



# LES 12 RESPONSABILITÉS DE LA GOUVERNANCE DE L'INFORMATION

LECTURE DE 5 MINUTES



# LES 12 RESPONSABILITÉS DU CONSEIL DE GOUVERNANCE DE L'INFORMATION

L'INFORMATION EST PRÉSENTE PARTOUT DANS VOTRE ENTREPRISE. LA RESPONSABILITÉ DE SA GOUVERNANCE APPARTIENT AUX DIFFÉRENTS DÉPARTEMENTS ET AUX DIRIGEANTS D'UNE GRANDE VARIÉTÉ DE DISCIPLINES ET DE SERVICES.



## 1. JURIDIQUE

- > Détermine le profil de risque d'une entreprise en fonction de son exposition aux litiges, des exigences internationales en matière de confidentialité, de sa protection, de la propriété intellectuelle, de son environnement de travail et plus encore.
- > Développe et approuve le calendrier de conservation des dossiers et la politique de gestion de l'information (GDI).
- > Désigne les classifications de confidentialité.
- > Développe les règles pour la gestion des emails, des réseaux sociaux, des appareils mobiles, électroniques et réseaux.
- > Communique les changements organisationnels suite aux fusions, acquisitions et cessions.
- > Émet des approbations pour la destruction sécurisée.
- > Communique les changements de règles et de réglementations à la direction des risques, de l'information et aux équipes informatiques.
- > Collabore avec les parties prenantes clés de la gouvernance de l'information.



## 2. INVESTIGATION

- > Communique, donne des instructions et coordonne les business units et les professionnels de l'information devant être conservées, préservée et fournie pour respecter les exigences en matière de litige.
- > Gère les demandes de liberté de l'information dans les pays comme la France. Ceci comprend le fait de tenir les responsables au courant du statut des obligations de conservation de l'information et du moment où elle peut être libérée pour réintégrer la gestion normale du cycle de vie de l'information.
- > Tient à jour les équipes de GDI et informatique à propos des changements apportés aux exigences d'investigation.
- > Met en place un processus reproductible avec des directives afin de gérer l'ensemble du litige qui impacte le contrôle des obligations de conservation dans le cadre du dispositif.



### 3. RISQUE

- > Protège la marque, les finances et les activités de votre organisation en gérant et atténuant l'exposition au risque.
- > Doit comprendre entièrement le profil de risque de l'entreprise (litiges, enquêtes, exigences réglementaires, protection des informations personnelles et propriété intellectuelle) et les contrôles qui y sont associés.
- > Collabore avec le service juridique pour créer une politique sur l'utilisation acceptable.
- > Collabore avec le service informatique pour élaborer des processus de reprise et de continuité de l'activité après un sinistre, et sélectionne les fournisseurs de SaaS/Cloud.
- > [Forme les employés](#) à propos de la prévention des activités liées aux risques.
- > Donne son avis à propos des indicateurs de risque clés.



### 4. CONFORMITÉ

- > Assure que votre entreprise est sensibilisée aux exigences des règles et réglementations imposées par les autorités et qu'elle les respecte (comme l'UE, les autorités de contrôle, les autorités de protection des données et les différents secteurs).
- > Détermine les mesures et les contrôles internes; établit un programme de vérification à l'échelle de l'entreprise; réagit aux et gère les demandes des autorités de contrôle, des auditeurs, des enquêteurs, des clients et des tierces parties.



### 5. GESTION DES DOCUMENTS ET DE L'INFORMATION

- > Développe et publie la politique du programme de GDI pour les documents papier et fichiers électroniques.
- > Soutient la mise en œuvre à l'aide de formations et de communications continues.
- > Détermine et mesure la conformité.
- > Limite les coûts à l'aide de la sensibilisation au cycle de vie de l'information, de choix des solutions de conservation et de la destruction sécurisée.
- > Participe à des projets informatiques pour l'évaluation et la mise en œuvre de logiciels.
- > Propose son soutien aux différentes directions métiers afin d'intégrer un réseau de coordination des documents.
- > Reste à l'affût des tendances en matière de GDI (Cloud, Big data, politique BYOD/PAP).
- > Communique et collabore avec les parties prenantes clés pour déterminer la politique ou l'approche.

Lorsque l'autogouvernance au niveau de l'entreprise devient institutionnalisée, le service de GDI doit créer un environnement de libre-service à partir duquel les personnes concernées peuvent se procurer l'information dont elles ont besoin afin de respecter les exigences de la gouvernance de l'information de la GDI.

La mise en place d'une gouvernance de l'information fera en sorte que cette fonction passe d'une base axée sur les documents à l'inclusion de toutes les informations, qu'elles soient physiques ou électroniques.



## 6. DATA OFFICE OU GOUVERNANCE DES DONNÉES

- > Aide les entreprises et les autres fonctions à assurer une approche uniforme et contrôlée par rapport au développement et à l'utilisation des actifs informationnels et des éléments de données critiques dans une entreprise (rôle de la fonction du responsable des données) et précisément le rôle de responsable des données (responsable des informations en matière de santé dans le secteur de la santé).
- > Guide la mise en place de processus et de systèmes pouvant créer, conserver et partager les données conformément aux normes en matière de données et des réglementations/lois externes d'une entreprise.
- > Met en œuvre un cadre de contrôle pour soutenir une gestion efficace des données (en collaboration avec les membres du conseil de gouvernance de données de l'entreprise).

Le responsable des données (CDO) collabore avec les responsables de la gouvernance assignés aux fonctions et aux activités dans l'ensemble de l'entreprise. Ensemble, ils effectuent des évaluations des pratiques de gouvernance des données ou de gestion des données à l'aide de différents outils, tels qu'un modèle de maturité des données, une plateforme de qualité et des plans de mise en œuvre des normes en matière de données.



## 7. INFORMATIQUE

- > La fonction se modifie pour s'aligner davantage avec les directions métiers et leurs objectifs.
- > Augmente la capacité à gérer le volume élevé de données créées et reçues.
- > Élimine des coûts, particulièrement ceux des technologies redondantes et du stockage.
- > Contribue aux contrôles de la GDI en s'occupant de la protection et de l'authentification des données et de leur accessibilité pour l'utilisation, la préservation et la destruction sécurisée.
- > Collabore avec la GDI ainsi qu'avec le service des risques et de la conformité pour établir les plans appropriés de reprise et de continuité des activités après sinistre.
- > Collabore avec tous les autres rôles de gouvernance de l'information pour comprendre le choix des technologies et les exigences de déploiement de chacun.



## 8. CONFIDENTIALITÉ DE L'INFORMATION

- > Gère les risques et les effets sur l'activité des lois et des politiques relatives à la confidentialité.
- > Réagit aux préoccupations des autorités de contrôle et des clients par rapport à l'utilisation des informations personnelles identifiables (IPI), y compris les données médicales et financières, et par rapport aux lois et réglementations sur l'utilisation et la protection des transactions financières et bancaires des consommateurs.
- > Donne des conseils à propos de la protection et des précautions appropriées pour des informations spécifiques à risque élevé et leurs effets sur les contrôles des risques de GDI.



## 9. SÉCURITÉ DE L'INFORMATION

- > Développe, met en œuvre et gère l'approche sécurité, la stratégie, la politique et les programmes de l'entreprise.
- > Crée une politique, sélectionne la technologie, met en œuvre la politique et surveille et informe les parties à propos des logiciels malveillants, des fuites, du piratage et d'autres événements reliés.
- > Transmet les politiques et les procédures à l'ensemble de l'entreprise.
- > Permet l'adoption de normes de sécurité dictées par des clients, entre autres les administrations publiques.
- > Informe les parties nécessaires en cas de fuite d'informations.
- > Émet des codes de classification des données (conjointement avec le service juridique).
- > Reste conforme avec la CNIL et les autres autorités de contrôle de protection des données.



## 10. ARCHITECTURE DE L'INFORMATION

- > Se concentre sur l'organisation de l'information et le développement de bases de données pour soutenir les besoins de votre entreprise.
- > Conçoit des systèmes informatiques complexes et partagés.
- > Participe à la sélection et à la gestion des services dans le Cloud.
- > Soutient la création d'archives pour le contenu des emails et des réseaux sociaux.
- > Soutient la création de sites Web et d'intranets efficaces pour soutenir la GDI.



## 11. ENTREPRISE

(DIRECTIONS MÉTIERS, BUSINESS UNITS ET/OU SERVICES)

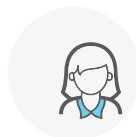
- > Assure la conformité avec les politiques de gouvernance de l'information.

La gestion du cycle de vie de l'information est plus efficace lorsqu'elle utilise les attributs, balises, indices ou métadonnées nécessaires pour la conformité le plus rapidement possible après la création, par exemple en ajoutant un marqueur sur une information afin d'indiquer son caractère confidentiel ou qu'elle contient des informations personnelles identifiables ou qu'elle appartient à une classe ou un groupe précis de documents.

Les directions métiers se plaignent souvent que la gestion des documents les empêche de mener à bien leurs activités. Afin d'améliorer la situation, les services informatique et de la GDI devraient travailler en étroite collaboration avec les directions métiers afin de déterminer comment mieux contrôler leurs informations à l'aide de la technologie et comment la traiter de la manière la moins intrusive possible.

Les directions métiers sont les mieux placées pour juger la valeur de l'information qu'elles créent, conservent ou reçoivent au-delà de leur utilisation originale. Plusieurs types de documents peuvent être utilisés pour dégager les tendances marketing, surveiller les problèmes de contrôle de la qualité, élargir les profils de clients et identifier les « mauvais joueurs » dans un environnement réglementé. Le service de GDI devrait travailler avec les directions métiers pour identifier les informations importantes et la manière dont elles doivent être protégées de manière sécurisée et conforme.

Il existe une forte tendance visant à rendre les directions métiers responsables de l'autogouvernance d'une variété d'exigences d'entreprise, y compris la GDI. C'est particulièrement le cas dans les grandes entreprises dispersées géographiquement avec des directions métiers diversifiées. L'entreprise s'attend à récupérer l'information nécessaire pour s'autogouverner et de se la procurer auprès du service de GDI et du service juridique.



## 12. REPRÉSENTATION INTERNATIONALE

Étant donné que la gouvernance de l'information devrait s'étendre à toute une entreprise, il doit y avoir une forte représentation géographique au sein du conseil. Cette représentation peut être un délégué d'une région (c.-à-d. Asie-Pacifique, EMOA et Amérique du Nord) apte à parler des préoccupations des différentes juridictions au sein de la région.



Vous avez besoin de plus d'informations,  
d'aide ou de conseils ?