p. 4 ▶ Succès
GEODIS, le RGPD en mode express

p. 6 ▶ Conviction
Cybersécurité : comment construire la confiance dans un monde ultra-connecté ?

p. 8 ▶ Actualité
La feuille de route 2018 du Compliance Officer

p. 10 ▶ Rencontre
La compliance, un instrument éthique de prévention des risques

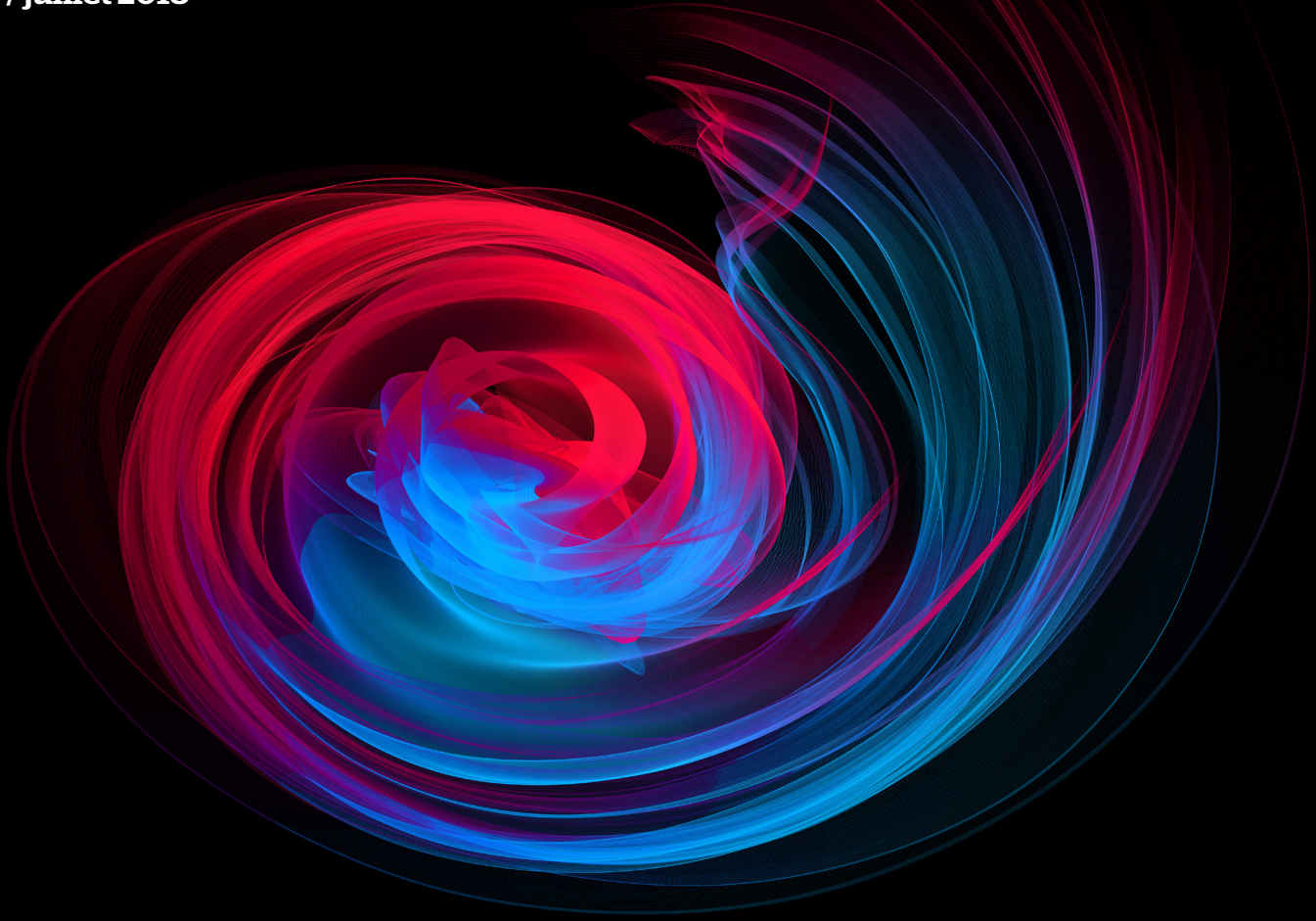
p. 12 ▶ Tendances
L'assurance face à ses propres risques

p. 14 ▶ Banque
De la crise systémique au système en crise

connexion

la newsletter d'Atos Consulting

#13 / juillet 2018



Risque, Conformité, Éthique

Savoir en faire une combinaison gagnante

Trusted partner for your **Digital Journey**

Atos Consulting

Atos Consulting, le cabinet de conseil en management du groupe Atos, est un acteur majeur de la transformation digitale du cœur de métier des entreprises et des organisations publiques.
Nos consultants accompagnent nos clients tout au long de la réalisation de leurs programmes et projets : de la définition de la stratégie jusqu'à la mise en œuvre des solutions.

Nos expertises
En plus d'une connaissance approfondie des marchés sur lesquels nous intervenons, nous nous appuyons sur des lignes d'expertises transverses, des centres d'excellence européens et des communautés de capitalisation des savoirs au sein du réseau global Atos Consulting. Ces lignes d'expertises et nos centres d'excellence permettent à nos clients de bénéficier de méthodologies éprouvées, d'échanges d'expériences et d'une vision internationale sur leurs préoccupations majeures.

Un regard différent
Chez Atos Consulting, nous contribuons à la réussite de nos clients en les aidant à prendre une longueur d'avance. Nous les accompagnons dans la construction du socle d'excellence opérationnelle. Nous faisons avec eux de la technologie et du digital une force d'innovation et de rupture, moteur de leur performance durable.

Nous contacter

Banque et Assurance
▸ **Jacques de Parcevaux**
jacques.deparcevaux@atos.net

Secteur Public
▸ **Emmanuel Arpino**
emmanuel.arpino@atos.net

Télécommunications, Media & Utilities
▸ **Cédric Porco**
cedric.porco@atos.net

Manufacturing, Retail, Services & Transport
▸ **Guillaume George**
guillaume.george@atos.net

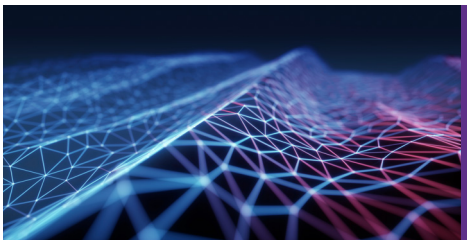
Régions
▸ **Guillaume George**
guillaume.george@atos.net

Sommaire

4 Succès
GEODIS, le RGPD en mode express

6 Conviction
Cybersécurité : comment construire la confiance dans un monde ultra-connecté ?

8 Actualité
La feuille de route 2018 du Compliance Officer



10 Rencontre
La compliance, un instrument éthique de prévention des risques

12 Tendances
L'assurance face à ses propres risques

14 Banque
De la crise systémique au système en crise

À propos d'Atos

Atos est un leader international de la transformation digitale avec environ 100 000 collaborateurs dans 73 pays et un chiffre d'affaires annuel de l'ordre de 12 milliards d'euros. Numéro un européen du Big Data, de la Cybersécurité, des supercalculateurs et de l'environnement de travail connecté, le Groupe fournit des services Cloud, solutions d'infrastructure et gestion de données, applications et plateformes métiers, ainsi que des services transactionnels par l'intermédiaire de Worldline, le leader européen des services de paiement. Grâce à ses technologies de pointe et son expertise digitale & sectorielle, Atos accompagne la transformation digitale de ses clients dans les secteurs Défense, Finance, Santé, Industrie, Médias, Énergie & Utilities, Secteur Public, Distribution, Télécoms, et Transports. Partenaire informatique mondial des Jeux Olympiques et Paralympiques, le Groupe exerce ses activités sous les marques Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify et Worldline. Atos SE (Societas Europea) est une entreprise cotée sur Euronext Paris et fait partie de l'indice CAC 40.

Edito

Oser faire de la gestion des risques un motif de confiance

Antoine Beullier,
Associate Partner, Atos Consulting, France

La gestion du risque vise à réduire la probabilité de survenance et l'impact d'un évènement pouvant compromettre l'atteinte des objectifs d'une organisation. La méthode consiste à recenser et analyser ces scenarii et à définir collectivement les mesures pour maîtriser le risque. Cet « examen de conscience », quand il est relayé au plus haut niveau de l'entreprise et déployé de manière opérationnelle, se révèle un levier majeur d'optimisation.

Les lignes de défense existent depuis longtemps mais nous assistons à une convergence progressive des domaines d'intervention pour assurer leur plus grande efficacité et la prise en compte des obligations tant réglementaires qu'imposées par les investisseurs, partenaires et clients. Le développement de ces filière permet de saisir de nouvelles opportunités pour les organisations.

Nous tenons particulièrement à remercier Marc Lotito, Directeur de la transformation de la fonction finance chez GEODIS, pour son témoignage sur la manière pragmatique dont il a conduit le projet de mise en conformité au Règlement général sur la protection des données personnelles. En effet, les entreprises qui ne pourront pas prouver leur sérieux seront exclues des écosystèmes digitaux. Elles se verront ainsi distancées par celles qui, au contraire, auront accès aux données et sauront les gérer.

Dans un monde piloté par les données, où les services sont numériques et interconnectés, la cybersécurité est désormais un prérequis pour la résilience d'une organisation. Si le besoin immédiat est la protection des personnes et des biens, l'intégration de la sécurité dès la phase de conception devient un facteur essentiel de réussite pour tout nouveau projet digital.

L'inflation réglementaire, fortement perceptible depuis une décennie et consécutive notamment à la crise financière mondiale de 2008, se télescope à la fois avec un changement profond du comportement et des attentes des consommateurs, et avec une numérisation à marche rapide de tous les secteurs d'activité. Jean-Baptiste Siproudhis, Global Head of Compliance d'Atos, positionne ainsi la conformité comme un instrument éthique de prévention des risques.

Les directeurs de la prévention des risques et de la conformité sortent de l'ombre et gagnent les avant-postes de la réflexion stratégique et de son exécution. La banque et l'assurance ont depuis longtemps l'habitude de composer avec cet univers réglementaire et de risques financiers ou de sinistres. Leurs environnements changent eux-aussi, les obligeant à tirer les leçons de la crise de 2008 pour les unes et à trouver les solutions de couverture des risques émergents pour les autres. Ces deux professions sont également mises à l'honneur dans ce numéro de Connexion.

Nous vous en souhaitons une très bonne lecture, en espérant vous apporter quelques points de repère dans notre monde de risques.

«La gestion des risques était préventive, elle est aujourd'hui un levier de conquête pour les entreprises.»

GEODIS, le RGPD en mode express

Comme beaucoup d'entreprises, GEODIS a dû s'adapter dans des délais très courts pour répondre aux exigences du RGPD. Mais grâce à une approche rigoureuse et pragmatique, le logisticien a pu mettre en place dans les temps les principaux éléments techniques et organisationnels de la conformité. Rencontre avec Marc Lotito, Directeur de la transformation de la fonction finance, en charge du projet RGPD chez GEODIS.

Comment le sujet du RGPD a-t-il été abordé chez GEODIS ?

C'est Henri Linière, notre Directeur des Systèmes d'information Groupe, qui, le premier, a porté le sujet devant le comité exécutif. En septembre 2017, la direction de l'entreprise a pris la mesure de l'enjeu, et les préparatifs ont débuté aussitôt, soit huit mois à peine avant l'échéance. Pour éviter que le projet RGPD ne se réduise à sa dimension technique, la DSI estimait préférable de ne pas le prendre dans son giron, et le premier choix fort a été de le confier à la fonction finance, entité à la fois transverse et sensible à la question de la qualité des données. Comme la plupart des entreprises, nous avions peu de compétences sur un sujet aussi neuf et complexe que le RGPD et guère le temps de les développer en interne. Un accompagnement était donc nécessaire, et nous avons retenu Atos Consulting, qui nous donnait des gages de sécurité et de rapidité. Atos Consulting avait notamment analysé en profondeur les impacts de la réglementation pour une entreprise internationale telle que la nôtre tout en apportant au sujet une vision très concrète, étayée par ses expériences antérieures et une connaissance de première main des solutions techniques.

Quelle a été la première phase du projet ?

La première étape consistait à assimiler la réglementation, et surtout ses conséquences pour notre activité. Pour cela, nous avons organisé une série d'ateliers combinant une lecture approfondie des textes, préparée par notre direction juridique, et une réflexion sur les risques que nous encourions. Dans notre activité de livraison, nous manipulons beaucoup de données personnelles, comme les adresses et les numéros de téléphone. En outre, nous opérons pour de grands groupes, notamment d'e-commerce, qui se doivent d'être irréprochables en la matière car leur réputation est en jeu. Pour nous, le principal risque est donc commercial : il nous faut pouvoir démontrer notre conformité à nos clients qui en font un critère de plus en plus important dans leurs appels d'offres. Fin janvier, en consolidant les travaux des différents ateliers, nous avons abouti à un plan d'action en deux temps : une première série d'actions prioritaires, à réaliser avant l'échéance du 25 mai, puis une seconde vague de chantiers, échelonnés jusqu'à la fin de l'année 2018.

Comment avez-vous mis en œuvre ces actions prioritaires ?

Le peu de temps dont nous disposions nous a incités à être pragmatiques. Notre ligne directrice était de constituer une boîte contenant des outils adaptés, efficaces et simples à déployer, comme les supports de communication et de formation par exemple. Atos Consulting nous y a grandement aidés, que ce soit pour définir les processus, rédiger les politiques ou développer le module d'e-learning. De cette façon, l'essentiel était prêt le 25 mai : nous avions défini nos politiques, nous disposions d'une première version du référentiel des traitements, et notre DPO (Data Protection Officer) et son organisation

étaient en place. Sur ce point, Atos Consulting nous avait avertis des différentes options possibles, et nous avons opté pour un DPO Groupe entouré de correspondants plutôt que pour un DPO par pays. C'est pour nous le moyen le plus sûr de maîtriser les processus et la communication en cas d'incident, réel ou supposé. Nous opérons dans 120 pays, mais notre présence y est souvent trop limitée pour assumer localement un risque pesant sur le groupe dans son ensemble. À ce jour, nous sommes conformes sur la plupart des points du RGPD. Reste à déployer le dispositif dans l'ensemble de notre organisation et à mettre en œuvre un certain nombre de dispositifs techniques qui renforceront la sécurité et la confidentialité des données. C'est le programme des mois à venir.

Quel bilan tirez-vous de ce projet ?

Comme lors du passage à l'euro ou à l'an 2000, beaucoup prédisaient un séisme insurmontable. Jusqu'à présent, cela n'a pas été le cas et nous sommes assez optimistes pour la suite. Notre approche rigoureuse et pragmatique nous a permis de tenir notre feuille de route. Nous sommes également très satisfaits de notre collaboration avec Atos Consulting, qui nous a apporté la pertinence de ses analyses, sa rigueur méthodologique, et une somme des connaissances, d'expérience et de benchmarks qui nous a permis de faire les bons choix. Nous avons ainsi découvert des outils que nous ne soupçonnions pas, par exemple pour automatiser la mise à jour du registre des traitements. Le bilan est donc très positif. Seul bémol, comme beaucoup sans doute, nous avons sous-estimé l'emballement que tout le monde a pu constater au cours des dernières semaines. Tout à coup, les demandes de clients ont afflué, et la diversité des formats et des exigences ne permettait pas d'automatiser ou de standardiser nos réponses. Cela a représenté une soudaine et importante charge de travail, à laquelle s'ajoutait le traitement de la démarche similaire que nous avons nous-mêmes engagée auprès de nos fournisseurs.

En avez-vous déjà tiré des bénéfices ?

Bien que l'objectif à long terme du RGPD soit de bâtir le cadre de confiance nécessaire au développement du digital, à court terme, cela reste une réglementation à appliquer, avec les coûts que cela suppose et peu de bénéfices directs. Toutefois, on peut considérer le référentiel des traitements comme un acquis qui nous sera très utile à l'avenir, par exemple dans le cadre des projets d'infrastructure IT. Et pour la fonction finance, c'est une expérience précieuse aussi bien au plan individuel que collectif. Cela nous a permis d'approfondir notre expertise en matière de gestion des données, d'élargir notre éventail d'interlocuteurs et de démontrer notre capacité à mener de grands projets. Rétrospectivement, le RGPD constituera certainement pour toute l'entreprise un cap culturel dans la façon d'appréhender les données.

Filiale du Groupe SNCF, GEODIS est l'un des principaux opérateurs de la chaîne logistique en Europe et dans le monde. GEODIS est notamment le leader du transport et de la logistique en France, et se place au quatrième rang européen. Fort de 40 500 collaborateurs, GEODIS est directement présent dans 67 pays et rayonne dans plus de 120 pays. En 2017, GEODIS a réalisé un chiffre d'affaires de 8,1 milliards d'euros.

Pour plus d'information, contacter >>
celia.allouche@atos.net

Cybersécurité : comment construire la confiance dans un monde ultra-connecté ?

Technologies portables (wearables), voitures autonomes, réalité augmentée... le futur sera résolument connecté. Mais, aussi fascinantes soient-elles, ces technologies n'en sont pas moins vulnérables et porteuses de nouvelles menaces. Pour que se réalisent les promesses des systèmes intelligents, il convient de juguler ces risques émergents. Pour cela, la cybersécurité doit tout à la fois prendre de la hauteur et descendre au cœur même des projets digitaux.

L'actualité le démontre désormais tous les jours : pour les entreprises et les organisations publiques, le cyber-risque n'est plus une question de « si », mais de « quand », de « comment » et de « combien ». Et à mesure que se développent et se généralisent les nouvelle technologies connectées, ces trois interrogations deviennent de plus en plus brûlantes.

Les risques : malveillance, défiance, expérience

Le cyber-risque évoque aussitôt les attaques de pirates, qui sont de plus en plus organisés et ingénieux. Leurs objectifs : causer des dommages, déstabiliser leur cible ou encore dérober des données sensibles, comme de la propriété intellectuelle ou des données à caractère personnel.

Bien que la malveillance (souvent favorisée par la négligence) reste la première des menaces, l'entreprise doit aussi prendre garde à ne pas rompre elle-même le contrat de confiance implicite qui sous-tend chaque service numérique. En collectant trop de données, en les exploitant de manière opaque, en les monétisant à l'insu de ses utilisateurs ou en leur forçant la main, elle court en effet le risque d'engendrer une défiance qui, très vite, mène à la désaffection et aux pertes de revenus.

Les facteurs aggravants : volume, variété, valeur, vitesse

Pour paraphraser les fameux 4V caractérisant le Big Data (volume, variété, vélocité, véracité), on peut considérer que quatre facteurs, 4V, contribuent à complexifier l'équation sécuritaire dans le monde connecté.

Premier de ces facteurs, le volume renvoie naturellement à l'essor exponentiel de la sphère digitale : des milliards d'objets, des millions d'utilisateurs, des centaines de milliers de transactions à chaque instant... Non seulement les périmètres à sécuriser, surveiller et contrôler sont immenses, ce qui rend d'autant plus facile à un intrus d'y passer inaperçu, mais de tels volumes soumettent les systèmes à une pression terrible. Par exemple, la consommation de bande passante des objets connectés mettra à rude épreuve les autres communications sans fil, qui fonctionnent également sur les fréquences mégahertz comme la radio, la télévision, les services d'urgence, etc. En outre, l'effet de réseau s'en trouve démultiplié, et avec lui l'ampleur des risques et la vitesse de leur propagation. Qu'il s'agisse d'un smartphone ou d'une cafetière, le moindre périphérique vulnérable peut devenir l'épicentre ou le relai involontaire d'une infection foudroyante.

La variété des objets constitue d'ailleurs elle-même un deuxième facteur aggravant. Que ce soit dans l'entreprise, avec le BYOD (Bring Your Own Device) notamment, ou au-delà, la diversité des plateformes matérielles, des systèmes d'exploitation, des versions logicielles et des fournisseurs rendent de plus en plus complexes la conception et le déploiement des solutions de sécurité. Il reste inévitablement des failles, dans lesquelles ne manquent pas de s'engouffrer les pirates.

Et s'ils le font si volontiers, c'est en raison du prix croissant de ce qu'ils peuvent récolter ou détruire. La valeur, troisième facteur d'amplification des risques, va de pair avec l'essor du digital. Plus la technologie est intégrée aux actions quotidiennes, plus elle apporte d'intelligence, et plus les systèmes renferment des données précieuses : coordonnées bancaires, données de santé, fichiers clients, propriété intellectuelle... Informations qui aiguisent les appétits et critiques pour l'organisation.

Enfin, la vitesse des changements constitue le dernier, mais non le moindre, des facteurs qui compliquent la tâche des entreprises en matière de cybersécurité. Qu'il s'agisse de technologie, d'usages, de réglementation, d'exigences

sociétales ou des cycles de l'activité, le rythme s'est considérablement accéléré au cours des dernières années. Et pour les équipes chargées de la cybersécurité, ce tempo effréné devient de plus en plus difficile à suivre.

Une cybersécurité qui prend de la hauteur...

Dans ce contexte de risques à la fois plus variés, plus sérieux et plus difficiles à contrer, les approches traditionnelles de la cybersécurité montrent leurs limites. Au château-fort (un périmètre ceint de murailles supposées infranchissables) et à l'armure (barder les points vulnérables de protections) doivent succéder de nouveaux paradigmes fondés en priorité sur l'analyse de risques.

Bien que d'incitation réglementaire, les projets RGPD constituent à cet égard un exemple et un précédent intéressants. Focalisés sur une catégorie de risques (ceux associés aux données à caractère personnel), ils ont bénéficié d'une approche globale et systémique, qui a nécessité la réalisation préalable d'un état des lieux, puis la constitution d'un référentiel et la mise en place d'une organisation et d'une gouvernance appropriées. Ces dispositifs, auxquels ont été ensuite subordonnés le choix et la mise en œuvre des divers outils de protection (chiffrement, gestion des identités et des accès, prévention des fuites de données...), offrent la garantie d'une cybersécurité pérenne et proportionnée, capable de s'adapter à un environnement en évolution perpétuelle.

... et s'invite au cœur des projets digitaux

Cette expérience du RGPD, comme les approches que mettent d'ores et déjà en œuvre les entreprises et les secteurs les plus sensibles, révèle le tournant fondamental pris aujourd'hui par la cybersécurité. Pour répondre efficacement aux risques actuels et futurs : dorénavant, on s'attache moins à sécuriser des composants techniques (une base de données, un réseau...) que des objets métiers (une transaction, un dossier client...). Offrir une sécurité intrinsèque, adaptée à leur niveau de criticité et à leur exposition à chacun de ces objets devient une caractéristique de base, voire un prérequis. La cybersécurité s'articule donc entre une approche « macro » du risque, envisagée au plus haut niveau de l'entreprise, et une approche « micro », orientée métier et déclinée au sein des projets.

Dès lors, se pose la question de la mise en œuvre de cette cybersécurité « by design » qui rompt avec les pratiques traditionnelles en intégrant de la sécurité dès la phase de conception, surtout dans les délais réduits des projets digitaux. Comment garantir la sécurité d'une application développée en quelques semaines et la pérenniser au fil de ses évolutions ? Comment maintenir la confiance tout au long de son cycle de vie ? Des approches méthodologiques et des technologies éprouvées permettent d'intégrer les enjeux de sécurité au développement des projets avec, par exemple, la protection des données ou la gestion d'identité numérique.

Atos et ses 5 000 experts cybersécurité ont notamment développé et mis en pratique chez plusieurs de leurs clients une démarche permettant de sécuriser les projets. Cette démarche tient en quatre points clés :

1. Se préparer et gérer ses priorités : il faut tout d'abord identifier les risques et les menaces associés aux éléments métiers du projet, puis en évaluer la criticité de manière à prioriser les mesures à mettre en œuvre.

2. Mettre en place une organisation efficace : les rôles et les responsabilités sont clairement attribués en matière de sécurité au sein de l'équipe, ainsi que la fréquence et le périmètre d'intervention des experts sécurité.

3. Réaliser les tests et contrôles au fil de l'eau : la sécurité n'est plus traitée séparément, en toute fin de projet, mais intégrée aux développements et testée au rythme du projet, autant que possible à l'aide d'un framework de développement dédié.

4. Avoir une vision élargie de la sécurité : le cadre technologique et métier dans lequel s'inscrit le projet, ainsi que les ressources techniques ou humaines extérieures mises à contribution, doivent être plus vastes, pour assurer une sécurité de bout en bout.

Pragmatique et très opérationnelle, cette démarche permet en outre à l'entreprise de s'acculturer, de s'outiller et de monter en compétences de manière progressive. Essentielle à la confiance, la cybersécurité devient de plus en plus une condition nécessaire à toute activité. Pour l'entreprise, développer dès aujourd'hui les bons réflexes en la matière, c'est prendre une option décisive sur sa réussite dans le monde hyper-connecté de demain qui ne tiendra toutes ses promesses qu'avec une sécurité « by design » et de bout en bout reposant sur la sécurisation des projets et des objets ainsi que de leur fonctionnement.

Pour plus d'information, contacter >>
laurent.sauphanor@atos.net
jeremy.renard@atos.net

La feuille de route 2018 du Compliance Officer

Chargé en premier lieu de s'assurer que l'entreprise respecte les règles édictées par les autorités, le Compliance Officer ne manque pas de chantiers à l'heure où de nombreux textes majeurs entrent en vigueur, notamment la loi Sapin 2 et le RGPD.

Dans un environnement international de plus en plus instable juridiquement, le Compliance Officer est un acteur prépondérant de la gestion des risques. En 2018, sur sa liste de priorités, figure la mise en conformité avec plusieurs textes importants, susceptibles d'impacter fortement l'entreprise.

La loi Sapin 2

Adoptée le 8 novembre 2016, la loi Sapin 2 relative à la transparence, la lutte contre la corruption et la modernisation de la vie économique entre progressivement en vigueur depuis le 1er juin 2017. L'un de ses principaux volets, qui s'applique aux sociétés ou groupes français d'au moins cinq cents salariés et 100 millions d'euros de chiffre d'affaires, est de mettre en place huit mesures principales afin de prévenir et détecter des faits de corruption ou de trafic d'influence, que ce soit en France ou à l'étranger. Ce sont :

- un code de conduite,
- un dispositif d'alerte,
- une cartographie des risques,
- des procédures d'évaluation des clients, des fournisseurs de premier rang et des intermédiaires,
- des procédures de contrôle comptable,
- un dispositif de formation du personnel,
- un régime disciplinaire,
- un dispositif de pilotage, de contrôle et d'évaluation interne.

La loi relative au devoir de vigilance

Promulguée le 21 février 2017, soit quatre ans après l'accident du Rana Plaza*, la loi sur le devoir de vigilance impose aux entreprises de mettre en place un plan de vigilance permettant d'identifier les risques et de prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes, et l'environnement. Le plan de vigilance concerne l'entreprise et ses filiales (sous contrôle), mais aussi ses sous-traitants et ses fournisseurs. Il comprend une cartographie des risques, des processus d'évaluation des partenaires (due diligence), des mesures de réduction des risques, un mécanisme d'alerte, et un dispositif de suivi.

En application des lois Sapin 2 et sur le devoir de vigilance, Atos a renforcé son dispositif de prévention de la corruption et des atteintes aux droits de l'homme en établissant des partenariats d'intégrité qui prévoient une coopération accrue en matière de veille, d'alerte et d'investigations internes.

Le RGPD

Le règlement général sur la protection des données personnelles (RGDP ou GDPR en anglais) est entré en vigueur le 25 mai 2018 mais la mise en œuvre des mesures nécessaires occupera sans doute les entreprises durant encore plusieurs mois. Indépendamment de la nationalité de l'entreprise, elle s'applique dès lors que celle-ci manipule des données à caractère personnel de citoyens européens, qu'il s'agisse de collaborateurs, de clients ou de partenaires. Ses principaux objectifs sont de garantir le respect du droit à la vie privée, d'encadrer le transfert et l'exploitation des données personnelles, et d'en prévenir la violation.

Le projet de mise en conformité avec le RGPD s'organise en quatre étapes :

1. **La définition** du périmètre d'application du texte au sein de l'organisation, l'identification des acteurs clés et un diagnostic des pratiques existantes (collecte, stockage, traitement...) ;
2. **La réalisation** d'une analyse des risques juridiques et d'une analyse de conformité ;
3. **La définition** d'un plan d'action, hiérarchisant et ordonnançant les chantiers à mener ;
4. **La mise** en œuvre progressive des divers chantiers et actions à réaliser.

Afin de faciliter la conduite du changement au niveau international, Atos Consulting a développé un module d'e-learning RGPD multi-langues permettant de sensibiliser et former le personnel de l'entreprise.

Bâle 3 et MIF 2

Enfin, dans la banque et l'assurance, le Compliance Officer a d'autres sujets de préoccupation avec l'entrée en vigueur progressive des accords de Bâle 3, qui harmonisent les règles de solvabilité et de contrôle prudentiel au niveau mondial, et de la directive MIF 2, qui encadre les marchés et les services, et renforce notamment la protection des investisseurs.

Dans son action, le Compliance Officer s'appuie largement sur l'IT, si bien qu'apparaît de plus en plus souvent la fonction de Compliance Officer IT. Son rôle est de suivre les contraintes règlementaires pour s'assurer qu'elles sont convenablement implémentées dans les applications. Il coopère également avec le responsable de la sécurité des systèmes d'information pour s'assurer du respect des exigences de sécurité. Il s'appuie, bien souvent, sur des spécialistes extérieurs qui l'assistent dans sa mission de cadrage réglementaire : évaluation des risques de non-conformité, gestion des identités et des accès, prise en compte et mise en œuvre des exigences de sécurité, documentation du parc applicatif...

Pour plus d'information, contacter >>
dorothee.golliet@atos.net

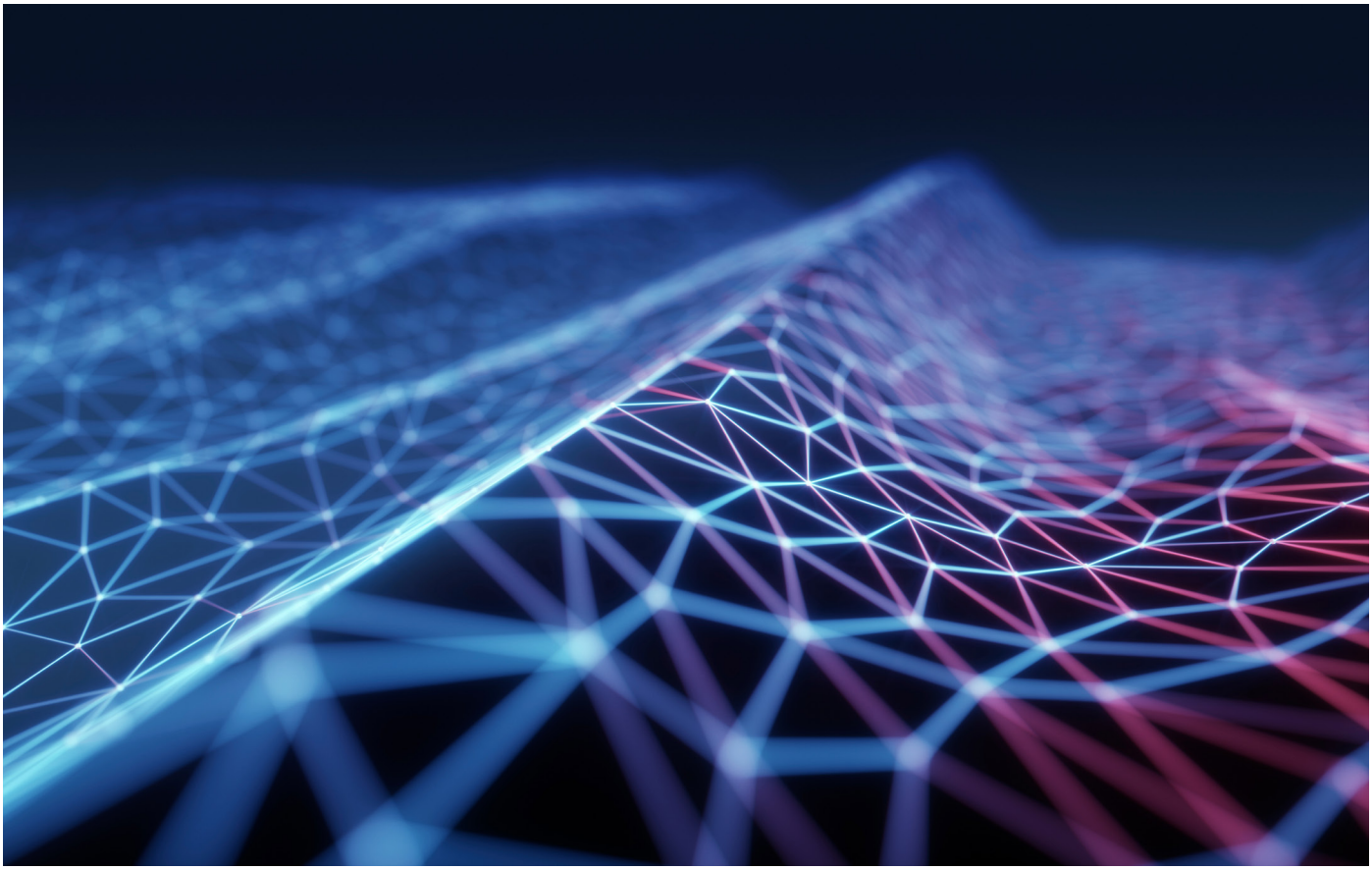
* L'effondrement, le 24 avril 2013, du bâtiment Rana Plaza, près de Dacca au Bangladesh, a fait plus de 1 100 morts et se classe parmi les catastrophes les plus meurtrières de l'histoire du travail.

La compliance, un instrument éthique de prévention des risques

Dans un monde d'incertitudes, la compliance vise à développer les pratiques responsables qui constituent le meilleur rempart contre des crises aux effets dévastateurs. **Jean-Baptiste Siproudhis**, Global Head of Compliance d'Atos, détaille cette approche en plein essor qui, au-delà de la conformité aux textes, touche à la culture même de l'entreprise.

Longtemps réservée aux secteurs les plus réglementés, comme la banque ou l'assurance, la compliance est devenue une préoccupation largement partagée. Comment l'expliquez-vous ?

Presque chaque jour, je vois des entreprises lourdement sanctionnées pour avoir enfreint des règles – parfois tacites – de bonne conduite. Elles paient cher pour apprendre que les temps ont changé. Ce qui était secret ne le reste pas, ce qui était toléré l'est de moins en moins, et respecter le droit ne suffit plus. Cette évolution, qui remonte notamment à la crise de 2008, s'est considérablement accélérée ces dernières années. Aujourd'hui, les autorités de contrôles, les ONG et les médias ont une volonté et des capacités d'investigation sans précédent à travers le monde, et l'opinion publique se montre un juge parfois autant intransigeant qu'une juridiction. En outre, personne ne souhaitant être incriminé par association, les parties prenantes sont de plus en plus regardantes sur l'intégrité des entreprises, à l'image des investisseurs qui se détournent de certains secteurs ou des donneurs d'ordre qui renforcent leurs cahiers des charges. Dans cet environnement, où l'instabilité juridique et géopolitique va de pair avec des sanctions accrues, une entreprise rattrapée par une affaire court trois principaux risques : un risque de sanctions financières, un risque d'accès aux marchés, en raison des boycotts et embargos éventuels par les pays comme par les clients, et un risque de dégradation durable de son image et de son crédit. C'est pour les prévenir qu'est apparue la compliance, une nouvelle fonction à mi-chemin entre la gestion des risques traditionnelle et la conformité réglementaire. La compliance a pour mission d'inculquer aux employés des pratiques business plus respectueuses des règles et de la déontologie. Quoique principalement défensif, son rôle est aussi offensif, car conduire ses affaires de manière intègre et responsable est aujourd'hui un puissant facteur de confiance et d'attractivité pour les investisseurs, les clients et les (futurs) collaborateurs.



Sur un tel sujet, l'écueil n'est-il pas d'en rester aux discours et aux bonnes intentions ?

En effet. Il faut pouvoir démontrer que nous sommes «compliant» et ne pas seulement l'affirmer. En cas de mise en cause de l'entreprise, avoir des difficultés à apporter les preuves de ses efforts préventifs est devenu un facteur aggravant. Pour dépasser l'affichage, il faut donc se doter, derrière un Chief Compliance Officer (CCO), d'une organisation capable de déployer, documenter et évaluer l'efficacité de ses actions préventives. À partir d'un environnement très complexe, où se mêlent droit, géopolitique, culture et technologie, l'objectif est d'extraire quelques règles simples et de bons réflexes à diffuser dans toute l'organisation. La première étape consiste donc à identifier les thématiques sur lesquelles se concentrent les principaux risques. Où encourons-nous les sanctions les plus lourdes ? Quels sont les sujets les plus sensibles en matière de réputation ? Chez Atos, nous avons dénombré sept sujets clés de compliance : la corruption, la protection des données, le droit du commerce international (sanctions internationales et exportation des biens à double usage), la concurrence, le blanchiment d'argent et le financement du terrorisme, le respect des droits humains, et enfin le harcèlement et la discrimination au travail.

Concrètement, comment mettez-vous en œuvre la compliance ?

Mettre en œuvre la compliance passe par de la formation, de la sensibilisation, la mise en place de processus de contrôle, de vérification et d'alerte, des appels à la vigilance... L'objectif est de faire naître de bons réflexes : faire preuve de discrétion en public, de discernement dans les relations, ne pas hésiter à rapporter des comportements inappropriés. Surtout, les règles doivent être simples, compréhensibles, applicables et diffusées dans des formats appropriés. Nous privilégions, par exemple, les courtes vidéos pédagogiques aux documents trop longs à lire et nous puisons dans l'actualité des exemples à la fois frappants et riches d'enseignements. Il faut surtout éviter d'accabler les collaborateurs de nouvelles contraintes, sans quoi la démarche restera lettre morte. Lorsque j'ai pris mes fonctions, nous avions, pour couvrir ces sujets, une quinzaine de politiques dont le détail occupait plus de 150 pages de règles. Aujourd'hui, il n'y en a plus qu'une, qui tient en moins de 15 pages. Au-delà des règles, il faut donc parvenir à infuser les opérations et les processus au quotidien pour que chacun comprenne et s'approprie la compliance. Il faut aussi donner l'assurance que l'organisation intervient à l'appui du Groupe mais aussi, et surtout, de l'ensemble de ses salariés. Aujourd'hui, tout change très vite, au point qu'à l'exception notable du RGPD, les textes sont souvent en retard sur les usages. C'est pourquoi il faut parfois davantage chercher à inculquer l'esprit que la lettre. En somme, la compliance consiste à développer une éthique par la pratique.

La compliance relève donc d'un changement culturel à l'échelle de l'entreprise...

Tout à fait, et c'est pourquoi l'impulsion et l'exemple doivent venir du sommet. La compliance est portée par le CEO et par le comex, et ce sont les cadres dirigeants qui la déploient au sein de leur organisation, métier ou géographie. Tout en respectant un certain nombre d'exigences minimales, les lignes directrices globales ont vocation à être adaptées à la culture, aux pratiques et aux risques propres à chaque entité. Par exemple, dans certains pays, accepter le moindre cadeau est déjà assimilé à une forme de corruption alors que dans d'autres, on froisserait gravement son interlocuteur en le refusant. Rattaché au Chief Compliance Officer (CCO), un réseau de compliance officers aide les top managers à adapter et mettre en place les dispositifs au niveau local. Par la diversité de leurs profils et leur proximité avec le terrain, ils nourrissent aussi le travail de veille permanent du CCO. Pour l'entreprise, la compliance est une ligne directrice, mais c'est une ligne souple. Il faut constamment l'adapter à la réglementation, à la société, aux orientations de l'entreprise et aux collaborateurs pour que les règles se fondent le plus naturellement possible dans les pratiques quotidiennes.

Pour plus d'information, contacter >>
jean-baptiste.siproudhis@atos.net

L'assurance face à ses propres risques

Professionnels des risques s'il en est, les assureurs ont clairement identifié pour eux-mêmes deux menaces majeures : manquer le virage des nouvelles technologies et ne pas répondre aux besoins émergents de leurs clients. Sous la pression, l'heure est à la réinvention.

Pour les assureurs, courtiers, mutuelles et autres Institutions de Prévoyance, le temps est loin où la pression concurrentielle était relativement faible et les clients plutôt captifs. Désormais, les menaces fusent de toutes parts. D'un côté, se multiplient les assurtechs avec leurs modèles disruptifs comme l'assurance à l'usage, la souscription 100 % en ligne pour les risques professionnels ou les robots comparateurs qui ont d'ores et déjà transformé le marché de l'assurance des particuliers. De l'autre, le péril vient d'un fort mouvement de concentration et d'une course à la taille qui touche tous les acteurs, que ce soient les assureurs globaux (rachat du groupe XL Catlin par AXA) ou les mutualistes et autres Institutions de Prévoyance. Le secteur est fragilisé par des taux d'intérêt chroniquement bas qui obligent à une rigidité tarifaire quand bien même le marché est en surcapacité. Enfin, il voit déferler la vague du big data, qui promet beaucoup à ceux qui sauront tirer parti de l'immense gisement de données. Mais à condition que les GAFA ne l'exploitent pas les premiers en se lançant dans l'assurance.

Digitalisation à marche forcée

L'irruption du numérique et la rapidité de son adoption par les consommateurs bouleversent la relation client, obligeant les assureurs à une profonde refonte de leurs processus et de leurs organisations. Au contraire des «pure players» digitaux, qui peuvent concevoir leurs plateformes de services à partir d'une feuille blanche, les assureurs « historiques » doivent composer avec l'existant. Ils ne peuvent faire abstraction ni du poids de leurs organisations, ni de la complexité de leurs systèmes hétérogènes, lesquels compliquent la mise en place des technologies agiles nécessaires à la centralisation de leurs données clients.

Selon une étude réalisée en juillet 2017 par l'éditeur Liferay, seuls 49 % des assureurs français affirmaient disposer d'une vision globale de leurs clients (liste des contrats, préférences, dernières interactions...). Et, tandis que 25 % reconnaissaient débuter tout juste leur transformation digitale, 3 % à peine estimaient avoir achevé la leur. Outre la satisfaction client, la digitalisation des services est perçue par deux assureurs sur trois comme la principale source de réduction des coûts grâce notamment aux self-services digitaux (portails clients et chatbots permettant de payer ses primes, d'obtenir une attestation, une pré-autorisation médicale, une synthèse de ses polices, etc.).

IA et blockchain, ruptures annoncées

Mais, pour les assureurs, la révolution technologique ne s'arrête pas au digital. En back-office, le développement de l'intelligence artificielle ouvre en effet d'immenses perspectives en matière de robotisation et d'automatisation des processus (RPA) pour le traitement administratif d'importants volumes de données : premiers traitements des déclarations de sinistres, facturation, réassurance, reporting réglementaire...

Enfin, des réflexions théoriques, la blockchain arrive au stade des premières applications, laissant entrevoir son immense potentiel en matière de simplification et de sécurisation des échanges. C'est ainsi qu'en 2017 quatorze assureurs ont validé un principe de blockchain pour une plateforme d'échange sécurisé des données des assureurs emprunteurs (la loi Hamon permettant maintenant de changer d'assurance emprunteur en cours de prêt).

Risques émergents ou risques submergeant ?

Toujours en phase avec les besoins de la société, l'assurance est une matière en constante évolution. Or, notre monde ne manque pas de risques nouveaux qui demandent, d'une façon ou d'une autre, à être couverts. On peut notamment citer les cyber-risques, pour lesquels les entreprises reconnaissent désormais majoritairement qu'elles ne peuvent plus faire l'économie d'une assurance. Citons également l'émergence des véhicules autonomes, qui questionnent la notion de responsabilité. Ou encore l'essor des drones qui pourraient, demain, sillonner nos ciels pour le meilleur et pour le pire. L'économie collaborative et du partage pose également de sérieux défis : si demain, par exemple, les particuliers ne possédaient plus leur propre véhicule, qu'adviendrait-il de la branche auto

qui représente aujourd'hui 55 % du marché ? Alors que la branche assurance santé offre quant à elle parmi les plus forts potentiels de croissance, l'e-santé et la télémédecine deviennent des terrains fertiles d'innovation. On voit par exemple certains assureurs activement collaborer avec des startups de la healthtech sur des concepts novateurs comme des télécabines de consultation en médecine générale.

Du côté des entreprises, la demande évolue également. On constate en particulier une forte tendance à protéger davantage les actifs intangibles (propriété intellectuelle, données clients, réputation...) et à se prémunir de scenarii nouveaux occasionnant des pertes d'exploitation sans dommages matériels, suite par exemple à la carence d'un fournisseur, au retrait d'un agrément ou d'une autorisation administrative, à l'évolution de la réglementation, à une épidémie...

L'inflation des risques traditionnels

Souvent liés aux évolutions technologiques et sociétales, ces risques émergents ne doivent cependant pas faire oublier les risques traditionnels, qui non seulement perdurent mais se révèlent de plus en plus coûteux. Ce sont notamment les dommages liés aux catastrophes naturelles, multipliées et amplifiées par le réchauffement climatique, et les catastrophes humaines, comme la gigantesque explosion du port de Tianjin en août 2015 qui a fait 169 morts et 800 blessés, et causé 1 milliard d'euros de dégâts. 2017 fut ainsi la troisième plus mauvaise année de l'histoire du secteur avec 306 milliards d'actifs, dont 136 milliards assurés, détruits par des catastrophes naturelles et humaines.

Dans un monde où les crises s'enchaînent à un rythme de plus en plus soutenu et avec des conséquences de plus en plus lourdes, les assureurs, qui ont vocation à soulager les hommes, les sociétés et même les États de certains de leurs risques, se doivent avant tout d'être eux-mêmes résilients. Or, face à l'ampleur mais aussi l'urgence des changements et des risques auxquels ils sont confrontés, le défi est de taille.

Pour plus d'information, contacter >>
antoine.bourbon@atos.net

De la crise systémique au système en crise

Retenant la leçon de 2008, les établissements bancaires et financiers ne comptent pas seulement sur la réglementation pour juguler les risques d'un emballement systémique. Ils disposent également de leviers managériaux, organisationnels et technologiques pour limiter d'eux-mêmes les risques d'une nouvelle crise.

Avec l'abrogation en 1999 du Glass-Steegall Act, qui visait à séparer les activités de prêts et de dépôts des activités opérations sur titres et valeurs mobilières, la culture du risque des banques d'affaires a sapé la culture de prudence traditionnelle des banques de dépôt, lesquelles pouvaient en outre utiliser les dépôts de leurs clients pour investir sur les marchés. Ceci a fragilisé tout le système bancaire américain, dont l'effondrement s'est ensuite trouvé accéléré par l'essor au cours des années 2000 des prêts immobiliers à des personnes dites N.I.N.J.N.A (« no income, no job, no asset »). En effet, lorsque le marché immobilier a commencé à se retourner en 2006, les défauts de paiement se sont multipliés, les prix ont commencé à baisser et les ventes sur saisies n'offraient plus aux banques une couverture suffisante. Ces prêts aux NINJNA ayant déjà été revendus sur les marchés, le piège s'est alors refermé. Malgré son origine purement américaine, la crise s'est ensuite globalisée car – second facteur – une crise de confiance structurelle s'est alors installée sur le marché interbancaire à l'échelle mondiale. La conséquence fut un net recul des investissements dans le système bancaire, à l'instar des banques américaines qui, dans les années suivantes, refusèrent de prêter aux établissements européens. S'en est suivi un manque de liquidités qui a pénalisé toute l'économie.

En plus de la conformité aux réglementations instaurées depuis, les acteurs bancaires cherchent à se prémunir par eux-mêmes de la répétition d'un tel scénario. Pour cela, ils ont à leur disposition trois principaux leviers : la refonte des fonctions Risques et Conformité, les smart contracts et la modernisation des moyens de paiement.

Levier n°1 : la refonte des fonctions Risques et Conformité

Le premier levier pour se prémunir d'une crise similaire à celle de 2008 réside dans un changement culturel et organisationnel des fonctions Risques et Conformité, dont le fréquent cloisonnement ne permet pas une vision globale, partagée et homogène de la gestion des risques. Chacune employant leur langage et leurs outils propres, elles ont des approches du risque différentes et difficiles à réconcilier. Une solution serait d'intégrer toutes les fonctions de gestion du risque au sein d'une direction unique dont les principes pourraient être les suivants : confier l'analyse et la compréhension de la réglementation aux équipes Conformité ; orienter le travail des opérationnels Risques et Conformité sur des tâches à plus forte valeur ajoutée ; utiliser des outils de monitoring pour automatiser la consolidation des données et la création des reportings. Outre les gains d'efficacité et de précision, ces outils permettraient de mieux suivre l'évolution des risques, d'en décentraliser la gestion auprès des métiers et de s'assurer que les mesures correctrices ont été prises.

Levier n°2 : les smarts contracts

Le deuxième levier de prévention d'une crise majeure est technologique. L'usage de smarts contracts pourraient permettre en effet d'éviter une perte généralisée de confiance comme en 2008. Les « contrats intelligents » inscrivent dans la blockchain les termes d'un accord et les modalités de son application de sorte qu'un tiers de confiance n'est plus nécessaire. Autonomes, programmables et immuables, les smart contracts exécutent en outre le contrat automatiquement sitôt remplies les conditions définies au préalable. Ils doivent enfin assurer la cohérence des balances des comptes (sans la moindre exception) et prémunir contre les tentatives de fraudes d'acteurs qui voudraient maximiser leurs gains contre le système. Ces caractéristiques permettent, par exemple, de régler les échanges entre les banques en quelques minutes (et non quelques jours) ce qui élimine presque totalement le risque de contrepartie - principale cause de manque de confiance pendant la crise économique.

Pour les banques, les avantages des smart contracts sont de trois ordres. Ils renforcent la sécurité des transactions et des données, la blockchain donnant aux parties la garantie que les termes de leur accord ne peuvent être modifiés si les parties prenantes l'avaient souhaité. Enfin, ils contribuent à une réduction des coûts, notamment sur les processus administratifs de vérification, d'exécution, d'arbitrage et de détection des fraudes. Ce serait ainsi plusieurs milliards de dollars que pourraient économiser les secteurs de la banque et de l'assurance.

Recourir aux smart contracts permettrait ainsi aux banques d'investissement et de détail d'offrir à leurs clients de meilleurs services à moindre coût, mais aussi de restaurer et renforcer leur confiance mutuelle. Ce qui, in fine, favoriserait l'investissement et l'activité économique.

Levier n°3 : la modernisation des moyens de paiement

On l'a vu, l'une des conséquences de la crise de 2008 a été un assèchement des liquidités préjudiciable à toute l'économie. Pour prévenir un resserrement des flux d'argent qui accélèrerait le cercle vicieux de la perte de confiance, un des enjeux concerne la rapidité et la spontanéité des paiements. Or, en la matière, on constate que le système financier s'appuie souvent sur des technologies vieillissantes. L'utilisation de nouvelles technologies plus modernes permettrait d'accélérer significativement les transactions, et donc la circulation de l'argent dans l'économie.

Au niveau institutionnel, le règlement des transactions interbancaires prend aujourd'hui deux jours ; grâce à des systèmes fondés sur des livres distribués, comme prévoient d'en implémenter les bourses allemandes et australiennes, ces délais pourraient être ramenés à moins de deux minutes ! Outre le gain de temps colossal, les bénéfices en termes de productivité sur les processus de compensation et de règlement pourraient être réinvestis, ce qui accroîtrait d'autant plus les liquidités en circulation (exemple : Ripple, un système de règlement brut en temps réel, un marché des changes et un réseau d'envois de fonds par la société Ripple).

Au niveau des entreprises, et notamment les PME, très vulnérables aux aléas de trésorerie, de nouvelles applications permettant des paiements quasi-instantanés, que ce soit au niveau domestique ou international – lents et coûteux, les « wire transfers » traditionnels peuvent prendre jusqu'à cinq jours. Même si, globalement, les entreprises privilégient encore le système financier traditionnel aux applications innovantes, certains pays, comme l'Australie, ont commencé à implémenter des systèmes basés sur des échanges instantanés entre les acteurs financiers locaux. Des entreprises pourront toujours retarder leurs paiements, mais les délais seront toujours moins importants avec l'usage de nouvelles applications de paiements.

Pour plus d'information, contacter >>
eli.bailey@atos.net

Atos Consulting

Transformer les risques en opportunités

Atos Consulting accompagne ses clients pour créer un environnement performant de gestion des risques et de la conformité. Notre démarche permet de structurer une approche méthodologique, de sécuriser les processus et les données, et d'apporter une réelle capacité de pilotage avec une vision à 360° des risques majeurs.

Gestion des Risques

Conformité

Protection des données

Cybersécurité

connexion 13

Direction de la publication : Juliette Chantereau, Yves Duplaix (Atos Consulting), Marie Iserbijt, Goska Moll (Marketing & Communication France, Atos).
Rédacteur en chef : Yves Duplaix
Comité éditorial : Yacine Ait Madi, Celia Allouche, Eli Bailey, Antoine Beullier, Antoine Bourbon, Eric Delaye, Dominique Dexyl, Dorothee Golliet, Jie Li, Marjolaine Lombard, Jacques de Parcevaux, Charles Piron, Jérémy Renard, Mickael Ribeiro, Laurent Sauphanor, Jean-Baptiste Siproudhis, Jean-Baptiste Voron.
Design : Atos Marcom Agency
Crédits photo : Banque d'Images Atos, Getty Images. tous droits réservés.

Atos, le logo d'Atos, Atos Codex, Atos Consulting, Atos Worldgrid, Bull, Canopy, equensWorldline, Unify, Worldline et Zero Email sont des marques déposées du groupe Atos. Juillet 2018 © 2018 Atos.

CT_180716_SKR_Connexion_FR