De l'impérieuse nécessité de repenser les dispositifs de sécurité financière

Par François Jaussaud

Associate Partner, Industry Solutions, IBM France

Table des matières

À propos de l'auteur

François Jaussaud
Associate Partner, Industry Solutions, IBM France

Intervenant à l'Université Paris Dauphine, il est directeur des offres gouvernance, gestion des risques opérationnels et conformités d'IBM France.

Expert métier, aux côtés de nos clients, il conçoit des dispositifs antifraudes, de lutte contre le blanchiment et de financement du terrorisme qui exploitent les capacités technologiques telles que l'intelligence artificielle ou la blockchain.

Diplômé de l'ESC Bordeaux en ingénierie financière, il dirige depuis 2003 de grands projets de transformation des fonctions Conformité de grands établissements financiers français.

Dans son dernier rapport annuel d'activité[1], TRACFIN souligne que l'année « 2016 est marquée par une nette dégradation de la pertinence des signalements et un appauvrissement sensible du travail d'analyse réalisé par les professionnels ».

Ce constat est d'autant plus inquiétant qu'il intervient au moment où TRACFIN observe que « les réseaux spécialisés dans les escroqueries de grande envergure continuent d'innover ».

Pour les observateurs et les acteurs du secteur bancaire et financier, il est indispensable que les dispositifs de lutte contre la fraude, le blanchiment et le financement du terrorisme soient repensés.

« Les réseaux spécialisés dans les escroqueries de grande envergure continuent d'innover »

Rapport annuel d'activité TRACFIN, juillet 2017.

1. La combinaison de plusieurs facteurs, externes et internes, à l'origine du constat critique réalisé par TRACFIN

Les facteurs externes

a. Le nouveau paysage de la finance : le marché bancaire a été bouleversé par l'émergence de nouveaux usages (digitalisation des services bancaires), de nouveaux acteurs (agrégateurs de comptes, initiateurs de paiement), de nouveaux moyens de paiement (Apple Pay, Paylib…), de nouveaux modes de financement (crowdfunding, crowdlending, crowdequity) et même de nouvelles monnaies virtuelles (Bitcoin, Ethereum…). Même s'ils sont difficilement quantifiables, ces phénomènes impactent directement les risques opérationnels.

1. Rapport annuel d'activité TRACFIN 2016, publié le 19/7/2017, www.economie.gouv.fr/files/ra-tracfin-2016_0.pdf.

En 2016, hausse historique du nombre d'informations reçues et analysées par TRACFIN[1]

- 64 815 informations adressées à TRACFIN (+43 % vs 2015),
- 13 592 enquêtes réalisées à partir des informations reçues (+28 % vs 2015),
- 448 notes transmises à l'autorité judiciaire et 1 441 notes transmises aux administrations.

1. Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016, publié le 12/12/2017 - www.economie.gouv.fr/files/rapport-analyse-tracfin-2016.odf

b. Une réglementation française, européenne et internationale complexe, exigeante, contraignante : l'obligation de moyen pour lutter contre la fraude, le blanchiment et le financement du terrorisme s'est peu à peu transformée en obligation de résultat.

Complexe : la révision par l'administration Obama de l'embargo US imposé à l'Iran est un parfait exemple de cette complexité. Les sanctions n'ont été levées que partiellement. Être en conformité avec les obligations de cet embargo partiel exige un examen approfondi du sous-jacent et des contreparties pour être en mesure d'apprécier la nature conforme ou non conforme d'une opération en provenance ou à destination de l'Iran.

Exigeante : ces dernières années, certaines responsabilités relevant de la puissance publique ont été progressivement transférées aux acteurs privés. Et les pouvoirs publics attendent d'eux une vigilance irréprochable.

Dans son rapport annuel d'activité[2], TRACFIN indique que le « secteur est supposé avoir une connaissance très approfondie et actualisée de ses clients, de leur patrimoine et de leurs pratiques financières, qui devrait conduire à des analyses pertinentes des faits générateurs de soupçons. Pour ces raisons, le Service attend de ces professionnels que leurs déclarations de soupçon présentent des analyses pertinentes et mettent les faits générateurs de soupçon en perspective avec les éléments liés à la connaissance du client ».

Contraignante : le Code pénal stipulant que le « blanchiment [est] le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit », les conséquences d'un manque de diligence et de rigueur de la part des établissements financiers peuvent être lourdes pour les structures, leurs dirigeants et leurs collaborateurs.

2. Rapport annuel d'activité TRACFIN 2016, publié le 19/7/2017, www.economie.gouv.fr/files/ra-tracfin-2016_0.pdf

« En cas de défaut de vigilance, l'ACPR peut, entre autres, prononcer une sanction financière dont le montant est fixé dans la limite du plus élevé des deux plafonds suivants : 100 millions d'euros ou 10 % du CA total »

C'est l'ACPR qui dispose du pouvoir de prendre des mesures de police administrative et du pouvoir de sanction.

En cas d'insuffisances caractérisées du dispositif, de défaut de vigilance, de carence dans l'organisation des contrôles ou d'une exposition non maîtrisée au risque, elle peut :

- Nommer un administrateur provisoire ;
- Prononcer une sanction financière dont le montant peut être fixé dans la limite du plus élevé des deux plafonds suivants : 100 millions d'euros ou 10 % du CA total ;
- Prononcer une interdiction d'exercer en cas de responsabilité directe et personnelle.

En 2017, plusieurs grandes banques françaises ont été sanctionnées par l'ACPR, le montant global des pénalités infligées cette année ayant doublé par rapport à 2016.

Mentionnons également une mauvaise campagne de presse qui pourrait impacter l'image publique de l'entreprise ou encore entraîner une surveillance renforcée de l'établissement par l'autorité de contrôle, ce qui l'obligerait à réduire son appétit au risque et pourrait impacter ses résultats.

c. Le profil des criminels a changé : les réseaux criminels et les « loups solitaires terroristes » ont émergé.

Les réseaux et entreprises criminelles : le ratio bénéfice/risques a conduit des organisations criminelles à se positionner et à investir pour développer des capacités de fraude et de blanchiment.

Elles sont polymorphes (plus ou moins structurées), internationales (pour faciliter leur immunité judiciaire), pluridisciplinaires (capables de faire appel à des compétences de hackers, de mules…) et susceptibles d'investir du temps et de l'argent pour étudier leurs cibles et développer des stratégies d'attaque sur le court, moyen et long terme.

Un exemple d'action criminelle « décloisonnée » : le bust-out

Le « bust-out » est une méthode particulièrement redoutable qui revêt diverses formes. Nous prendrons l'exemple d'une banque de détail et d'un client particulier. L'entrée en relation se fait sous une fausse identité, le titulaire du compte simule une activité de salarié, un statut de locataire, etc. Ses revenus sont conformes à son profil, ses dépenses sont raisonnables, sa propension à épargner est dans la moyenne. Un peu plus d'un an après l'ouverture de son compte, il sollicite un découvert, une hausse du plafond de sa carte à débit différé ou un prêt pour réaliser un projet. Une fois le prêt débloqué, tout va très vite : au cours d'un week-end, les comptes sont vidés (virements, chèques et carte sont utilisés simultanément par le réseau criminel qui se dissimule derrière la fausse identité). Les biens acquis sont monétisables (billets de train remboursables, véhicule revendu…). Pendant l'année de fonctionnement « normal », le compte a en réalité été utilisé pour blanchir de l'argent ; les fonds obtenus lors de la sortie frauduleuse peuvent être employés à des fins de financement d'actes terroristes.

Les « loups solitaires » terroristes : partageant un lien idéologique avec une entreprise criminelle, ils opèrent avec un isolement relatif et font le plus souvent appel au microfinancement.

Leur discrétion rend leur identification complexe, le risque étant de discriminer systématiquement certains sous-ensembles de la population française dont le profil répond aux mêmes critères.

d. Les différents types d'actions criminelles ne sont plus cloisonnés : si la loi établit une distinction claire entre la fraude, le blanchiment et le financement du terrorisme, l'observation sur le terrain révèle l'inverse : les frontières s'estompent.

TRACFIN indique ainsi dans son rapport d'analyse 2016 : « les réseaux d'escroquerie d'envergure, agissant en bande organisée, se conjuguent avec les réseaux de blanchiment internationaux à grande échelle. L'interaction est permanente. (…) un même réseau peut cumuler plusieurs activités.

Les réseaux se superposent et s'entrelacent entre eux, ce qui crée des synergies entre les différentes escroqueries, les fraudes douanières, la fraude fiscale et le blanchiment ».

Les facteurs internes

a. Une surveillance ensilotée : depuis plusieurs années, les établissements sont conscients de leurs responsabilités. En réaction aux différentes vagues d'attaques et de réglementations, ils ont élaboré des réponses adaptées à chaque nouvelle menace (phishing, fraude carte…)/exigence (procédure LAB et LAT…). Chaque réponse a fait l'objet d'une solution personnalisée, déployée et maintenue par des ressources opérationnelles dédiées.

Avec le temps, ces mesures efficaces pour détecter des schémas spécifiques (et anciens) se sont révélées insuffisantes et coûteuses.

Les établissements financiers ont rencontré des difficultés pour faire évoluer ces solutions ultraspécialisées, pour adresser de nouveaux schémas, pour traiter de nouvelles sources de données (non structurées, internes et externes…), pour s'intégrer dans les chaînes transactionnelles et s'interconnecter avec d'autres systèmes de surveillance... Ces systèmes d'analyses en silos ont rapidement été identifiés et leurs failles exploitées par les fraudeurs.

b. Des faux-positifs mortifères : au quotidien, les systèmes actuellement déployés génèrent à tort des alertes. Ces faux-positifs sont inévitables et même nécessaires.

Seuls l'œil et l'expertise humaine sont capables de qualifier une anomalie : tentative de fraude, de blanchiment, de financement du terrorisme…

Cependant, le taux de faux-positifs est surveillé de près par les responsables de la sécurité financière pour deux raisons :

- La multiplication des faux-positifs dégrade la productivité des collaborateurs qui doivent examiner l'alerte ;
- L'accumulation de faux-positifs nuit à la vigilance humaine et donc à l'efficacité du dispositif. Ce point est d'ailleurs particulièrement délicat en matière de gestion de ressources humaines.

c. Des faux-négatifs ignorés en raison des limites techniques d'apprentissage et de croisement de données. L'étude des signalements internes, des contentieux, des réclamations clients et des demandes d'information des autorités se heurtent :

- À l'accessibilité difficile, voire impossible, des données externes et internes, qui demandent à être agrégées et croisées ;

- À la rigidité et à la puissance limitée d'apprentissage des systèmes, peu avancés en matière de conceptualisation et de modélisation pour bâtir et faire évoluer un référentiel.

Les solutions des éditeurs spécialisés ont permis d'absorber le choc de l'accélération des agressions et de l'inflation des réglementations ces dernières années.
Ainsi aidées, les banques ont déployé de nouveaux systèmes de sécurité financière dans un temps record.

Pour autant, comme le souligne TRACFIN, le chemin vers un dispositif très efficace est encore long. Comment expliquer au régulateur que le système a bien généré une alerte, mais qu'elle a été noyée dans un tsunami de données… et donc classée sans être examinée attentivement ? Comment reprocher à un collaborateur de ne pas accorder de crédit à un système qui n'est fiable que dans 5 % des cas ? Comment expliquer à un collaborateur, qui prend le temps de justifier sa décision de classer une alerte, que ses retours ne seront pas pris en compte par le système lors de futures alertes semblables ?

L'avenir repose sur les collaborateurs, qui ont développé des expertises fortes, qui perçoivent les limites des logiciels en place et sont désormais en capacité de formuler leurs besoins en matière de dispositif pérenne, holistique, intégré et agile.

2. Repenser les outils de sécurité financière

« Les établissements qui conservent la meilleure qualité d'analyse sont également ceux qui ont réussi à conserver une certaine maîtrise du flux »

Rapport annuel d'activité TRACFIN, juillet 2017.

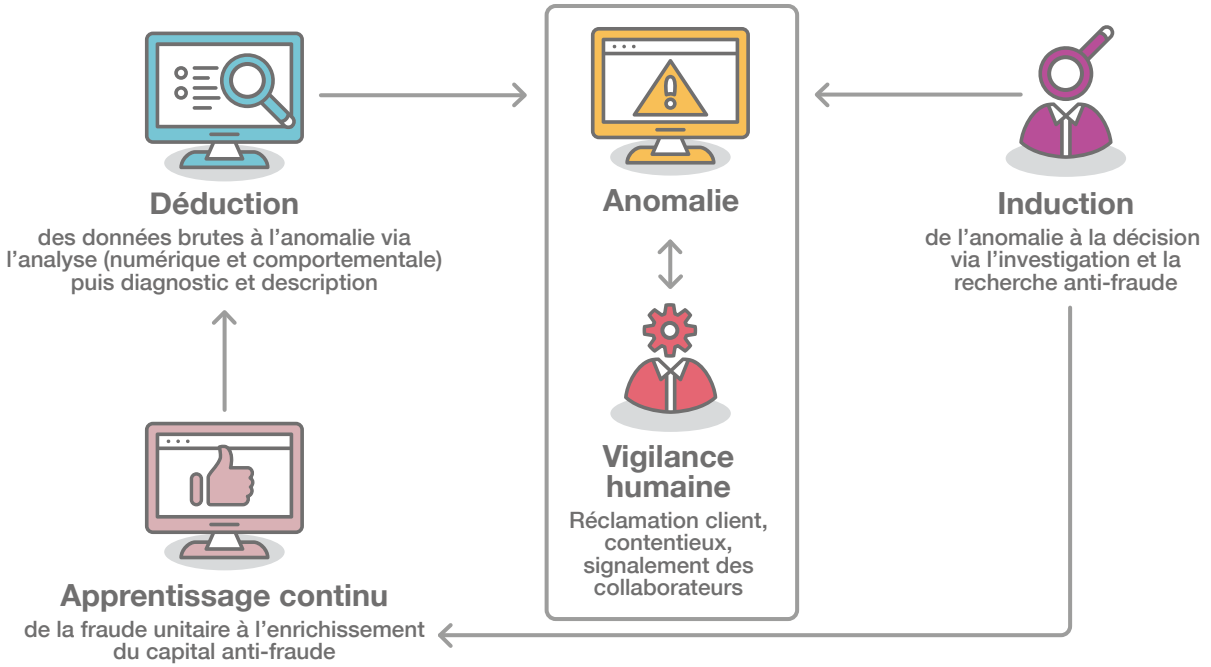
Dans son rapport annuel d'activité 2016, TRACFIN met en cause des déclarations erronées de la part des banques : « dans nombre de cas, le soupçon déclaré porte moins sur des opérations douteuses/suspectes que sur des opérations simplement inhabituelles, lesquelles ne justifient pas nécessairement l'envoi d'une déclaration ».

Et de souligner que « certaines entités de ces groupes [bancaires] se distinguent par une très bonne qualité d'analyse qui se traduit par des « taux de mise en investigation » et de transmission élevés, tandis que d'autres établissements semblent porter leurs efforts sur des typologies peu élaborées de donation non déclarée ou de retraits d'espèces sans soupçon précis sur l'illicéité de l'opération au détriment d'autres schémas de fraude ou de blanchiment qui requièrent une analyse plus poussée (…).

Ces éléments semblent révéler que les établissements qui conservent la meilleure qualité d'analyse sont également ceux qui ont réussi à conserver une certaine maîtrise du flux, au travers d'une cartographie des risques fine et révisée périodiquement ainsi qu'à la mise en place de scénarios élaborés et pertinents ».

Combiner les approches inductives et déductives…

Pour outiller au mieux les opérationnels, le système de sécurité financière doit combiner les démarches déductives et inductives.

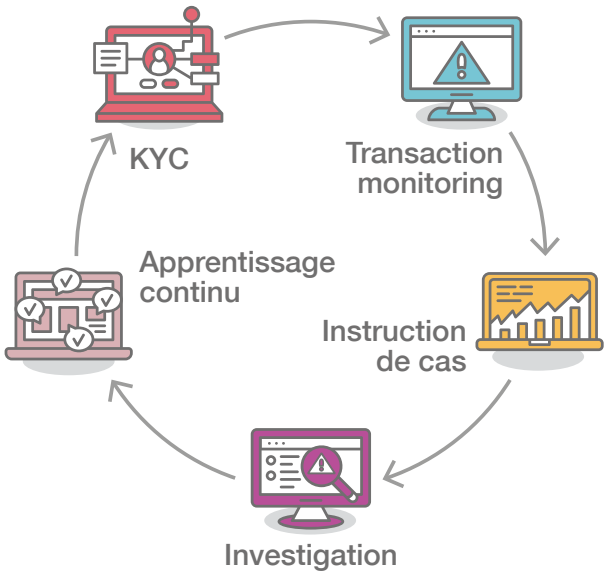


… pour respecter de nouvelles exigences

Les établissements doivent maîtriser les risques et les coûts ; ils formulent donc une double exigence : « faire plus » et « faire mieux » avec les ressources consacrées pour lutter contre les fraudes, le blanchiment et le financement du terrorisme.

« Faire plus signifie »

- Réduire le taux de faux positifs,
- Accélérer le traitement unitaire des alertes et le processus de prise de décision,
- Augmenter la capacité globale de traitement du dispositif,
- Concentrer les analyses sur les tâches à forte valeur ajoutée,
- Être capable d'identifier de nouvelles menaces (révéler les réseaux criminels…).



« Faire mieux signifie »

- Réduire le taux de faux négatifs,
- Croiser les données, structurées ou non, qu'elles soient internes ou externes,
- Identifier l'intégralité des « persons of interest », des points de compromissions…
- Considérer qu'une alerte, une réclamation, un contentieux (…) est une opportunité d'apprentissage,
- Permettre une réévaluation des risques (client, contrepartie…) à la volée,
- Enrichir et ajuster les contrôles continus (amélioration de la détection réalisée en amont), permanents et périodiques,
- Ne plus simplement détecter (a posteriori) mais prévenir (a priori).

Un nouveau dispositif efficace de sécurité financière doit s'articuler autour de cinq grandes capacité

1. KYC (Know Your Customer) : identification, connaissance et évaluation des risques des clients (et plus globalement des tiers) lors de l'entrée en relation et au fil de la relation (revues périodiques) ;

2. Transaction monitoring : détection d'anomalies dans les opérations grâce à la combinaison de techniques telles que le profilage dynamique fondé sur les opérations ou le filtrage des opérations sur la base de listes ;

3. Instruction de cas : organisation du traitement des anomalies (alertes issues du transaction monitoring ou de signalement humain) et des cas (regroupement d'alertes) ;

4. Investigation : examen approfondi des anomalies complexes et nouvelles afin de permettre une compréhension rapide des comportements et une identification claire des tenants et des aboutissants d'une anomalie ;

5. Apprentissage continu : limitation des faux-positifs et enrichissement de la surveillance grâce au traitement des faux-négatifs.

À ces capacités essentielles, il convient d'ajouter celles de pilotage et d'audit indispensables pour — respectivement — une gouvernance fine du dispositif et la mise en place de contrôles automatisés susceptibles d'alimenter le contrôle interne ou l'inspection (notamment lors des phases de préparation des missions).

Finalement, le nouveau système devra être :

- **Robuste** pour être progressivement interconnecté (vision 360°) et intégré dans les chaînes opérationnelles, référentielles et transactionnelles (fonctionnement en temps réel) pour prévenir les opérations risquées ;
- **Puissant** dans l'analyse pour être capable d'appréhender la complexité des nouveaux schémas ;
- **Simple** et **explicite** dans la restitution et la proposition d'action ;
- **Agile** et **évolutif**, aisément gérable par une petite équipe dédiée ;
- **Auditable** de bout en bout.

3. Proposition de démarche pour faire évoluer rapidement un système de sécurité financière

En quelques années, nous sommes passés de la surveillance des opérations, à la surveillance des comptes, puis à la surveillance des clients. La nature des schémas mis en place actuellement par les fraudeurs exige de franchir une nouvelle étape dans l'évolution : une surveillance multi-acteurs/une surveillance environnementale.

Les dispositifs de sécurité financière doivent cependant évoluer progressivement de manière à ne pas exposer l'établissement à des risques opérationnels induits par une transition très rapide.

Réorganiser l'alimentation de données

Les anciens dispositifs de sécurité financière (AML notamment) se contentaient d'opérations comptables. Il convient désormais de :

- **Exploiter toutes les sources des données disponibles**
  - **Internes :**
    - Obtenir des données atomiques (granularité la plus fine), les plus riches, issues des systèmes transactionnels (systèmes de paiements), opérationnels (gestion des mandataires…) et référentiels (KYC…),
    - Rapatrier l'intégralité des agrégats (statistiques, profils…) et des alertes issus des systèmes décisionnels en amont.

- **Externes :**
  - Réseaux sociaux,
  - Registres du commerce (sans négliger les historiques : anciens mandataires).

- **Extraire (et rendre explicite) les informations issues des différents flux de données**
  - L'IBAN de la contrepartie d'un virement indique le code banque, le code pays, le code agence…
- **Enrichir les données issues des référentiels et des systèmes transactionnels**
  - Dans le cas des virements internet, récupérer toutes les données techniques (IP, device fingerprint…).
- **Augmenter les données afin d'apprécier le risque de chaque type de flux**
  - Exploiter les données géographiques incluses dans les paiements pour positionner les flux sur une cartographie,
  - Évaluer le risque associé à chaque zone.
- **Rapprocher les différentes sources et constituer des historiques**
  - Reconstituer l'historique des agences en matière d'ouverture et de gestion d'un compte (ou d'une relation),
  - Etre capable de répondre à la question : « qui ont été les conseillers en charge de ce compte depuis son ouverture ? ».

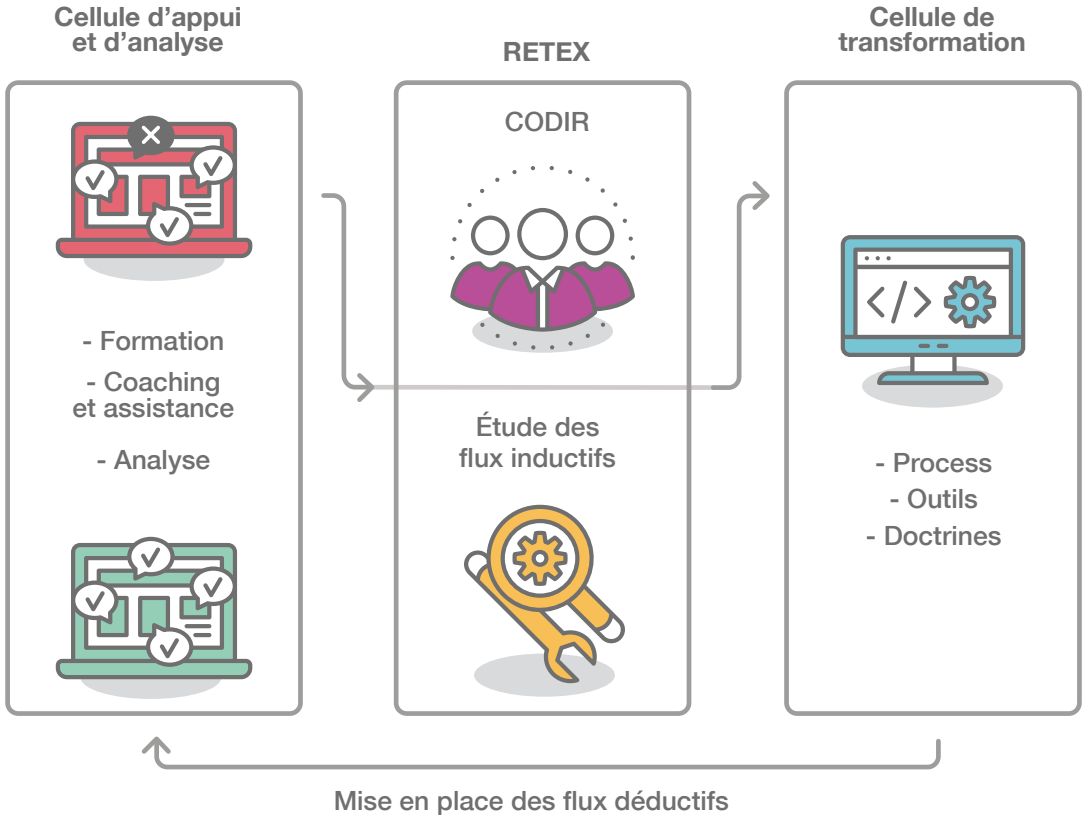
Repenser l'organisation projet pour améliorer la réactivité

Les banques doivent relever un double défi organisationnel : être réactives sur le court terme et capables de se transformer en profondeur sur le long terme. Ces deux ambitions sont complexes à concilier. Dans un univers où les mécaniques traditionnelles de surveillance sont souvent organisées en silo, avec des capacités de traitement des données limitées et des méthodes plus « artisanales » qu'industrielles, on imagine aisément qu'un projet de transformation qui voit le jour un an après avoir été conçu ne puisse plus répondre aux besoins immédiats des opérationnels.

« Pour être réactives sur le court terme et capables de se transformer sur le long terme, réformer les pratiques et les outils d'investigation est un excellent point de départ pour les banques »

Pour concilier ces deux objectifs, réformer les pratiques et les outils d'investigation est un excellent point de départ. Dans cette optique, les responsables de la conformité peuvent s'appuyer sur une organisation faisant appel à ses collaborateurs expérimentés sur le sujet de la fraude, à des analystes criminels, à des data-scientists et à des informaticiens.

Ces ressources seront réparties dans 3 cellules : une Cellule d'appui à l'analyse, une Cellule de transformation et une Cellule Retex (Retour d'Expérience) servant d'interface entre les deux précédentes entités.



Organisation tripartite de l'entité de lutte contre la fraude, le blanchiment et le financement du terrorisme

Prenons l'exemple concret d'un analyste ayant identifié dans des échanges d'emails un certain nombre de variables indices d'une activité criminelle. Sur la demande de la Cellule d'appui à l'analyse, le modèle est soumis au Retex. Il fait alors l'objet d'une évaluation d'intérêt, d'un examen juridique (dans quelle mesure et sous quelles conditions les emails peuvent-ils être analysés ?), puis d'une estimation technique (quelle solution, pour quel budget ?) avant d'être confié à la Cellule de transformation. Ce circuit décisionnel permet d'éviter la création de solutions sous-formatées ou sur-calibrées — propices à la génération de faux positifs ou de faux négatifs — qui constituent le principal indice de l'échec de la mission.

La Cellule d'appui à l'analyse est de nature opérationnelle. Son premier objectif est de former puis de coacher des équipes dédiées aux outils et aux méthodes d'analyse criminelle. Encadrée par des professionnels issus du monde de la police, de la justice, du renseignement, cette cellule passe des cas d'école à l'analyse concrète des données de l'entreprise. Son objectif est de développer l'expertise et la méthode des analystes afin de leur permettre d'identifier rapidement les modèles de blanchiment et de financement délictueux.

La Cellule de transformation travaille, en parallèle, sur l'outil, ses liens avec les systèmes internes et externes, mais aussi les process, les savoir-faire, les doctrines. Les experts de cette cellule sont familiers avec la méthode agile, connaissent la logique projet, les technologies, les systèmes d'informations bancaires en amont et comprennent parfaitement les enjeux et les problématiques métier.

Ces deux cellules ont leur vie propre, mais s'alimentent mutuellement via la **Cellule Retex** (retour d'expérience), chapeautée par un Codir (Comité de direction) Retex, qui réunit les professionnels des deux mondes, opérationnel et projet. Dans la pratique, après une première étape d'analyse du savoir-faire réalisée par la Cellule d'appui à l'analyse, la Cellule de transformation va produire une V1 de la nouvelle solution d'investigation en 8 semaines. Après 2 semaines de formation, la Cellule d'appui à l'analyse peut exploiter la V1 et effectuer des retours sur les difficultés d'usage ou sur les nouveaux schémas de blanchiment à implémenter. À la suite de quoi, la Cellule de transformation proposera une V2, etc. Ce système itératif et collaboratif, validé par l'entité Retex, permet d'obtenir des résultats immédiats.

L'organisation tripartite « Cellule d'appui à l'analyse/Retex/Cellule de transformation » tire son efficacité de la combinaison entre l'analyse criminelle, le design thinking et la méthode agile. C'est une organisation qui permet de répondre avec efficacité aux exigences de conformité dans un environnement de plus en plus complexe. Cette organisation ne se limite pas à améliorer dans l'urgence l'efficacité du dispositif existant, c'est une solution long terme qui garantit aux établissements financiers de pouvoir toujours être en mesure de contrer la capacité créative néfaste des organisations criminelles.

3. En conclusion

Afin de relever les défis de la sécurité financière, les établissements financiers doivent repenser leurs dispositifs en termes de processus, d'organisation, de compétences et d'outils.

Compte tenu de la complexité de ces projets, nous avons acquis la conviction qu'il est indispensable de capitaliser sur les compétences métier, informatique bancaire et technologique.

C'est pourquoi IBM propose un partenariat aux banques et aux assurances souhaitant se moderniser pour concevoir, développer et déployer un nouveau dispositif pérenne, évolutif et agile.

Nous tenons compte de votre outillage actuel et insufflons l'innovation technologique et organisationnelle pour assurer la protection de votre établissement, de vos collaborateurs et de vos clients à court, moyen et long terme.

Contacts

Vous souhaitez en savoir plus ? Contactez :

François Jaussaud
Associate Partner, Industry Solutions, IBM France
f.jaussaud@fr.ibm.com

Laurent Jaeger
Investment Banking Leader
IBM Global Services
laurent.jaeger@fr.ibm.com

Le contenu des pages 11 et 12 de ce document est paru dans *Les Échos* le 08 février 2018.