TONE at the TOP®

*L'essentiel sur la gouvernance à destination des administrateurs, des comités d'audit et du management des organisations.*

**Numéro 97 | Février 2020**

# Gouvernance des données : ce que les administrateurs doivent savoir

*Les données révolutionnent le monde de la gouvernance.*

Les responsabilités des administrateurs évoluent en permanence, mais de temps à autre s'opère un changement radical, qui transforme fondamentalement les règles de bonne gouvernance. L'entrée en vigueur de la loi Sarbanes-Oxley, pour ne nommer qu'elle, faisait suite à une vague de défaillances de gouvernance après le scandale d'Enron Corporation. Du jour au lendemain les responsabilités des administrateurs ont considérablement évolué. L'ordre du jour des conseils s'est complexifié et les réunions se sont multipliées.

Aujourd'hui, la gouvernance d'entreprise traverse un nouveau bouleversement. Cette fois, il n'est pas question des dispositifs de contrôle financier, mais de données. Et il se pourrait que ce soit l'évolution la plus significative à ce jour.

Que les responsabilités des conseils d'administration en matière de données évoluent n'est guère étonnant. Selon un article paru en 2018 sur Forbes.com, c'est au cours des deux années précédentes qu'auraient été créées 90 % des données à travers le monde. C'est un chiffre impressionnant. Chaque jour, ce sont pas moins de 2,5 quintillions d'octets de données qui sont produits sur les cinq continents, et la cadence s'accélère encore. Bien qu'à l'heure actuelle, les centres de données consomment environ 2 % de l'électricité mondiale, certains analystes estiment que ce chiffre devrait atteindre 8 % à horizon 2030.

Et le lancement de la 5G promet à nouveau une augmentation *exponentielle* des données collectées. Aujourd'hui, l'unité de mesure utilisée pour parler de la collecte des données est le gigaoctet. La 5G nous promet un changement d'échelle, qui irait jusqu'au zettaoctet (milliers de milliards d'octets). Longuement attendue, cette révolution technologique permettra aux organisations de recueillir des quantités de données titanesques, lesquelles pourront être utilisées pour prendre des décisions stratégiques avisées, et pour intégrer « l'intelligence » dans tous les domaines.

## À chaque nouvelle opportunité ses risques

Dans la mesure où les entreprises détiennent de telles quantités d'informations dans leurs systèmes, les processus de gouvernance des données ont un impact critique sur les opérations, ainsi que sur le risque de conformité et sur le résultat annuel. Le périmètre que les données et leur analyse peuvent affecter dans nos organisations peut aller bien au-delà de ceux de la sécurité des données et des systèmes d'information.

## À propos de l'IIA

The Institute of Internal Auditors Inc. (IIA) est une association professionnelle qui compte plus de 200 000 membres répartis dans plus de 170 pays et territoires à travers le monde. Porte-parole mondial de la profession d'audit interne, l'IIA intervient en tant que leader incontesté dans les domaines de la formation, de la recherche et de la formulation de normes.

## The IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

## Abonnements gratuits

Consultez le site www.theiia.org/tone pour vous abonner gratuitement.

## Avis des lecteurs

Envoyez toutes vos questions et observations à l'adresse : tone@theiia.org.

## Conseil consultatif en matière de contenu

Riches de plusieurs décennies d'expérience comme membres de la direction ou du conseil d'administration, les professionnels énumérés ci-après ont revu le contenu de la présente publication :

Martin M. Coyne II
Michele J. Hooper
Kenton J. Sicchitano

Nouvelles formes de marketing, de production, de recherche, de travail... les données offrent d'impressionnantes alternatives inédites aux entreprises, dont certaines peuvent s'avérer très lucratives.

Prenons l'exemple de l'industrie automobile. Aujourd'hui, les voitures connectées intègrent des capteurs qui génèrent des données relatives aux états et processus internes du véhicule et qui recueillent des informations sur les conditions de route, le trafic, les conditions météorologiques, et même sur la personne au volant. La valeur de ces données est considérable. Les fabricants automobiles les utilisent ; que ce soit dans le cadre de la conception, du marketing, des actions qualité ou de la gestion des rappels. Grâce à elles, ils peuvent inciter les consommateurs à effectuer l'entretien et les réparations recommandés. En outre, les informations issues de ces voitures connectées peuvent également être vendues à des tiers, comme des compagnies d'assurances par exemple. Un rapport de McKinsey & Company estime que d'ici 2030, le chiffre d'affaires généré chaque année par la monétisation des données automobiles à l'échelle mondiale pourrait atteindre 750 milliards de dollars. Dans l'éventualité d'un accident, les messages d'urgence émis par les véhicules connectés peuvent même sauver des vies. (L'eCall est une exigence du Parlement européen, applicable aux nouveaux véhicules, rédigée spécialement à cet effet).

Les opportunités que recèle le Big Data sont gigantesques. En revanche, les responsabilités qui en découlent le sont tout autant. Pour collecter les données produites par les véhicules, leurs fabricants devront être en mesure de prouver qu'ils ont obtenu le consentement des consommateurs, en respectant les règles en vigueur. De la conception à la commercialisation des nouveaux produits et services, l'éthique applicable aux données ainsi que la vie privée et la transparence doivent être prises en compte. Les questions de sécurité requièrent que les données soient exactes et que les fuites de données fassent l'objet d'une communication externe, conformément aux différentes règles à travers le monde.

Rien qu'aux États-Unis, les lois et règlements fédéraux et étatiques sur la protection des données sont nombreux, avec plusieurs autorités de régulation chargées de leur surveillance. Les exigences en la matière sont en constante évolution : par exemple, le CCPA *(California Consumer Privacy Act)* est entré en vigueur au mois de janvier et les législateurs proposent déjà des amendements. De nombreux autres états ont voté des lois relatives à la protection des données personnelles, et le Congrès envisage de réformer considérablement les lois fédérales sur le sujet. Selon l'ITIF (Information Technology & Innovation Foundation), si la législation fédérale proposée reflète les principales prévisions de la loi votée en Californie ou celles du RGPD, entré en vigueur en Europe en 2018, alors le coût de ces nouvelles exi-

gences réglementaires sur l'économie américaine avoisinerait les 122 milliards de dollars par an ; soit 483 dollars par Américain.

Ces coûts donnent le vertige, mais la conformité aux réglementations sur les données personnelles ne représente qu'un seul des enjeux de la gouvernance des données. Les programmes de gouvernance prennent également en compte les enjeux liés à l'intégrité des données, de même qu'à leur exactitude, exhaustivité, cohérence, efficience, efficacité, confidentialité, disponibilité, fiabilité et à leur caractère éthique. C'est une tâche titanesque et elle continue de prendre de l'ampleur.

## Responsabilité juridique des administrateurs

Le risque va croissant pour les administrateurs que leur responsabilité personnelle soit engagée s'ils ignorent les règles en matière de protection des données personnelles ou tout autre critère de gouvernance essentiel. En juin 2019, la Cour suprême du Delaware a rendu une décision qui affirmait de nouveau que les administrateurs étaient juridiquement responsables ; même lorsqu'il n'existe aucune procédure de remontée d'information au conseil d'administration concernant les sujets essentiels de la conformité. Dans l'affaire Marchand c. Barnhill (aussi appelée « affaire Blue Bell ») la Cour a déclaré que les administrateurs font preuve de mauvaise foi relativement à leur devoir de loyauté lorsqu'ils s'abstiennent de toute tentative pour s'assurer qu'un système de reporting raisonnable existe. Bien que la responsabilité des administrateurs et des autres dirigeants soit généralement protégée, dans la plupart des états, les administrateurs n'ont pas le droit de « manquer à leurs devoirs quant aux problématiques essentielles » de leur entreprise. Pour les administrateurs, choisir délibérément de « ne pas surveiller ou superviser les opérations [de l'organisation], s'empêchant ainsi d'être tenus informés sur les risques ou problèmes qui nécessitent leur attention » est également qualifié de manquement à leur devoir de surveillance.

La décision de l'affaire Marchand, qui suit toujours son cours actuellement dans les juridictions du Delaware, se concentrait sur le manquement du conseil d'administration relativement à la supervision des risques « critiques à leur mission » en matière de sécurité alimentaire. Toutefois, les conseils d'administration ont reçu le message : l'ignorance n'est plus une excuse.

## QUESTIONS SUR LA GOUVERNANCE DES DONNÉES POUR LES ADMINISTRATEURS

1. **Quel type de données nous concerne ?**
   Une gouvernance des données efficace commence par la connaissance du type de données collectées, de leur lieu de stockage et de la façon dont elles sont utilisées à travers l'organisation. Dans de nombreux cas, un diagramme des flux de données peut renforcer la gouvernance des données et en améliorer la compréhension.

2. **Nos données sont-elles utilisées convenablement ?**
   Les données doivent être disponibles à tout moment, à des fins légitimes pour l'organisation. Le système de gouvernance des données devrait participer à en donner l'assurance. En outre, il doit également protéger les informations sensibles et assurer que l'utilisation des données respecte l'éthique.
   Les administrateurs doivent savoir si l'organisation a créé des règles et procédures adéquates relatives à l'utilisation des données, et ils doivent s'assurer que des dispositifs de contrôle existent pour les surveiller et les faire respecter.

3. **Avons-nous attribué des objectifs spécifiques à notre programme de gouvernance des données ?**
   Chaque organisation est différente. Il n'existe donc pas d'approche unique et standardisée en matière de gouvernance des données. Si le programme de gouvernance des données est encore relativement jeune, identifier les données critiques ou sensibles de l'ensemble de l'organisation peut être une tâche considérable, par exemple.
   Avec plus de maturité, les priorités peuvent être réorientées, notamment sur la minimisation des risques, l'augmentation de la valeur des données ou l'amélioration du flux d'information. Par conséquent, les objectifs de la gouvernance des données et ses priorités devraient être évalués à nouveau régulièrement.

4. **Comment avons-nous évalué les risques ?**
   Chaque organisation doit composer avec des risques comme la perte, la corruption ou la fuite de données, sans oublier les non-conformités. Éliminer tous les risques est impossible, mais il est important que les conseils d'administration reçoivent en temps utile les informations relatives aux risques afférents aux données, et qu'ils évaluent si le niveau d'exposition aux risques correspond à l'appétence pour le risque de l'organisation.

5. **Lorsque des anomalies sont identifiées, comment obtenons-nous l'assurance qu'elles ont été résolues convenablement ?**
   Le conseil d'administration doit comprendre les processus de communication et de résolution des anomalies significatives de gouvernance des données. Ils doivent également s'assurer que lorsque des problèmes ont été identifiés, ils sont convenablement résolus.

6. **Qu'en est-il des référentiels de gouvernance des données ?**
   Un référentiel de gouvernance des données fournit des directives quant à l'utilisation des données, leur gestion et la résolution des anomalies. Il identifie les personnes et services responsables du contrôle et de la gestion des différents types de données. À l'échelle de l'organisation, le référentiel pourrait inclure un comité de gouvernance des données qui contribuerait à la mise en application du programme, ainsi qu'une instance de gouvernance ou un comité qui prioriserait les projets de gouvernance de données, approuverait les politiques d'utilisation, les processus et procédures, et identifierait les responsables du traitement ainsi que les parties prenantes. Si votre entreprise n'a pas encore approuvé de référentiel de gouvernance des données pour identifier les acteurs et leurs responsabilités, il est peut-être temps de demander pourquoi.

**Ressources :**
NIST Cybersecurity Framework
NIST Privacy Framework

## Responsabilités des conseils d'administration

Il y a de cela une décennie, la gouvernance des données pouvait, ou non, être à l'ordre du jour des conseils d'administration. Lorsqu'elle l'était, la discussion se limitait souvent à un seul aspect, comme la sécurité des données ou la confidentialité. Et souvent, si les administrateurs avaient des questions sur la gouvernance des données, ils se fiaient simplement au management pour leur fournir les informations dont ils avaient besoin.

Compte tenu des risques liés aux données aujourd'hui, cette approche n'est plus adaptée. Dans un rapport récent paru dans Compliance Week, 46 % des conseils d'administration interrogés étaient tenus informés de la gouvernance des données au moins tous les trois mois. Presque la moitié d'entre eux avait mis en place, ou mis à jour, des politiques internes relatives à la vie privée. En matière de protection des données personnelles, 43 % s'étaient dotés de ressources supplémentaires et avaient augmenté leur budget. Seuls 5 % des interrogés ne recevaient aucune information sur la gouvernance des données.

Afin de remplir leur devoir de supervision, les administrateurs doivent recevoir une assurance indépendante et objective que les risques liés aux données sont gérés de manière adaptée. Cela implique que les risques significatifs en matière de gouvernance des données doivent être audités. Néanmoins, il appartient également aux administrateurs de poser les questions difficiles sur ce sujet. Pour Brian Stafford et Dottie Schindlinger, co-auteurs de *Governance in the Digital Age, A Guide for the Modern Corporate Board Director*, « les administrateurs doivent savoir ce qu'ils ignorent, et cela demande beaucoup de courage. Ils doivent être capables de poser des questions et de faire preuve d'honnêteté sur ce qu'ils ne comprennent pas, sans quoi ils ne seront pas en mesure de fournir le niveau de supervision et d'éclairage dorénavant requis ».

### Sondage rapide

**Votre organisation dispose-t-elle d'un programme formel de gouvernance des données ?**

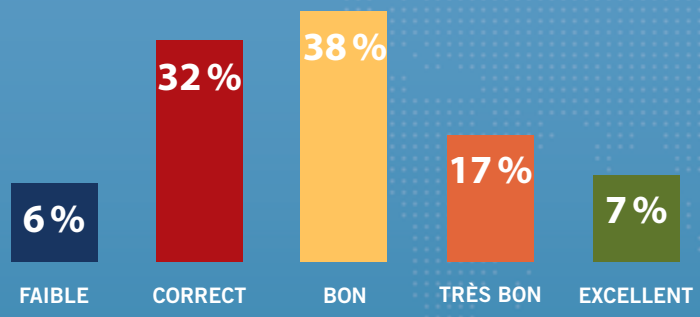
- ❑ Non, et nous n'avons pas l'intention d'en établir un.
- ❑ Non, mais nous avons l'intention d'en établir un.
- ❑ Oui, mais il n'est pas encore mature.
- ❑ Oui, nous disposons d'un programme mature*.
- ❑ Je ne sais pas. Il est temps de le découvrir.

Rendez-vous sur www.theiia.org/tone pour répondre à cette question et connaître les réponses des autres.

** Un programme de gouvernance des données mature définit les responsabilités spécifiques, surveille la conformité et permet le reporting des informations relatives à la gouvernance des données au management et au conseil d'administration.*

## RÉSULTATS DU SONDAGE RAPIDE :

Comment qualifieriez-vous l'efficacité du leadership de votre conseil d'administration et de votre management en matière de gouvernance ?




Source : Tone at the Top | Sondage du numéro de décembre 2019