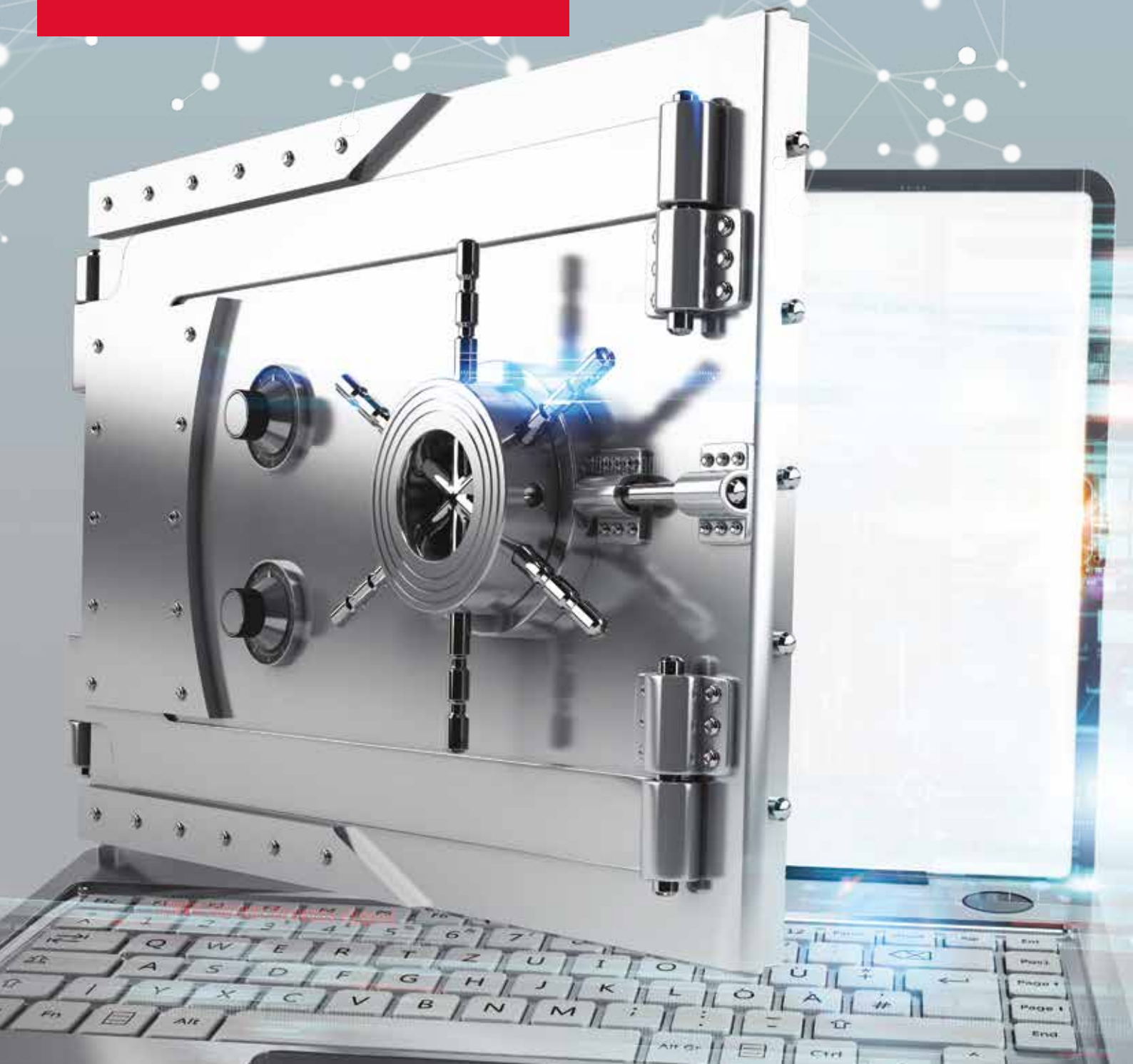
CGI

La force de l'engagement[MD]

PROTECTION **DES BANQUES**

Une nouvelle approche pour lutter contre le crime financier



Solution de protection des banques

Les banques ressentent de plus en plus le fardeau associé au crime financier, qui crée d'énormes pressions sur leurs ressources et sur leurs budgets. Comme les fraudeurs les plus astucieux continuent de contourner et d'éluder les contrôles des banques, les organismes de réglementation de tous les territoires mettent continuellement en place de nouvelles mesures. Les objectifs visés par les activités de conformité des établissements bancaires sont donc en constante évolution.

Vu la tendance des paiements en temps réel et l'accélération de la transformation numérique en vue de répondre aux attentes des consommateurs, qui recherchent l'instantanéité et la personnalisation, les banques disposent de peu de temps pour assurer le suivi des transactions et remédier à leurs faiblesses. Cette lacune se traduit par une pression accrue sur les services de conformité, déjà surchargés.

Ces facteurs changent la façon dont les institutions financières luttent contre le crime financier. L'approche cloisonnée ne convient plus, car la prévention du crime financier touche désormais l'ensemble des services, des processus et des produits d'une entreprise, de même qu'un grand nombre de ses membres. La gestion efficace du crime financier doit passer par la mise en place d'une plateforme intégrée.

Solution de protection des banques

Bien que chaque institution possède divers moteurs de vérification et de suivi en temps réel des transactions, leur mise en œuvre est différente d'une banque à l'autre. Cependant, nous avons pu constater que certains aspects sont communs à toutes les banques. Par exemple, la plupart des opérations sont effectuées en vases clos au sein de l'institution.

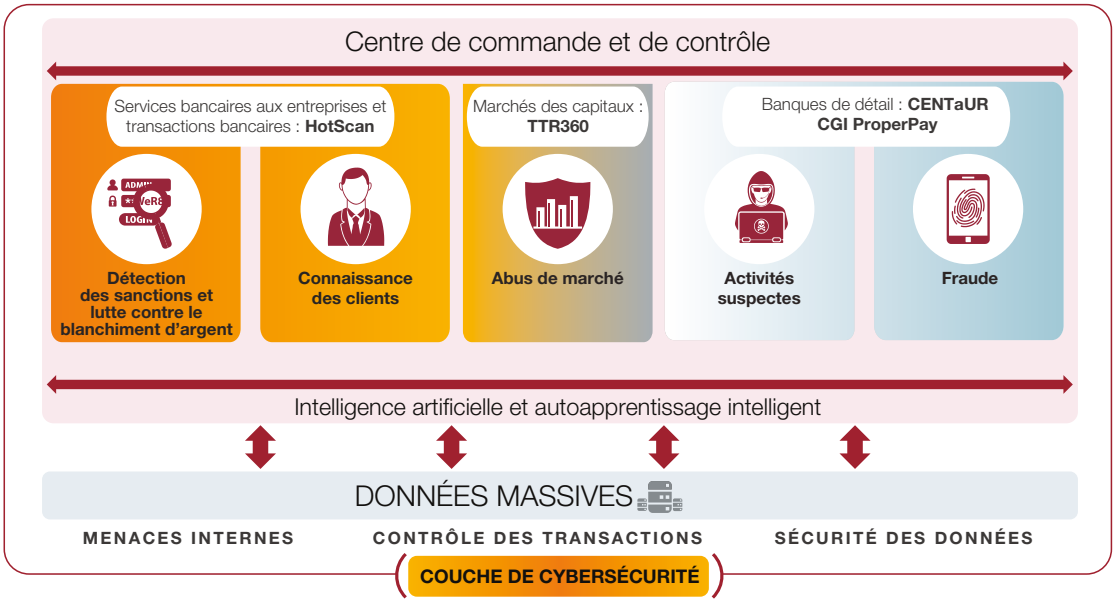
Avant d'émettre des recommandations quant à l'application de la solution de protection des banques de CGI et aux éléments du cadre de gestion à choisir de façon à obtenir rapidement des avantages, nous devons évaluer la situation actuelle de la banque par l'entremise d'un court mandat de services-conseils. Dans la mesure du possible, cette évaluation est prise en charge par un expert sectoriel travaillant dans la même région que la banque.

La solution de protection des banques regroupe plusieurs composantes, ou outils numériques, dans un seul cadre de gestion qui convient à toute organisation. Elle ne vise généralement pas à remplacer l'ensemble des moteurs d'analyse et des solutions de filtrage de base, mais plutôt à mettre en place une série d'outils conçus pour accroître l'efficacité, la vitesse et la précision de l'infrastructure existante. Dès sa mise en œuvre, la solution de protection des banques contribue à réduire le nombre de faux positifs, à repérer de nouveaux types de fraude et à générer une efficacité accrue.

Fonctionnement

La solution globale de protection des banques assure la prévention du crime financier à l'échelle de l'organisation. CGI collabore avec ses clients en leur offrant un ou plusieurs des services suivants : services-conseils en stratégie, gestion du changement organisationnel et des programmes, intégration des systèmes, mise en œuvre de la solution, gestion déléguée et impartition des processus d'affaires.

Le cadre de gestion de la solution de protection des banques de CGI s'intègre dans toutes les unités cloisonnées afin de mettre en place une plateforme efficace de gestion du crime financier. Sa mise en œuvre peut se faire indépendamment des autres solutions déployées au sein de la banque. CGI propose toutefois des produits et services à la fine pointe du marché afin de compléter la solution de protection des banques, notamment : le logiciel de filtrage HotScan qui offre des fonctions de détection des sanctions et de connaissance des clients, CENTAuR pour surveiller les activités suspectes,



la solution ProperPay de CGI qui comporte des capacités de prévention de la fraude, ainsi que le produit TTR360 qui gère la production de rapports sur les abus de marché et les transactions.

Ces solutions sont regroupées dans un centre de commande et de contrôle (ou gestionnaire de cas) où l'ensemble des alertes et des avis font l'objet d'une gestion, d'une distribution, d'un traitement et d'un suivi centralisés.

Afin de générer les gains d'efficience nécessaires, chaque composante fait appel à des fonctions d'autoapprentissage intelligent appliquées à chaque unité cloisonnée et alimentées par les sources de données massives. Examinez le graphique ci-dessus afin de découvrir les détails des composantes et processus de base de la solution de protection des banques.

Il est de plus en plus difficile de réduire les coûts tout en améliorant les contrôles internes et la conformité aux mesures de lutte contre le blanchiment d'argent, de prévention de la fraude et de sanctions. Cette difficulté tient surtout au volume élevé de transactions, au flux continu de nouvelles réglementations complexes, aux systèmes désuets de suivi des activités suspectes et de détection de la fraude, ainsi qu'aux processus manuels laborieux. Les banques doivent mettre en place des contrôles technologiques robustes qui leur permettent de lutter contre le crime financier et d'avoir accès à une piste de vérification de qualité.

La solution de gestion de cas Case Management de CGI met en place un gestionnaire de cas intégré qui reçoit et gère l'ensemble des alertes, des avis et des transactions non conformes repérés par tous les services de la banque. La solution Case Management est utilisée comme centre de commande et de contrôle pour gérer efficacement les alertes, les sanctions, la fraude, les activités suspectes et le cybercrime.

Elle offre notamment les fonctions suivantes :

- Automatisation des flux de travaux (nombre illimité de processus ou de règles d'affaires)
- Gestion des documents
- Communication (messagerie, rappels, reports)
- Suivi de l'état
- Planification et établissement de calendriers (y compris la planification automatisée ou l'utilisation d'un calendrier interactif)
- Production de rapports
- Configuration (permet aux utilisateurs professionnels avancés de gérer le modèle d'information)
- Renseignements sur les règles d'affaires et sur les flux de travaux des unités d'affaires
- Modèle de sécurité en fonction du rôle (offre des menus de navigation personnalisés en fonction des droits d'accès de l'utilisateur)

Le centre de commande et de contrôle assure une efficience et une protection accrues. Vu le volume croissant de transactions, la complexité grandissante des actes criminels parrainés par l'État et l'augmentation du nombre des fonctions d'entreprise qui adoptent des solutions en temps réel, il s'agit d'un outil indispensable pour la plupart des institutions financières. Ce n'est qu'en regroupant les alertes dans un seul système que les banques sont en mesure de repérer des cyberattaques et des crimes financiers complexes à l'échelle de l'organisation. En plus d'offrir une protection accrue, cette fonction est essentielle pour générer les gains d'efficience nécessaires à la transition vers les transactions en temps réel.

Détection des sanctions

Les institutions financières sont prises entre leur obligation de prévenir les transactions illégales et les coûts croissants des activités de conformité. Une fonction robuste de détection des sanctions permet de réduire considérablement le temps et le coût associés à la conformité aux sanctions en analysant toutes les transactions et en avertissant automatiquement l'organisation des correspondances avec les listes de surveillance.

HotScan, le logiciel primé de détection des sanctions de CGI, fournit aux institutions financières les moyens de se conformer à la réglementation internationale en matière de lutte contre le blanchiment d'argent. Il fait appel à des techniques de correspondance approximative, gère une multitude de listes et de territoires, traite des données structurées et non structurées, et met à profit l'exploration de données. La solution HotScan recherche des références à des personnes, des entreprises et d'autres entités avec lesquelles les transactions sont illégales, qui sont visées par des sanctions ou qui représentent un risque accru.

Le logiciel de filtrage HotScan de CGI est conçu pour analyser toutes les données sur les paiements et sur les clients, pour avertir la banque des correspondances avec les listes de surveillance et pour répondre à la réglementation croissante en matière de conformité. Sa capacité de pointe de réduction des faux positifs minimise les retards de transactions et examine rapidement toutes les données sur les clients tout en assurant une diminution des risques et des coûts opérationnels.

HotScan comporte les éléments suivants :

- Techniques de « correspondance approximative » fondées sur des algorithmes évolués qui détectent les personnes et entités frappées de sanctions, malgré les fautes d'orthographe accidentelles ou volontaires pouvant masquer leur véritable identité
- Contrôle des données non structurées et comparaison avec les données structurées
- Capacités de traitement dans la langue d'origine afin d'analyser et d'interpréter tous les alphabets étrangers, scripts et translittérations
- Algorithmes permettant l'analyse rapide en temps réel des données
- Paramètres et règles d'analyse configurables qui permettent l'ajustement pour améliorer la précision et atteindre les objectifs propres à l'organisation en matière de risque

Connaissance des clients

HotScan offre également des capacités de connaissance des clients. Elles comprennent notamment des vérifications diligentes ponctuelles en temps réel et un processus de détection par lot intégré aux vérifications mensuelles des comptes des clients.

Le logiciel comporte un module permettant d'établir la liste des personnes politiquement vulnérables ainsi que des capacités intégrées d'autoapprentissage intelligent. L'intégration de l'autoapprentissage intelligent aux processus de connaissance des clients permet de mettre en place un filtre d'apprentissage qui réduit considérablement le nombre de faux positifs et augmente l'efficacité sans nuire aux activités.

Grâce aux capacités de connaissance des clients de HotScan, les banques peuvent :

- rehausser leur productivité en diminuant les interventions manuelles et en éliminant les interruptions de traitement;
- minimiser le risque opérationnel par l'atteinte d'un équilibre entre la vérification des comptes bloqués et le maintien du traitement continu des transactions;
- évaluer les risques par comparaison des données aux listes de terroristes, d'entités frappées de sanctions, de personnes politiquement exposées et d'autres groupes à risque;
- réduire jusqu'à 50 % le nombre de fausses alertes sans compromettre la diligence et l'exactitude du filtrage, ce qui diminue le nombre de transactions à vérifier manuellement, améliore l'efficacité des opérations de contrôle de conformité et entraîne d'importantes économies de coûts.

La surveillance des activités suspectes, qui passe notamment par l'analyse ou l'enquête des modèles d'action inhabituels, est une question de premier plan assujettie à d'importantes réglementations (la Bank Secrecy Act, par exemple). Ce processus repose sur la détection de situations établies comme irrégulières par les organismes de réglementation ou par les services de police. Son efficacité démontre à quel point il est nécessaire de moderniser les méthodes traditionnelles, qui présentent des lacunes, en réduisant au maximum les activités en vases clos, et de fusionner les processus d'affaires dans une perspective synergique.

Le maintien de l'approche cloisonnée entraîne l'apparition de zones grises et, qui plus est, la perte des synergies. Les avantages créés par cette synergie ont également une incidence sur les unités fonctionnelles, comme celles responsables des contrôles internes, de la conformité et des enquêtes, de la gestion du risque et de la gestion de la lutte contre la fraude. La solution de protection des banques favorise à la fois les synergies et la réduction des coûts.

La solution de surveillance des activités suspectes CENTAuR de CGI intègre une plateforme modulaire ouverte qui permet d'évaluer et d'analyser le risque en surveillant le comportement des comptes sur un ou plusieurs canaux à l'aide de données

Fraude

La fraude est un acte malhonnête ou criminel visant à tromper pour obtenir un avantage financier ou personnel.

Un fraudeur est une personne qui agit dans l'intention de tromper, habituellement en affirmant avoir certaines compétences ou certifications alors que ce n'est pas le cas.

À la lumière de ces définitions, on constate toute l'étendue de la problématique et de ses nombreux aspects. La fraude est un comportement criminel. Il faut donc faire appel aux qualités humaines et à l'informatique judiciaire pour empêcher les fraudeurs d'avoir une longueur d'avance.

La solution de lutte contre la fraude ProperPay de CGI aide les institutions bancaires à prédire, à prévenir et à contrer les actes frauduleux. Elle peut être configurée selon les règles d'affaires propres à l'organisation. Accessible dans le nuage sécurisé Microsoft Azure, la solution offre des fonctions d'analyse prédictive, de gestion des flux de travaux et de gestion des règles ainsi que des meilleures pratiques reconnues à l'échelle mondiale pour une souplesse et une puissance accrues. Voici ses principales caractéristiques :

internes et externes. Elle comporte également des règles prédéfinies utilisées en vue de repérer les activités et les transactions suspectes réalisées par les clients ou les employés.

CENTAuR offre les caractéristiques suivantes :

- Système puissant et extensible d'évaluation du risque en temps réel
- Adaptateur doté d'une interface d'intégration
- Module d'analyse prédictive fondé sur des méthodes statistiques évoluées, des graphiques et des modèles
- Visualisation des données et résultats des processus analytiques
- Gestion de cas
- Production de rapports
- Entreposage des données issues des analyses (y compris la création de profils et de caractéristiques comportementales)
- Des algorithmes avancés permettant de prédire les comportements et les anomalies dissimulés dans les données – La suite Cortana Analytics de Microsoft met à profit l'apprentissage artificiel, l'intelligence perceptive et l'informatique en nuage pour réaliser des analyses prédictives. En intégrant les nouvelles données reçues, les modèles sont en mesure de produire des résultats d'une fiabilité et d'une reproductibilité accrues.
- Une fonction d'analyse visant à prévenir les fraudes et à protéger les clients en permettant au personnel de cerner les comportements et de vérifier les données au moyen de divers écrans et tableaux de bord.
- Un accès sécurisé visant à protéger les renseignements sur les clients – Le nuage Azure Cloud satisfait à de nombreuses normes de conformité internationales et sectorielles, notamment les normes ISO 27001, HIPAA1, FedRAMP2, SOC 1 et SOC 2.
- Une technologie permettant de détecter, d'interrompre et de récupérer les transactions irrégulières afin de préserver les revenus de la banque – Les fonds générés par la récupération des paiements irréguliers permettent d'améliorer l'expérience client. Par ailleurs, la convivialité des fonctionnalités d'affaires offre au personnel des TI la possibilité de traiter d'autres priorités.

Intelligence artificielle et autoapprentissage intelligent

Les fonctionnalités d'intelligence artificielle et d'autoapprentissage intelligent sont conçues pour offrir rapidement un rendement du capital investi aux institutions qui doivent contrôler la réduction de leurs faux positifs. L'une des caractéristiques les plus importantes de toute plateforme de gestion du crime financier est sa capacité d'autoapprentissage intelligent. En effet, cette fonction génère une boucle de rétroaction qui améliore le filtre en découvrant automatiquement les personnes et entités autorisées, ce qui réduit le nombre de faux positifs et simplifie le processus d'examen. De plus, il est possible de mettre en œuvre un certain degré d'intelligence artificielle dans le but d'améliorer l'analyse et le traitement en temps réel.

Il a été démontré que la capacité d'autoapprentissage peut entraîner une réduction du nombre de faux positifs allant jusqu'à 70 %, sans diminuer la précision du filtre ni rétrécir le champ de recherche.

Les utilisateurs ont en outre accès à l'historique des faux positifs, à la liste des bons clients repérés et à des modèles d'efficacité.

De nombreuses institutions utilisent déjà des solutions d'autoapprentissage intelligent, qu'elles appliquent à leurs unités cloisonnées. La plateforme de protection des banques de CGI offre cependant la possibilité d'étendre l'autoapprentissage à toutes les fonctions d'entreprise en leur donnant accès à des sources de données massives. Ainsi, de nouveaux algorithmes peuvent être mis en œuvre en vue de générer des gains d'efficience dans l'ensemble des fonctions et des processus, ce qui se traduit par l'amélioration globale de l'efficacité et de la protection. Les systèmes de gestion de la fraude et des sanctions peuvent alors communiquer entre eux afin de transmettre les données et les résultats en temps réel.

Analyse de données massives et gestion de données massives

Il arrive souvent que les données (petites ou massives) ne soient pas structurées (les instructions de paiement, les notes manuscrites, les listes électroniques disparates, etc.), ce qui peut faciliter la tâche aux criminels. Pour résoudre ce problème, non seulement les banques doivent disposer d'outils de détection capables de lire et de traiter les données non structurées, mais elles doivent aussi être en mesure de structurer ces données afin de les intégrer à un processus numérique simplifié.

En plus de mettre à profit son expertise, ses solutions et ses partenariats, CGI propose à ses clients l'approche Data2DiamondsMD, qui permet de simplifier la gestion des données et d'en tirer la pleine valeur grâce à l'analyse. Ce cadre de gestion propose un modèle pour réussir à optimiser l'utilisation de l'information. Nos objectifs sont les suivants.

- Réduire la « distance » qui sépare les données et les personnes qui en ont besoin
- Recueillir des renseignements sur les habitudes des populations et des machines
- Aider les clients à utiliser ces renseignements afin d'améliorer leurs résultats

Grâce à plus de 5 000 professionnels spécialisés en intelligence d'affaires et en gestion de l'information, CGI offre une vaste gamme de services d'intelligence d'affaires à ses clients, notamment des services-conseils, des services d'intégration de toutes les applications des principaux fournisseurs, des services de gestion déléguée ainsi que des services liés aux systèmes hébergés en nuage.

CGI a d'ailleurs démontré, dans le cadre de projets pilotes, que les sources de données existantes permettent de repérer de nouveaux types de fraude au moyen d'algorithmes qui cernent les modèles sans être fondés sur des règles. Au fil du temps, les données massives seront davantage intégrées aux éléments d'intelligence artificielle afin de pouvoir prédire l'origine des fraudes avant même qu'elles ne surviennent.

La solution de protection des banques tire profit des données massives pour offrir une protection accrue en repérant les types de fraude qui, auparavant, réussissaient à contourner les contrôles en place.

Cybersécurité

En règle générale, les infractions aux sanctions commises par les banques proviennent d'un membre qui a fait un usage abusif de ses identifiants ou qui a utilisé ceux de quelqu'un d'autre afin de contourner les processus de la banque. Ces manquements aux sanctions entraînent de lourdes amendes auprès des organismes de réglementation, une atteinte à la réputation et des retombées négatives importantes sur le bénéfice net.

La cyberprotection et la protection des données font partie intégrante des activités de CGI. Afin d'assurer la sécurité de leurs processus clés et des secteurs responsables de la conformité, les banques doivent parfois mettre en place des contrôles et des outils de cybersécurité supplémentaires qui cerneront les menaces internes avant qu'elles ne frappent. Nous adoptons une approche axée sur les activités opérationnelles pour tous les volets de la sécurité, notamment les audits, les exigences en matière de conformité, les politiques et l'architecture Notre offre complète comprend des services-conseils et des services de formation, l'intégration et la mise en œuvre, la gestion déléguée des services de sécurité ainsi que des services de cyberassurance.

La solution de protection des banques comporte diverses caractéristiques de cybersécurité visant à protéger davantage les banques, particulièrement contre les menaces internes, qui représentent le type d'atteinte à la sécurité le plus courant et le plus grave. Nous aidons nos clients à protéger leur entreprise par l'évaluation et l'analyse des risques informatiques potentiels, la surveillance constante des menaces en temps réel et la mise en place des moyens de défense nécessaires en vue d'assurer la continuité des activités, même en cas d'incident.

Abus de marché

Bien que rien ne puisse égaler la surveillance en temps réel du système commercial exercée par le cadre de contrôle, les organismes de réglementation passent au crible une tonne de données obtenues par le truchement de rapports sur les opérations et les transactions. Jusqu'à maintenant, ce sont ces organismes qui repéraient les irrégularités laissant entrevoir une manipulation ou un abus du marché et qui se servaient des vitrines commerciales pour déterminer dans quelle mesure les organisations s'acquittaient ou non de leurs responsabilités. Cette façon de faire entraîne souvent des enquêtes plus poussées.

Les systèmes intelligents de production de rapports permettent plutôt de prévenir ces problèmes, non seulement en validant les rapports dès le départ, mais également en exécutant un triage rapide et précis en vue de cerner la cause première le plus tôt possible. L'outil de dépistage des abus de marché intégré à notre solution de protection des banques offre aux institutions financières une solution globale de production de rapports et de gestion qui assure leur protection interne tout en garantissant leur conformité aux exigences de déclaration de chaque territoire.

La solution de production de rapports sur les opérations et les transactions TTR360 de CGI offre des services complets de gestion déléguée intelligente qui permettent de respecter les exigences réglementaires grâce à la déclaration des transactions et à la publication des opérations. Ce service assure la gestion des opérations et des transactions dans divers formats et langues en les normalisant et en les stockant avant d'envoyer les rapports réglementaires à l'APA (Approved Publication Arrangement), au TR (Trade Repository) ou à l'ARM (Approved Reporting Mechanism), selon les exigences.

La solution TTR360 est un service de gestion déléguée intelligente, car elle offre non seulement une fonction de validation préalable des rapports, mais également des capacités de triage automatisé, de gestion des exceptions et de gestion de cas pour les opérations refusées. De plus, des modules facultatifs de services juridiques et d'analyse prospective axés sur les futures réglementations connexes sont intégrés à la solution.

Conclusion

En adoptant une approche intégrée de gestion du crime financier, les institutions financières sont en mesure d'assurer une protection optimale, d'améliorer le rendement du capital investi en gestion du risque et en conformité, et de rehausser leur réputation.

La solution de protection des banques de CGI offre un service global et conforme à la réglementation de gestion du crime financier qui permet de mettre en œuvre des processus numériques simplifiés et abordables tout en assurant la sécurité de l'organisation.

À propos de CG

Dotés d'une expérience de plus de 20 ans en production et en distribution de solutions rentables de gestion du crime financier, les quelque 500 experts en conformité et en sécurité de CGI mettent à profit leur vaste compréhension du contexte réglementaire pour aider les grandes organisations du monde entier à lutter contre le crime financier.

CGI soutient et définit le marché des services financiers depuis près de 40 ans. Nous avons participé à l'élaboration de la toute première mouture du réseau interbancaire SWIFT et avons collaboré avec

70 % des principales institutions financières du monde, y compris 8 des 10 plus grandes banques mondiales.

Plus qu'un simple fournisseur, nous sommes un partenaire. Grâce à une approche cohérente, disciplinée et responsable en matière de prestation de services, CGI affiche un bilan inégalé de projets réalisés selon les échéances et budgets prévus. Grâce à notre engagement auprès de nos clients, leur indice moyen de satisfaction des 10 dernières années a été constamment supérieur à 9 sur 10. Nous aidons les institutions financières, y compris la plupart des grandes banques et compagnies d'assurance, à réduire leurs coûts, à augmenter leur efficience et à améliorer leur service à la clientèle.