevyhnutné opatrenia, ako je zablokovanie transakcie a ohlásenie príslušným orgánom.

Proces preverovania sankcií



Aby boli inštitúcie schopné držať krok s meniacim sa prostredím sankcií a zostali v súlade so svojimi regulačnými povinnosťami, je pre ne efektívny proces správy dát kľúčový. V tomto kontexte sa pozrieme na základy správy dát a potenciálny prístup k vybudovaniu robustného programu preverovania sankcií.

2. Čo je to správa dát?

Správa dát zahrňuje zhromažďovanie, údržbu a používanie dát bezpečným, účinným a efektívnym spôsobom. Organizácie vnímajú dáta čoraz viac ako kľúčové aktívum na vytváranie hodnoty, a preto rastie dôležitosť robustnej stratégie správy dát.

„Cieľom správy dát je pomáhať pracovníkom, organizáciám a súvisiacim stranám optimalizovať využitie dát v medziach predpisov a regulácie, aby mohli urobiť rozhodnutia a prijímať opatrenia, ktoré maximalizujú prínos pre organizáciu."[4]

Dobre udržovaná stratégia správy dát môže organizáciám pomôcť získať konkurenčnú výhodu nad ich obchodnými rivalmi, pretože zlepšuje prevádzkovú efektivitu a rozhodovanie. Organizácie, ktoré majú svoje dáta pod kontrolou, tiež môžu byť agilnejšie, môžu skôr zaznamenať trendy na trhu a skôr prijať proaktívne opatrenia.

„Zaobchádzanie s dátami ako s aktívom môže viesť k rôznym výhodám, ktoré sa dajú speňažiť, zmerať a spravovať."[5]

2. 1. Proces preverovania sankcií

Správa dát pozostáva z týchto prvkov:

Riadenie dát

Odkazuje na súbor pokynov (plánovanie, monitorovanie a presadzovanie) na riadenie dátových aktív a zaisťuje, aby všetci dodržiavali pravidlá.[6]

Architektúra dát

Dátová architektúra je koncepčná štruktúra alebo rámec prostredia správy dát, jeho súčastí a interakcií. „Prepája rámec, ľudí, procesy, projektové zásady, technológie a postupy správy a používanie cenných podnikových informačných aktív."[4]

Integrácia dát

Integrácia dát je proces spájania dát z rôznych zdrojov/kanálov zberu dát a ich vkladanie do formátu na spracovanie.

Ochrana dát

Ochrana dát sa týka súkromia a citlivosti osobných údajov o klientoch a postupoch na zabezpečenie toho, aby boli osobné údaje zhromažďované, zdieľané a používané vhodnými spôsobmi.

Kvalita dát

Kvalita dát sa týka presnosti, úplnosti, aktuálnosti a konzistencie dát spolu s požiadavkami a pravidlami na ich použitie. Problémy s kvalitou dát sú väčšinou spojené so správou dát. „Bez správy dát sa úsilie o zabezpečenie kvality dát stáva nákladným jednorazovým úkonom." Aby sa zabezpečila kvalita dát, je potrebné pochopiť jej účel, činnosti, kontext a spôsob merania.[4]

Správa hlavných dát

V obchodnom kontexte sa kmeňové dáta považujú za kľúčové dáta v systéme. Nemajú transakčný charakter, hoci môžu zahrňovať záznamy o transakciách. Predstavujú najcennejšie dátové aktíva organizácie. Účelom správy kmeňových dát je poskytnúť procesy na zber, agregáciu, párovanie a konsolidáciu dát. Kmeňové dáta predstavujú „jediný zdroj pravdy" organizácie, pokiaľ ide o konkrétny súbor dát, a zaisťujú spoločné chápanie situácie.

3. Význam cyklu správy dát pre účinné preverovanie sankcií

Princípy skupiny Wolfsberg hovoria:

> „Preverovanie sankcií sa využíva pri odhaľovaní, prevencii a narušovaní finančnej kriminality, najmä sankčného rizika. V rámci preverovania sa porovnávajú dáta získané z operácií finančnej inštitúcie, vrátane záznamov o klientoch a transakciách zo štruktúrovaných (KYC) aj neštruktúrovaných (produktová dokumentácia, poznámky klientov) so zoznamami sankcionovaných mien a s ďalšími ukazovateľmi sankcionovaných strán alebo miest.“[7]

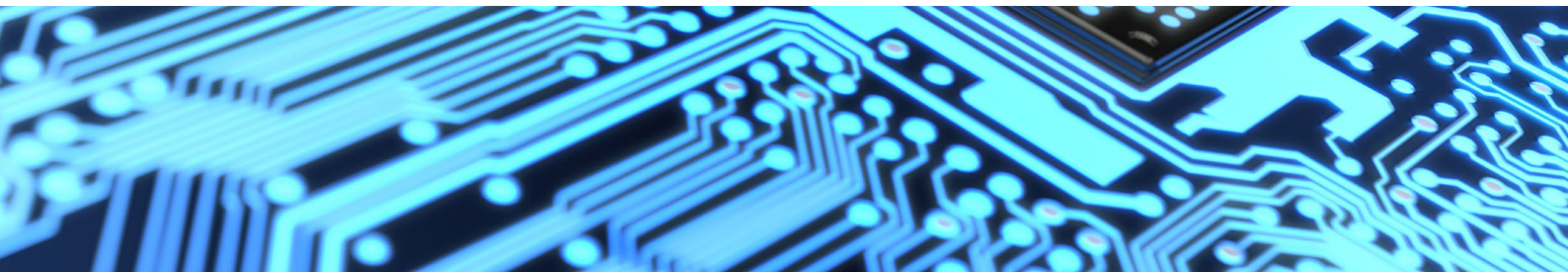
Vzhľadom na to, že finančné inštitúcie denne spracovávajú veľké objemy údajov o klientoch a transakciách, môže byť preverovanie týchto údajov s relevantnými zoznamami sankcií náročnou úlohou. Finančné inštitúcie sú podľa predpisov povinné zaistiť, že nebudú mať vzťah s jednotlivcami alebo subjektmi, ktoré sú na sankčnom zozname, ani so subjektmi, ktoré vlastnia sankcionované osoby a subjekty, alebo sú s nimi prepojené. To nie je jednoduchá úloha, pretože mnoho osôb používa podobné mená, čo má za následok veľké množstvo falošných zhôd vo výsledkoch. Na určenie presnosti zhody možno použiť dodatočné informácie, ako je geografická poloha, adresy, zamestnanie alebo dátum narodenia – úplnosť a kvalita dát zvyšuje možnosť potvrdenia skutočnej zhody.

Finančné inštitúcie sú tiež povinné preverovať vysokorizikové transakcie uskutočňované prostredníctvom klientskych účtov, aby sa zaistilo, že klienti nebudú prevádzať peniaze sankcionovaným jednotlivcom, subjektom, jurisdikciám alebo obchodným sektorom, resp. prijímať od nich peniaze. Každá inštitúcia by sa mala rozhodnúť, ktoré typy transakcií a ktoré atribúty v nich sú relevantné pri preverovaní sankcií. Príjemcovia a odosielatelia transakcií sú relevantní pre sankčné programy založené na zozname, kým adresy sú relevantnejšie na preverovanie podľa geografických sankčných programov. Medzi ďalšie bežné transakčné atribúty používané pri preverovaní patria plavidlá, agenti, sprostredkovatelia a iné textové polia, ako sú referenčné informácie o platbe alebo stanovený účel platby v poli 70 SWIFT správy.

3. 1. Správa dát získaných z preverovania sankcií

Kontroly preverovania sa spoliehajú na interné aj externé zdroje dát. Niektoré kľúčové interné zdroje dát týkajúce sa geografických lokalít a obchodných sektorov sú kmeňové (klientske) dáta, transakčné dáta a ďalšie klientske informácie špecifické pre obchodný sektor. Medzi externé zdroje dát patria sankčné zoznamy a ďalšie ukazovatele sankcionovaných strán. Na skríning a doplnenie zdrojov dát možno tiež použiť ďalšie externé zdroje dát, ako sú verejné registre, vládne zoznamy alebo iné spoľahlivé nezávislé licencované zdroje. Zdroje dát sa často distribuujú medzi viaceré IT systémy a musia byť identifikované, aby bolo možné posúdiť, ktoré prvky dát sú potrebné pre proces skríningu. Účelom identifikácie dát je získať celkový pohľad na klientsku základňu inštitúcie.

Je dôležité, aby všetky zdroje dát mohli byť prepojené a integrované na čo najpodrobnejšej úrovni. Zároveň by mali mať rovnaké štandardy kvality. Skôr ako možno klientske, referenčné alebo transakčné dáta použiť na skríning, musia byť extrahované, doplnené, zmapované, transformované a/alebo nahrané do jedinej platformy. Ak dôjde počas procesu k poškodeniu alebo ohrozeniu dát, model preverovania sankcií nebude fungovať tak, ako bolo zamýšľané. V dokumente pod názvom „Supervisory Guidance on Model Risk Management“, ktorý vydal Úrad menovej kontroly Ministerstva financií Spojených štátov amerických (Office of the Comptroller of the Currency), sa uvádza: „Proces overenia zahŕňa kontrolu, že interné a externé dátové vstupy sú aj naďalej presné, úplné, v súlade s účelom a dizajnom modelu, a v čo najvyššej možnej kvalite.“[8] Finančné inštitúcie by preto mali zabezpečiť, aby sa pravidelne testovala, dokumentovala a sledovala dátová kvalita, úplnosť a integrita.



3. 2. Správa sankčných zoznamov

Hoci sa môže zdať, že sankčné zoznamy sú jednoduché a priamočiare, v praxi zahrňujú veľké množstvo rôznych údajov vrátane mien uvedených subjektov a jednotlivcov, ale aj ďalšie podrobnosti, ako sú známe skratky, akronymy, aliasy a geografické polohy. S cieľom zaviesť efektívny proces riadenia by mali inštitúcie jasne definovať, kto je zodpovedný za doručovanie a vedenie sankčných zoznamov. Prvým krokom v procese správy sankčných zoznamov je určenie priority zoznamov považovaných za relevantné pri preverovaní. Môžu to byť externe získané zoznamy od tretích strán, alebo to môžu byť zoznamy získané z webových stránok regulačných orgánov (napr. OFAC, OSN, EÚ) a tiež interné zoznamy jednotlivcov, subjektov, regiónov, prístavov alebo zakázaného tovaru. Výber zoznamov závisí od rôznych faktorov, ako je typ klientov, ponúkané produkty a charakter podnikania.

Na účely výberu príslušných zoznamov by mali finančné inštitúcie vykonať posúdenie založené na riziku a vziať do úvahy príslušné regulačné požiadavky. Finančné inštitúcie, ktoré na získavanie a udržovanie regulačných sankčných zoznamov využívajú externých dodávateľov, by mali mať formálny proces na zosúladenie zoznamov poskytnutých treťou stranou s regulačnými zoznamami, aby bola zaistená úplnosť. Na druhej strane finančné inštitúcie, ktoré sa spoliehajú len na sankčné zoznamy z regulačných webových stránok, musia zabezpečiť, aby ich proces zahrňoval konsolidáciu dát z viacerých zdrojov, ktoré môžu byť v rôznych formátoch. Okrem toho budú niektorí jednotlivci/subjekty zahrnutí do viac ako jedného zoznamu, takže je nutné odstrániť duplikáty, pretože ak k tomu nedôjde, môže sa upozornenie vygenerovať dvakrát. V takých prípadoch by finančné inštitúcie mali zvážiť realizáciu systému správy sankčných zoznamov na čistenie, analýzu a formátovanie dát zoznamu, aby sa zlepšila presnosť zhody a znížil sa počet falošne pozitívnych výsledkov.

4. Výzvy pri správe dát v súvislosti s preverovaním sankcií

Finančné inštitúcie čelia mnohým problémom so správou dát na účely preverovania sankcií. Ďalej uvádzame vybrané príklady:

Preverovanie politicky exponovaných osôb (PEP) a osôb s väzbou na PEP

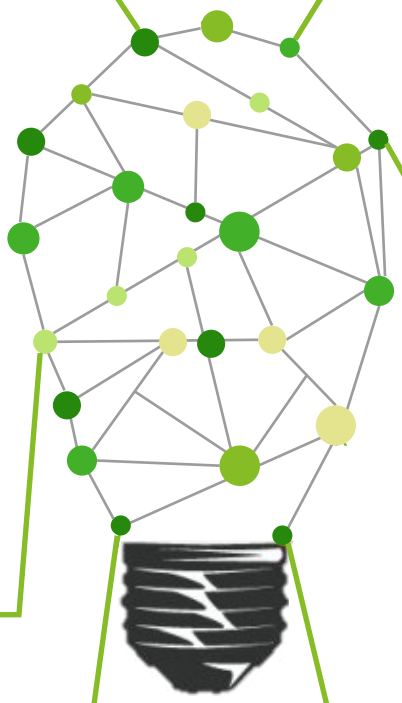
Hoci vládne nariadenia, ako je štvrtá smernica Európskej únie proti praniu špinavých peňazí alebo odporúčanie FATF, poskytujú detailnejšie požiadavky týkajúce sa PEP, neexistuje jasný spôsob, ako identifikovať PEP a ich spoločníkov na celom svete. Existuje mnoho externých poskytovateľov databáz PEP, môže však byť náročné použiť informácie, ktoré obsahujú, na správne priradenie klienta finančnej inštitúcie k PEP. V reakcii na dohľad, ktorý sa na PEP aplikuje, sa PEP snažia nájsť spôsoby, ako sa vyhnúť odhaleniu, ako je otváranie účtov na meno korporácií v offshore jurisdikciách namiesto ich vlastných mien alebo mien členov rodiny.

Rôzne systémy písania a regionálne konvencie pomenovania

Finančné inštitúcie musia často preverovať klientov, ktorí sa nachádzajú na zoznamoch, ale ich mená nie sú pôvodne napísané latinkou, ale čínštinou, azbukou alebo arabčinou, ako sú podozriví teroristi z krajín Blízkeho východu. Mnoho mien teroristov na zozname OFAC SDN tiež obsahuje aliasy. Môže byť užitočné poznať určité pravidlá týkajúce sa mien. Napríklad mnoho arabských mien začína slovom „Abu“, ktoré znamená „otec“. Abu, za ktorým nasleduje podstatné meno, znamená „sloboda“ alebo „boj“ a používajú ho teroristi aj legitímni politickí vodcovia.

Izolované systémy

V mnohých prípadoch nie sú systémy finančných inštitúcií po akvizícii alebo fúzii integrované do ich pobočiek a dcérskych spoločností.



Zjednotenie sankčného zoznamu

Finančné inštitúcie by mali zaviesť účinný proces, ktorý zaistí, že sankčné zoznamy, ktoré používajú v procese preverovania, poskytujú presný a úplný jednotný zoznam na preverovanie.

Nedostatočná správa dát

Neúplnosť, nedostatočná kvalita a integrita údajov sú hlavné dôvody zlej výkonnosti systémov preverovania sankcií. Chýbajúce alebo nesprávne informácie Know Your Customer (KYC) alebo chýbajúce informácie o akcionároch spoločnosti, konečných vlastníkoch, dodávateľoch alebo iných protistranách majú negatívny dopad na účinnosť skríningových nástrojov, pretože vytvárajú veľké množstvo falošne pozitívnych zhôd alebo znemožňujú odhaliť sankcionované subjekty či jednotlivcov.

Manuálne spracovanie dát

Klientske dáta sú často zadávané do bankového systému ručne počas procesu onboardingu, čo tiež zvyšuje pravdepodobnosť chýb.

Objem dát

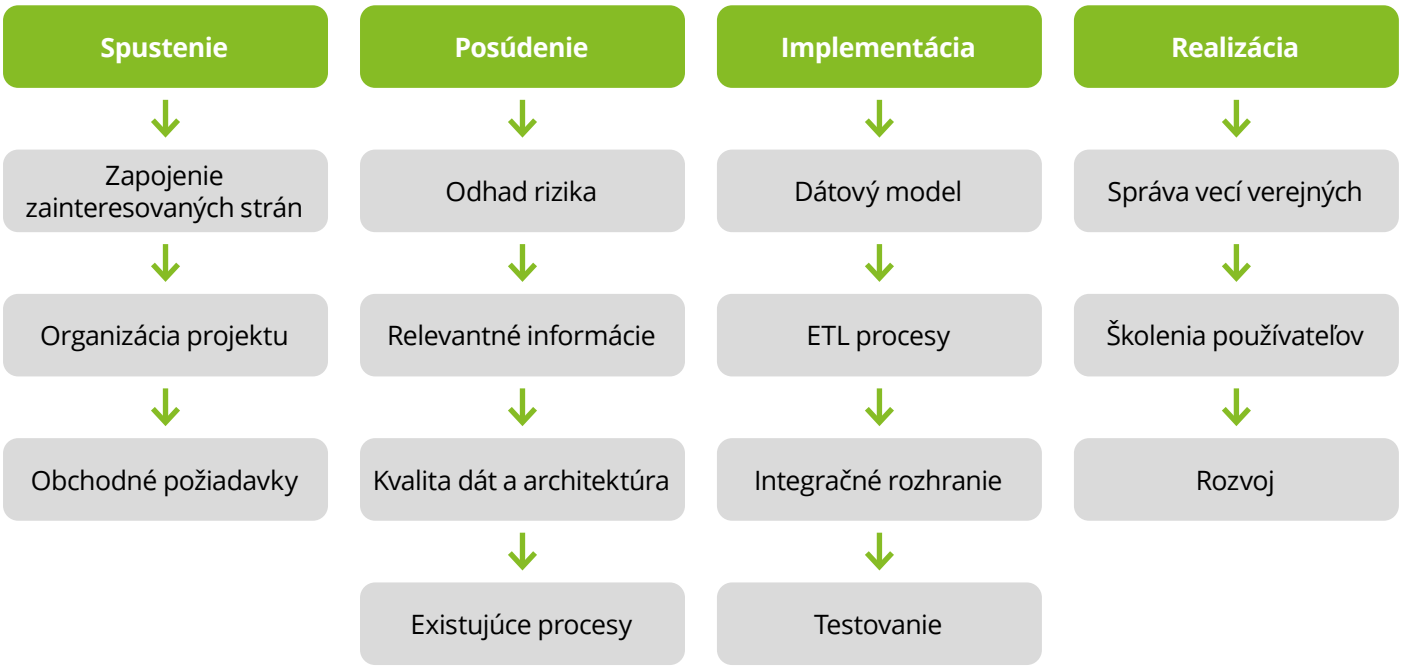
Veľký objem dát súvisiaci s komplexným procesom preverovania sankcií spôsobuje, že prevádzka systému manuálneho spracovania je veľmi náročná, resp. nemožná.

5. Možné riešenia a jeho prínosy

5. 1. Návrh a realizácia

Uvedený obrázok znázorňuje realizáciu a fungovanie riešení pre finančné inštitúcie pri zavádzaní efektívneho procesu preverovania sankcií. Riešenie by malo byť čiastočne automatizované, prispôsobené konkrétnym obchodným potrebám a navrhnuté s holistickým prístupom založenom na riziku. Riešenie vo všeobecnosti prebieha podľa definovaného procesu, ktorý sa skladá z nasledujúcich krokov:

Proces preverovania sankcií



Spustenie

Vyžaduje sa prístup zhora nadol, do ktorého sú od samého začiatku zapojené príslušné zainteresované strany. Na efektívny proces preverovania sankcií sú potrebné technológie a prístup založený na dátach. Organizácia projektu by mala byť definovaná vopred, aby bolo možné zapojiť príslušné zainteresované strany do všetkých fáz projektu.

Posúdenie

Posúdenie je založené na obchodných požiadavkách a zaoberá sa súvisiacimi rizikami, kvalitou požadovaných dát a dátovou architektúrou, ako aj existujúcimi procesmi, na ktoré má vplyv skríningový systém.

Implementácia

Dátový model vytvára technický základ pre potenciálne riešenia. Mal by byť flexibilný a rozšíriteľný. Prispôsobené procesy „extrakcie, transformácie, načítanie" (ETN) musia zaistiť, že sa budú zhromažďovať aktuálne dáta a že budú vhodne transformované. Integračné rozhrania umožňujú využívať informácie relevantným obchodným procesom.

Realizácia

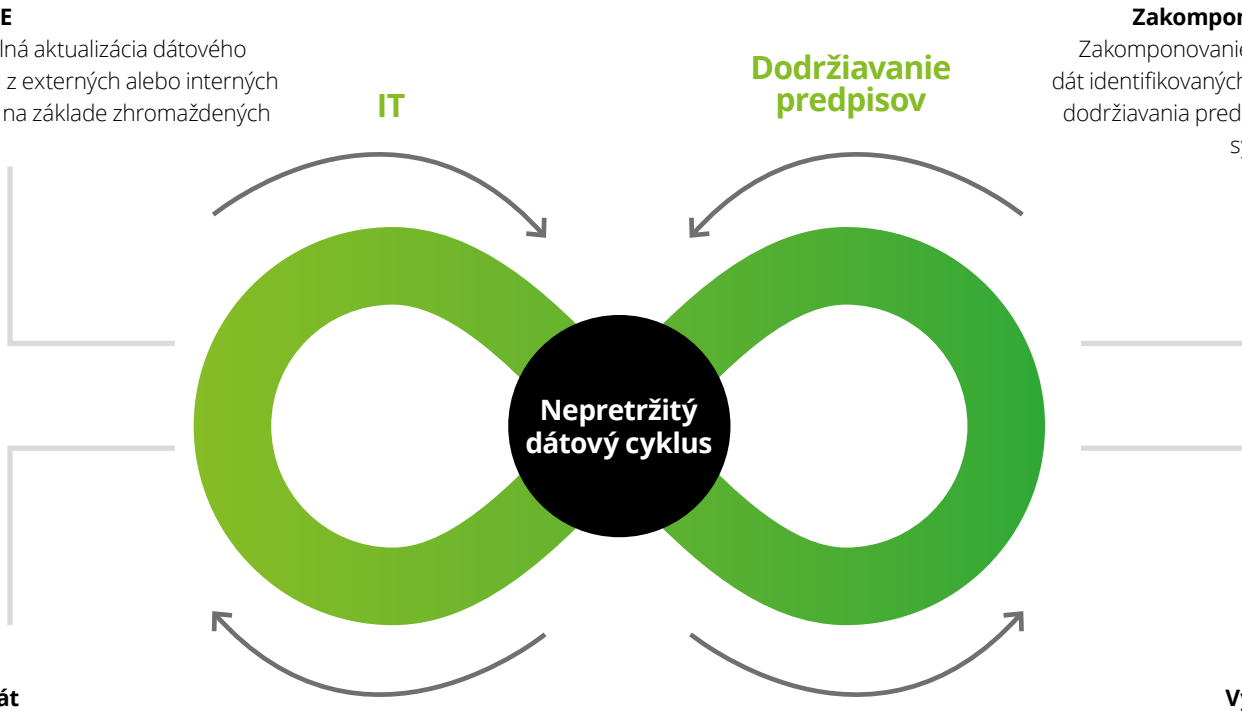
Pred uvedením technologického riešenia do prevádzky musí byť zadefinované riadenie procesu a používatelia musia byť vyškolení. Ďalším zásadným aspektom je nasadenie a údržba riešení, napr. riadenie jednotlivých verzií riešení v procese nasadenia, aby sa zaistilo zefektívnenie údržby a aby boli nové verzie správne nasadené.

5. 2. Návrh a vykonanie

Len čo je systém v prevádzke, mal by zabezpečiť nepretržitý cyklus dát medzi IT systémami organizácie a systémom skríningu oddelenia compliance. Dáta generované procesom kontroly sankcií by sa mali automaticky aktualizovať v zodpovedajúcich IT systémoch. Tieto dáta môžu obsahovať zistenia z interného vyšetrovania alebo z aktualizácie modelu hodnotenia rizikovosti klientov. To umožňuje IT systémom extrahovať presné dáta na ich zahrnutie do skríningového modelu.

UPDATE
Pravidelná aktualizácia dátového modelu z externých alebo interných zdrojov na základe zhromaždených dát

Zakomponovanie
Zakomponovanie ďalších dát identifikovaných v rámci dodržiavania predpisov do systémov



Zber dát
Zakomponované dáta sa zbierajú z bankových systémov a vkladajú sa do procesu kontroly sankcií

Využitie
Využitie aktualizovaných dátových modelov pre procesy dodržiavania predpisov

Táto schéma ukazuje rámec pre nepretržitý cyklus správy dát na účely preverovania sankcií. Interné dáta z IT systémov organizácie prúdia do procesu skríningu, kde sa dopĺňajú o ďalšie informácie a následne sa vracajú späť do IT systémov. Aby sa zaistila kontinuita procesu, mala by sa vymenovať osoba zodpovedná za správu dát, ktorá bude vykonávať funkciu dohľadu. Stručne povedané, efektívna správa dát a analýzy zohrávajú dôležitú úlohu pri odhaľovaní a znižovaní rizika finančnej kriminality. Regulačné orgány na celom svete zdôrazňujú dôležitosť zavádzania nových technológií na posilnenie programov preverovania sankcií finančných inštitúcií.

6. Trendy v preverovaní sankcií

Vzhľadom na rastúce množstvo dát a neustále sa meniace prostredie kontroly sankcií sa automatizácia spracovania a katalogizácie dát spolu s kontrolou sankcií v reálnom čase stáva nevyhnutnosťou. V poslednom čase sa vo veľkých inštitúciách objavuje trend zavádzania komplexnejšieho prístupu a väčšieho využitia dostupných dát.

„Zdieľanie informácií je zásadné v boji proti praniu špinavých peňazí, financovaniu terorizmu a financovaniu šírenia zbraní hromadného ničenia. Prekážky v zdieľaní informácií môžu negatívne ovplyvniť účinnosť úsilia v oblasti boja proti praniu špinavých peňazí/ financovaniu terorizmu. To zdôrazňuje význam rýchleho, zmysluplného a komplexného zdieľania informácií.“[9]

7. Zdroje

[1]"AML, KYC & Sanctions Fines for Global Financial Institutions Top $36 Billion Since Financial Crisis", Fenergo, 2020,
https://www.fenergo.com/news/aml-kyc-and-sanctions-fines-for-global-financial-institutions-top-$36-billion-since financial-crisis.html

[2]"Banks adopt AI to manage sanctions and compliance risk", A. Ross, 2020,
https://www.ft.com/content/98e82234- 16a8-11ea-b869-0971bffac109

[3]"Standard Chartered fined $24.9M for Ukraine sanctions breaches", N. Hodge, 2020,
https://www.complianceweek.com/sanctions/standard-chartered-fined-249m-for-ukraine-sanctionsbreaches/28686.article

[4]"What Is Data Management?", Oracle, 2020,
https://www.oracle.com/database/what-is-data-management/

[5]"Data integration: after the teenage years. Recruit Institute of Technology", B. Golshan, A. Halevy, G. Mihalia, W-G. Tan, 2017,
https://dl.acm.org/doi/pdf/10.1145/3034786.3056124

[6]"Big data privacy: a technological perspective and review. Journal of Big Data ", P. Jain, M. Gyanchandani, N. Khare, 2016,
https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-016-0059-y

[7]"Wolfsberg principles on sanctions screening", The Wolfsberg Group, 2019,
https://www.wolfsbergprinciples.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

[8]"Supervisory Guidance on Model Risk Management", Office of the Comptroller of the Currency, April 4, 2011,
https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

[9]"FATF Private Sector Information Sharing Guidance", Financial Action Task Force, November 2017,
https://www.fatfgafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

Kontakty:

Martin Kubačka
Partner | Deloitte Česká republika
mkubacka@deloittece.com
+420 776 306 694

Tomáš Mihóčik
Director | Deloitte na Slovensku
tmihocik@deloittece.com
+421 910 820 005

Marie Vichrová
Specialist Lead | Deloitte Česká republika
mvichrova@deloittece.com
+420 735 715 397

Preložené z anglického originálu Data management: Why it matters for effective sanctions screening,
ktorý bol publikovaný na webovej stránke Deloitte Switzerland.

Deloitte.