GUIDE PROFESSIONNEL

association française de la gestion financière

La cybersécurité en 4 étapes

Guide pratique pour les sociétés de gestion

Octobre 2019

L'Association Française de la Gestion financière (AFG) représente et défend les intérêts des professionnels de la gestion de portefeuille pour compte de tiers.

Créée en 1961, elle réunit tous les acteurs du métier de la gestion d'actifs, qu'elle soit individualisée sous mandat ou collective via les Organismes de placement collectif (OPC). Ses membres sont les sociétés de gestion de portefeuille, entrepreneuriales ou filiales de groupes bancaires ou d'assurance, français et étrangers. Depuis 2009, l'AFG accueille des "membres correspondants" (80 à fin 2018) représentatifs de l'écosystème de la gestion : avocats, cabinets de conseil, SSII, fournisseurs de données, succursales.

La gestion d'actifs française représente plus de 4 000 Mds € sous gestion, soit un quart du marché de la gestion d'Europe continentale. Source de plus de 85 000 emplois dont 26 000 propres aux sociétés de gestion, elle joue un rôle essentiel dans le financement de l'économie.

L'AFG a pour mission d'informer, d'assister et de former ses adhérents. Elle leur apporte un concours permanent dans les domaines juridique, fiscal, économique, comptable et technique.

Elle anime la réflexion de la profession sur l'évolution des techniques de gestion, la recherche, et la protection et l'orientation de l'épargne.

Interlocuteur des pouvoirs publics français, européens et internationaux, l'AFG contribue activement à l'évolution de la réglementation. Elle définit les règles de déontologie de la profession et joue un rôle moteur en matière de gouvernement d'entreprise.

L'Association contribue également à la promotion et au rayonnement de la gestion française (l'une des premières au monde) auprès de l'ensemble des acteurs concernés : investisseurs, émetteurs, politiques et médias, en France et à l'international.

41 rue de la Bienfaisance | 75008 Paris | Tél. +33 1 44 94 94 00
45 rue de Trèves | 1040 Bruxelles | Tél. +32 2 486 02 90
@AFG_France | www.afg.asso.fr

La cybersécurité en 4 étapes

Guide pratique pour les sociétés de gestion

Octobre 2019

sommaire

sommaire

sommaire

Préface

La sécurité informatique est devenue en quelques années un réel enjeu pour l'ensemble des entreprises, principalement dans le domaine de la finance. Les sociétés de gestion de portefeuille (SGP) n'y échappent pas.

Le risque cybersécurité apparaît pour plus de 50 % des sociétés de gestion comme faisant partie du "top trois" des risques les plus redoutés. La prise de conscience est donc réelle, ce qui est une bonne chose. En effet, que ce soit au niveau de l'ensemble des collaborateurs de la SGP ou de sa direction, le risque cyber doit être pris en compte par tous car chacun est acteur de la sécurité informatique.

Notamment le responsable de la sécurité des systèmes d'information, le RSSI.

Qu'il vienne d'être nommé dans une SGP nouvellement créée et se retrouve face à une page blanche, ou qu'il prenne ses fonctions dans une entreprise soucieuse de mieux gérer son risque cyber, ou bien qu'il souhaite évaluer son niveau de maturité, ce guide *La cybersécurité en quatre étapes* lui offre une synthèse de l'ensemble des actions à mettre en œuvre afin de bien gérer le risque cyber.

Quatre étapes car il ne s'agit pas de tout traiter de front mais de prioriser ces actions afin de disposer de bases saines et pouvoir ainsi construire les fondations nécessaires à la mise en place d'une sécurité robuste et efficace.

Ces quatre étapes seront présentes pour chacun des **six piliers de la sécurité informatique** :

1. Gouvernance
2. Contrôles
3. Postes de travail
4. Serveurs et applications
5. Échanges de données et accès internet
6. Sensibilisation

Vous retrouverez dans chaque chapitre les étapes suivantes :

- **Par où commencer ?**
- **Les actions à court terme**
- **Les actions à moyen terme**
- **Pour aller plus loin !**

Il est fortement conseillé d'avoir un niveau de maturité cohérent sur l'ensemble des piliers car on ne le répétera jamais assez : **le niveau de sécurité globale de votre système d'information sera celui de votre maillon le plus faible.**

CHAPITRE 1 / GOUVERNANCE

Par où commencer ?

1) Organisation : responsabilités (RACI), comités de gouvernance

Les actions ci-après sont fondamentales et ont pour objectif de clarifier les responsabilités et de favoriser la prise de décisions (lancement d'actions, octroi de moyens).

- J'identifie et/ou je définis **les relais assurant les missions de proximité** relatives à la SSI dans les métiers sans oublier la dimension internationale (filiales...).
- J'identifie et/ou je définis **les instances décisionnelles** où seront discutés les objectifs stratégiques SSI.
- Je fais une synthèse de l'organisation envisagée et fais entériner le dispositif par un comité de niveau Direction générale.

Interlocuteurs	Direction générale, DSI, Risques opérationnels, Conformité/Déontologie, Juridique, Fraude, Sécurité financière, Inspection générale
Points de contrôle	Document de procédure avec date de mise à jour, support des comités et des comptes-rendus

2) Formaliser un plan d'action sécurité

L'objectif est de disposer d'un plan d'action SSI spécifique à la société de gestion de portefeuille et de s'assurer de son adéquation avec les ressources et priorités de la DSI ou du métier.

- Je fais la liste des **projets** à lancer avec un indice de gain en sécurité et de coût de réalisation. Je propose des priorités pour chaque projet et, pour aider à l'arbitrage, je définis les risques à ne pas réaliser chacun des projets.
- Je prépare le **plan d'action récurrent** et définis un budget correspondant en lien avec le DSI.
- Je planifie un comité décisionnel afin d'obtenir les **arbitrages nécessaires sur les projets** ainsi que sur le plan récurrent.

Interlocuteurs	Direction générale, DSI
Points de contrôle	Plan d'action, support du comité et compte-rendu

3) Initier une politique de sécurité

Il est important de mettre en place une politique de sécurité afin de définir les règles applicables. Celle-ci doit être adaptée aux contextes métiers propres à votre société de gestion et être validée par la direction.

Ce document doit être mis à jour régulièrement afin de prendre en compte les nouvelles technologies, l'évolution des menaces ou encore les évolutions réglementaires.

En complément des règles générales, nous proposons de commencer la formalisation des points suivants :

A. Classification des données sur les aspects "confidentialité"

- Je définis les **niveaux de classification** dans la société de gestion
  Exemple : public, interne, confidentiel
  ainsi que les **mesures associées.**
  Exemple : les données confidentielles doivent être systématiquement chiffrées

B. Formalisation du processus de gestion des habilitations

- Voir le chapitre 2 qui présente quelques contrôles.

C. Formalisation du processus de mise à jour

- Voir les règles exposées au chapitre 3.

Interlocuteurs	Direction juridique, Conformité / Déontologie, DRH
Points de contrôle	Politique et date de dernière mise à jour, preuve de la validation par la Direction générale

Actions à court terme

1) Réaliser des analyses de risque au sein des projets

L'analyse des risques permet de limiter les impacts des dangers potentiels liés à un projet.

- **J'identifie les risques** liés au projet (humains, financiers, juridiques, environnementaux,...).
- **J'évalue et je hiérarchise** les risques.
- **J'élimine ou je traite** les risques identifiés.
- **Je réévalue, je documente et je reporte** périodiquement les risques résiduels afin d'améliorer la réactivité et l'efficacité.

Interlocuteurs	Direction générale, Conformité / Déontologie, Directions métiers, Direction des risques
Points de contrôle	Suivi des risques à effectuer périodiquement

2) Processus de gestion des incidents

La gestion des incidents de sécurité a pour objectif de remonter les incidents de sécurité au bon niveau pour alerter et déclencher les actions adaptées, mais aussi d'éviter que les incidents ne se reproduisent.

- **Avant l'incident** : je vérifie l'**existence d'une procédure de gestion des incidents** et **de gestion de crise** ; le cas échéant je m'assure de sa formalisation. Je complète ce document si besoin pour prendre en compte les spécificités Cyber et je m'assure d'être informé de tout incident lié à mon périmètre.
- **En cas d'incident : j'alerte** mes correspondants et, si besoin est, la direction générale. En fonction de la gravité, **j'active** le dispositif de gestion de crise et je soumets à décision l'attribution de moyens spéciaux afin de mener les actions visant à couvrir le risque (correction d'une vulnérabilité, cloisonnement réseau, etc.).
- **Après l'incident : je participe** à la **définition du plan d'action**, je m'assure du **suivi** de l'**exécution du plan d'action** et j'étudie les **conséquences de l'incident** en termes d'évolutions potentielles de la politique et des standards de sécurité (démarche d'amélioration continue).

Interlocuteurs	Direction générale, Direction des risques, Responsable PCA, Communication
Points de contrôle	Organisation de test de gestion de crise, date de mise à jour de la procédure

3) Programme de sensibilisation

L'objectif de la sensibilisation à la sécurité est multiple :

- Faire savoir à chaque acteur et prestataire ce qui est **attendu** de lui et ses **responsabilités** pour améliorer la protection de l'information.
- Expliquer la **nature et l'évolution des menaces**.
- Informer chaque acteur sur les **démarches à engager** face à des situations prédéterminées : démarrage d'un projet, événement suspect, etc.
- Expliquer à chacun **où trouver l'information** et comment **alerter**.

Pour la mise en œuvre :

- **J'identifie les populations à cibler en priorité** *(par exemple : Directions, utilisateurs de divers métiers, assistantes de direction, managers, etc.)*.
- **J'élabore des chantiers de sensibilisation** en définissant un média adapté à chaque cas (email, affiche, etc.).
- Je me réfère au chapitre 6, *Sensibilisation des utilisateurs*.

Actions à moyen terme

1) Cartographier les applications sensibles

L'objectif de cette cartographie est d'identifier les applications les plus critiques pour le fonctionnement de la société de gestion. Ceci permettra de prioriser la stratégie et les actions de sécurité (habilitation, audit, etc.).

- J'identifie la liste des **applications métiers les plus critiques** pour le fonctionnement de la société de gestion. Pour cela, il est conseillé de partir des processus critiques pour en déduire la liste des applications qui le supportent. Plusieurs métriques peuvent être ensuite utilisées pour réduire le nombre : DICP, impact financier, application disposant d'un PCA, etc.
- J'identifie les **éléments d'infrastructure essentiels** au fonctionnement de ces applications sensibles. Ces éléments sont les serveurs et bases de données permettant de faire fonctionner l'application.

Interlocuteurs	Direction des risques, Directions métiers et DSI
Points de contrôle	Cartographie

2) Gestion des prestataires : contrats, obligations légales, *due diligence*

La gestion des prestataires est essentielle pour garantir la sécurité de l'entreprise. Il faut définir précisément les exigences que vos prestataires doivent respecter et vérifier leur bonne application.

- **En amont de la contractualisation** et en fonction de la criticité pour la société de gestion de portefeuille, je vérifie le **niveau de sécurité du prestataire** à travers la présence de certifications et de réponses à des questionnaires sécurité. *(Voir le questionnaire de l'AFG sur son site internet www.afg.asso.fr - Espace membre)*
- **Lors de la contractualisation**, je fais en sorte que les **exigences de sécurité** soient **prises en compte** dans les contrats; je formalise notamment les exigences qui devront être prises en compte par les prestataires externes ou valide le plan d'assurance sécurité fourni par le prestataire. Afin d'accélérer ce processus, il est possible de définir un clausier sécurité avec les règles standard à appliquer.
- **Régulièrement**, en fonction de la criticité de la prestation, je vérifie la **prise en compte des exigences sécurité**. Pour cela, je peux utiliser la clause d'audit pour réaliser des tests d'intrusion lorsque nécessaire.

Interlocuteurs	Équipe achat, Direction juridique
Points de contrôle	Échantillonnage des contrats pour vérifier la présence de clauses sécurité adéquates

Pour aller plus loin !

1) Gouvernance de la gestion des accès

La mise en place d'une solution d'"*Identity and Access Management*" est l'opportunité de formaliser les étapes de validation, les responsabilités et les contrôles associés.

- Je vérifie que toute **affectation d'une habilitation** nécessite bien l'**accord formel** de sa **hiérarchie** et/ou du **propriétaire métier**.
- Je vérifie que chaque **ressource** pouvant faire l'objet d'une habilitation a bien un propriétaire métier.
- Je définis un ***workflow* d'arrivée et de départ** permettant de provisionner et déprovisionner les accès de façon automatique.
- Je vérifie que le **mouvement d'une personne** donne lieu à la **mise à jour de ses habilitations** (suppression des habilitations ne figurant pas dans le service cible) et génère une **demande de validation**.
- Je contrôle la bonne application de ces points, comme indiqué dans le chapitre 2.

Interlocuteurs	Équipe DSI, Correspondants métiers

Points de contrôle	Date de la dernière revue des habilitations par les différents propriétaires métier

CHAPITRE 2 / CONTRÔLES

Par où commencer ?

1) Self-audit via le questionnaire AFG et/ou les mesures essentielles de l'ANSSI

Un self-audit du risque de sécurité est nécessaire pour effectuer *a minima* une première évaluation et une première sensibilisation des intervenants internes et des dirigeants de la société de gestion.

- Je choisis la méthodologie : par exemple le questionnaire de l'AFG ou les *23 mesures essentielles de l'ANSSI*.
- Je détermine les acteurs participants au sein de la société de gestion : par exemple le RSSI avec la DSI.
- **Je déroule la méthodologie de manière pragmatique**, sans perfectionnisme excessif.
- **Je présente les résultats à la Direction générale, de préférence avec une comparaison avec un benchmark**, par exemple les résultats globaux du questionnaire AFG.

Interlocuteurs	RSSI, DSI, Direction générale
Points de contrôle	Matrice des résultats, éléments constitutifs justifiant *a minima* les réponses, support de présentation à la Direction générale

2) Test d'intrusion externe / interne

En complément du *self-audit*, il est essentiel d'effectuer des tests d'intrusion sur les systèmes internes ou externes. Alors que les audits consistent à dérouler une méthode préétablie d'analyse, le test d'intrusion permet de simuler réellement un *hacker* visant à exploiter les données sensibles ou à perturber le fonctionnement de la société de gestion.

- Je choisis l'entité qui va effectuer le test, de préférence une société indépendante des infrastructures de la société de gestion.
- Je détermine avec le prestataire **la méthode d'intrusion la plus adaptée au contexte** : donner au testeur une certaine connaissance de la structure du SI ou non ?
- Je détermine, avec la société retenue et en étroite collaboration avec la DSI, **les systèmes critiques cibles à tester** : annuaire type *Active Directory*, sites Web publics ou privés, messagerie électronique, outils métiers critiques, répertoires de fichiers sensibles, hébergeurs externes de données sensibles…
- J'informe de la mission une liste réduite de personnes **et je respecte les modalités d'information contractuelle des prestataires impactés** (info-gérants, hébergeurs de données) même au sein du Groupe d'appartenance.
- **Je partage les résultats et recommandations** avec les responsables concernés et j'en effectue une présentation à la Direction générale de la société de gestion et au Comité concerné (par exemple "risque opérationnel" ou "sécurité").

Interlocuteurs	RSSI, DSI, prestataires essentiels

Points de contrôle	Échanges avec le responsable (interne ou externe) de la structure testée, rapport de test, éléments techniques, liste des recommandations validées

Actions à court terme

1) Mettre en place des scans de vulnérabilité sur les interfaces exposées

Des scans de vulnérabilité permettent d'évaluer régulièrement les risques de compromission des systèmes exposés (internes ou externes).

- Je choisis l'entité qui va effectuer les scans, de préférence une société externe spécialisée indépendante.
- **Je détermine, en étroite collaboration avec la DSI, les systèmes critiques à scanner** : sites Web publics ou privés, messagerie électronique, outils métiers critiques, hébergeurs externes de données sensibles…
- Je respecte les modalités d'information et les modalités contractuelles des prestataires impactés (info-gérants, hébergeurs de données) même au sein du groupe d'appartenance.
- Je partage les résultats et recommandations avec les responsables concernés ; j'en effectue une présentation à la Direction générale de la société de gestion et au Comité concerné (par exemple "risque opérationnel" ou "sécurité").
- **Je formalise un plan de remédiation, hiérarchisé** en fonction du nombre de vulnérabilités et de leur criticité, **avec une priorisation et des délais**.

Interlocuteurs	RSSI, DSI, prestataires essentiels
Points de contrôle	Échanges avec le prestataire "scanné", rapport de scan, éléments techniques, liste des recommandations validées

2) Définir un plan de contrôle sécurité

La définition d'un "plan de contrôle sécurité SI" est indispensable en termes d'encadrement *ex-ante* des actions menées, de gouvernance interne et de matérialisation vis-à-vis des organismes externes (AMF, commissaires aux comptes de la SGP ou de l'OPC, consultants en *due-diligence*....).

- **Je détermine l'articulation des niveaux de contrôle** selon l'organisation de la société de gestion :
  - Niveau 1 par un responsable sécurité opérationnelle à la DSI + Niveau 2 par le RSSI
  - ou Niveau 1 par le RSSI + Niveau 2 par la Conformité.
- **J'élabore un plan de contrôle révisé annuellement** : simple sur des thèmes principaux dans un premier temps, plus sophistiqué dans un second temps au vu de la courbe de montée en maturité.
- **Je détermine les points de contrôle** (le contenu du plan), après un échange RSSI, DSI, Conformité.
- À titre d'exemple, **les principaux thèmes du plan de contrôle peuvent être les suivants** :
  - *Existence de scans de vulnérabilité ou tests d'intrusion, suivi des recommandations*
  - *Attribution et contrôle des habilitations sur les outils/ressources critiques*
  - *Attribution et contrôle des comptes à privilèges et administrateurs informatique (internes, externes)*
  - *Circuits des habilitations exceptionnelles et des entrées/sorties/mobilités*
  - *Suivi des incidents de sécurité SI et plans de remédiation induits*
  - *Résultats des anti-virus et des filtrages (Web, messagerie...), plan de remédiation*
  - *Résultats des analyses des systèmes de détection d'intrusion ou comportement anormal, remédiation*
  - *Application du plan de correctifs de sécurité ("patch management")*
  - *Intégration des analyses de sécurité dans les projets de la société de gestion*
  - *Application des standards de sécurité de la société de gestion (politique de password, cryptage de postes,....)*
  - *Diffusion d'un tableau de bord Sécurité SI incluant les résultats des contrôles, incidents et filtrages.*
- **J'effectue un rendu des contrôles** : notes de contrôles, recommandations, tableau de bord, intégration dans le plan de remédiation, intégration dans la cartographie des risques de la société de gestion...

Interlocuteurs	RSSI, Conformité/Déontologie, DSI

Points de contrôle	Plan de contrôle, présentation et validation *ex-ante* du plan, notes de contrôle, justificatifs associés, diffusion des résultats, recommandations émises et suivies, tableau de bord

Actions à moyen terme

1) Mettre en place une revue d'habilitation sur les applications sensibles

L'objectif de cette phase est de veiller à la maîtrise des accès aux outils / ressources critiques pour le fonctionnement de l'entreprise. Il convient de **bien différencier le processus de gestion / attribution des habilitations et le processus de contrôle *ex-post* des habilitations**. Dans "habilitations", il convient d'inclure à la fois les accès aux outils, mais également les pouvoirs attribués (lecture / écriture / administration), ceci tant pour les salariés que pour les prestataires.

- J'utilise **la cartographie des applications les plus critiques** pour le fonctionnement de l'entreprise (voir chapitre 1), en veillant à intégrer les services Web externes et les répertoires mémorisant les données sensibles.
- J'effectue une revue des habilitations existantes pour les outils de cette liste, pilotée par exemple par le RSSI :
  - liste des "habilitations cibles" admises pour chaque outil, suivant les différents métiers ;
  - **extraction des habilitations en vigueur dans ces outils et comparaison avec la cible** ;
  - identification des cas anormaux (utilisateurs ayant quitté la société de gestion ou non-habilités) ;
  - transmission aux responsables d'équipes concernés et arbitrage éventuel par la Direction ;
  - **correction des cas anormaux** dans les applications (clôture, réduction des droits).
- J'associe à la revue une rédaction ou mise à jour de la procédure de gestion des habilitations : attribution/modification en fonction des entrées / sorties / mobilité des salariés et prestataires.

Interlocuteurs	RSSI, DSI, Conformité / Déontologie, sociétés externes hébergeant des systèmes ou des services essentiels

Points de contrôle	Matrice des habilitations autorisées par outils/métiers, extractions des habilitations en vigueur, résultat du contrôle, échanges de validation, demandes de correction des accès

Actions à moyen terme (suite)

2) Audit indépendant ou audit interne

Après la mise en œuvre des premières actions et pour compléter les phases précédentes, il est souhaitable de faire effectuer un audit pour obtenir une vision plus approfondie et indépendante

- Je choisis l'organisation de la mission : commanditaire, auditeur (interne / externe), responsables interviewés.
- Si le choix porte sur un cabinet externe, **je choisis une société indépendante de l'infrastructure de la société de gestion**.
- J'organise des débriefings des résultats avec les responsables rencontrés puis une présentation des constats et recommandations à l'organe de gouvernance de la société et au comité concerné (par exemple "risque opérationnel" ou "sécurité").
- **J'inclus les recommandations dans le plan de remédiation** suivi par l'audit interne ou la Conformité, avec des priorisations et des délais.

Interlocuteurs	Direction générale, Audit Interne, Conformité / Déontologie, Directeurs métiers, Directeur risques, RSSI
Points de contrôle	Rapport d'audit (synthétique et détaillé), éléments justificatifs, support de présentation à l'organe de Direction, liste des recommandations validées

Pour aller plus loin !

1) Mettre en place un dispositif de supervision des événements de sécurité

Afin d'améliorer la prévention et la détection de comportements anormaux sur le SI de la société de gestion, celle-ci a intérêt à mettre en place un SOC *(Security Operation Center)*, service interne ou externe transmettant des alertes, à partir de l'utilisation d'outils :

- DLP *(Data Loss Prevention)* : alertes et blocages de comportements vis-à-vis de fuite de données ;
- SIEM *(Security Information Event Management)* : centralisation et analyse de corrélations des logs ou des actions constatées sur les différents composants du SI.

- Au vu des résultats et des tests d'intrusion et de l'audit (*cf.* points précédents dans ce chapitre), je détermine avec la DSI, et si besoin est avec une aide externe, le type d'outils et de services le plus adapté :
  - pour une société de gestion de taille modeste, je regarde les solutions externes (SOC sur le SI, alertes "de Place") ;
  - pour une société de gestion intégrée à un groupe, je cherche à mutualiser les services et les outils ;
  - pour une grande société de gestion, j'analyse l'opportunité d'une solution interne (outil SIEM, équipe SOC).
- Dans tous les cas, **j'organise le dispositif d'exploitation** : réception quotidienne des alertes, analyse des impacts, mesures urgentes de sécurisation, mesures de remédiation à moyen terme.
- **J'intègre les résultats des alertes dans un tableau de bord** à destination de la DSI, du RSSI et du comité en charge de la sécurité du SI.

Interlocuteurs	RSSI, DSI, RSSI, prestataires externes, éditeurs de logiciels
Points de contrôle	Dossier d'étude préalable, dossier de choix de la solution / outil, dispositif d'exploitation des alertes, tableau de bord synthétisant les alertes et leurs impacts

CHAPITRE 3 / POSTES DE TRAVAIL

Par où commencer ?

L'utilisateur plus ou moins au fait des bonnes pratiques de sécurité informatique est, dans de très nombreux cas, la première porte d'entrée des attaquants vers le système. Il est donc fondamental de mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique de l'entité (postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc.). L'implémentation des mesures suivantes est proposée pour sécuriser le poste de travail.

1) Mettre à jour les systèmes d'exploitation et les applications installées sur le poste de travail

Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors des mises à jour de sécurité. En absence de déploiement de mises à jour, les attaquants peuvent exploiter ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

- **Je définis et je fais appliquer une politique de mise à jour régulière** :
  - s'il existe un service informatique au sein de l'entreprise, il est chargé de la mise à jour du système d'exploitation et des logiciels ;
  - s'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du chef d'entreprise.

Interlocuteurs	Direction informatique
Points de contrôle	Politique de mise à jour des postes de travail, vérification manuelle sur un échantillon de postes

2) Antivirus

L'objectif ici est de disposer sur tous les postes de travail (et serveur) d'un antivirus à jour afin de limiter la propagation de codes malveillants.

- **J'installe sur tous les postes de travail** de mon entreprise **un antivirus** et je m'assure qu'il est **mis à jour régulièrement**.

Interlocuteurs	Direction informatique
Points de contrôle	Vérification manuelle sur un échantillon de postes

Actions à court terme

1) Chiffrement des disques sur les équipements mobiles / nomades

Les équipements mobiles peuvent contenir des données d'entreprise sensibles et sont par définition amenés à être transportés. Une perte / vol d'un équipement mobile peut entraîner l'accès et le vol de ces données sensibles et constituer un point d'entrée vers de plus amples ressources du système d'information.

- **Je chiffre** les disques durs des équipements mobiles.
- **Je sensibilise** mes utilisateurs à l'utilisation de ces équipements nomades lors de leurs déplacements.
- **Je banalise ces équipements nomades** tant que c'est possible en évitant toute mention explicite de l'entité d'appartenance (par l'apposition d'un autocollant aux couleurs de l'entité par exemple).

Interlocuteurs	Direction informatique
Points de contrôle	Vérification manuelle sur un échantillon de postes

2) Gestion centralisée des habilitations

Afin de faciliter l'attribution d'une action sur le système d'information en cas d'incident ou d'identifier d'éventuels comptes compromis, la gestion des habilitations doit être centralisée.

- J'utilise des comptes **nominatifs** et **individuels**.
- Je limite au strict minimum l'utilisation des compte génériques *(exemples : admin, guest, user...)*.
- Je centralise la gestion des habilitations *(exemple : Active Directory sur Windows)*.
- Je ne donne pas par défaut des droits administrateurs aux utilisateurs.

Interlocuteurs	Direction informatique
Points de contrôle	Vérification des habilitations

Actions à moyen terme

1) Mettre en place des règles de durcissement

Les postes de travail achetés ne sont pas, par défaut, sécurisés. Il faut donc que l'entreprise procède à une sécurisation de ces postes en phase avec ses exigences de sécurité.

L'objectif de cette phase est de s'assurer que les postes de travail de l'entreprise ont tous un niveau de sécurité minimal acceptable.

- Je retire les droits administrateurs des utilisateurs et je limite l'utilisation de ces comptes à privilège aux personnes habilités (équipe informatique principalement).
- Je m'assure que le poste de travail a un antivirus à jour, un pare-feu (quand c'est possible), et qu'il est mis à jour régulièrement.
- Je retire les applications non nécessaires installées par défaut.
- Je bloque l'utilisation des ports USB.

Interlocuteurs	Direction informatique
Points de contrôle	Politique de durcissement, vérification manuelle sur un échantillon de postes

Pour aller plus loin !

1) Mettre en place un MDM *(Mobile Device Management)*

Les terminaux fournis par l'entité et utilisés en contexte professionnel doivent faire l'objet d'une sécurisation à part entière, dès lors qu'ils se connectent au système d'information de l'entité ou qu'ils contiennent des informations professionnelles potentiellement sensibles (mails, fichiers partagés, contacts, etc.).

- J'utilise une **solution de gestion centralisée des équipements mobiles**. Il sera notamment souhaitable de configurer de manière homogène les politiques de sécurité inhérentes : moyen de déverrouillage du terminal, limitation de l'usage du magasin d'applications à des applications validées du point de vue de la sécurité, etc.
- En fonction du besoin de l'entreprise, l'utilisation d'une application sécurisée tierce pour accéder à ses emails par exemple peut être envisagée.

Interlocuteurs	Direction informatique
Points de contrôle	Solution de MDM

2) Cloisonner les usages professionnels / personnels *(byod – Bring Your Own Device)*

Les ordiphones et tablettes font partie de notre quotidien personnel et / ou professionnel.

- La première des recommandations consiste justement à **ne pas mutualiser les usages personnel et professionnel sur un seul et même terminal.**
  Ou bien de s'assurer que **le cloisonnement est bien effectif** entre les deux usages.

CHAPITRE 4 / APPLICATIONS ET SERVEURS

Par où commencer ?

1) Mettre à jour les OS et services majeurs

Les mises à jour du système d'exploitation, des logiciels métiers et des dispositifs de protection constituent le premier rempart de protection en matière de sécurité.

- Je définis une **politique de mise à jour régulière** des correctifs du système d'exploitation et des failles de sécurité qui soit centralisée si possible.
- Je règle le pare-feu de manière à **limiter les flux** d'entrée/sortie en fonction de la politique de filtrage de l'entreprise.
- Je mets en œuvre les **correctifs applicatifs** concernant les bugs dangereux et/ou problèmes relevés dans les versions antérieures. Si possible, j'effectue la mise à jour sur quelques machines avant d'intervenir sur le parc complet.
- J'évite **l'obsolescence** et reste en phase avec l'éditeur en intégrant les améliorations techniques et fonctionnelles proposées. Je connais les systèmes d'exploitation utilisés et j'anticipe les évolutions.
- Je recherche la **compatibilité** avec d'autres logiciels et protocoles.

Interlocuteurs	DSI

Points de contrôle	Tableau de bord des évolutions d'OS, scans de vulnérabilité

2) Antivirus

L'antivirus agit comme une surcouche de protection contre les failles de sécurité et les tentatives d'infection.

- Je mets en place une **architecture centralisée** de mises à jour et d'alertes.
- J'applique en **temps réel** les **mises à jour** proposées afin :
  - de limiter l'exploitation des failles résiduelles,
  - d'éviter l'expansion des menaces sur le réseau interne,
  - de prévenir le lancement automatique de code malveillant.

Interlocuteurs	DSI

Points de contrôle	Vérifier que les antivirus disposent de la dernière version des bases de signatures virales ou comportementales, s'assurer que l'exhaustivité des serveurs est à jour

Actions à court terme

1) Habilitation des administrateurs sur l'OS

L'administration du SI et des logiciels métiers est confiée à un nombre limité d'utilisateurs disposant de privilèges spécifiques. Il convient donc de **maîtriser le périmètre des actions effectuées par ces comptes à hauts risques**.

- Je limite le rôle du compte "Administrateur" par défaut.
- Je change la description et le nom du véritable compte d'administration.
- Je limite le nombre des comptes d'administration.
- Je préfère les comptes d'administration nominatifs aux comptes génériques toujours plus difficiles à tracer.
- Je limite les droits d'administration au strict nécessaire.

Interlocuteurs	DSI, Conformité / Déontologie, RSSI
Points de contrôle	Vérification périodique de la matrice des habilitations

2) Protection physique des locaux techniques

L'accès aux locaux techniques doit être strictement limité et contrôlé afin d'éviter les intrusions malveillantes.

- Je mets en place des **protections physiques et/ou électroniques** robustes pour les accès aux salles techniques.
- Je liste les différentes **catégories de personnel autorisées** (informaticiens, pompiers, gardiens...).
- Je **contrôle** et **trace** les **accès** des personnes physiques.

Interlocuteurs	DSI, Direction de la sécurité, Conformité / Déontologie, RSSI
Points de contrôle	Vérification périodique de la liste des accréditations

Actions à moyen terme

1) Mettre en place des règles de durcissement

Le durcissement consiste à renforcer les règles de sécurité du système d'exploitation afin d'améliorer la robustesse de la configuration.

- Je crée des mots de passe longs, complexes et non cycliques.
- Je désactive les services réseaux souvent inutilisés (NetBIOS, IPv6, assistance IP,...).
- J'active et je configure le pare-feu local du serveur.
- Je restreins les droits des utilisateurs (penser à interdire l'accès des serveurs aux utilisateurs).
- Je sécurise le *"boot"* (démarrage) des machines.

Interlocuteurs	DSI, RSSI

Points de contrôle	Lister périodiquement les règles en vigueur sur le pare-feu des machines

Pour aller plus loin

1) Habilitations sur les applications

Les métiers supposent d'attribuer des rôles à chacun des collaborateurs. Les applicatifs doivent refléter ces rôles et limiter les domaines d'intervention au strict nécessaire.

- J'applique un droit strictement limité au rôle de l'utilisateur afin d'éviter "l'abus de pouvoir".
- J'attribue le privilège "nécessaire et suffisant" pour que les utilisateurs effectuent les actions dont ils ont la responsabilité.
- Je trace les demandes de changements d'habilitations.

Interlocuteurs	Directions métiers, Audit interne, Conformité / Déontologie, Direction des risques, RSSI
Points de contrôle	Vérification périodique de la liste des accréditations et des modifications des accréditations

2) Réaliser des audits systématiques sur les applications sensibles

L'audit des applications permet de s'assurer de l'adéquation des pratiques et des règles en vigueur en regard des évolutions des logiciels et du matériel.

- Je fais auditer les tentatives de lancement des applicatifs les plus sensibles.
- Je qualifie la sécurité des nouveaux matériels impliqués dans les chaînes de traitement.
- J'analyse les remontées d'alertes de sécurité et d'incidents.
- Je liste les comptes non utilisés depuis quelques mois ou semaines.
- Je liste les comptes ayant subi des changements d'attributions.

Interlocuteurs	Audit interne, Conformité / Déontologie, Direction métiers, Direction des risques, RSSI
Points de contrôle	Rapport d'audit

CHAPITRE 5 / ÉCHANGE DE DONNÉES ET ACCÈS INTERNET

Par où commencer ?

1) Enregistrement des logs d'accès à internet

L'enregistrement des logs d'accès à internet permet d'avoir une piste d'audit dans le cas d'une attaque malveillante mais également en cas de réquisition judiciaire. En cas de fuite de données les logs peuvent aider pour remonter à la source de la fuite.

- Je mets en place un enregistreur de trace des accès internet.

Interlocuteurs	RSSI, DSI
Points de contrôle	Vérification de la bonne écriture des logs ainsi que de leur contenu

Actions à court terme

1) Mettre en place des règles de filtrage sur les sites internet présentant un risque (juridique ou malveillance)

Beaucoup d'informations circulent sur internet. Il existe une multitude de sites permettant l'échange d'information. Néanmoins, beaucoup de sites sont susceptibles d'apporter un danger pour l'entreprise. Le filtrage permet de bloquer en amont les sites malveillants et présentant un risque juridique, RH ou de sécurité.

- Je définis une **politique de filtrage**.
- **Je mets en place un proxy** afin de bloquer les sites dangereux ou non conformes à la politique de la société.
- Je bloque les sites malveillants.
- Je bloque les sites de partage d'information grand public (webmail, partage de documents, etc.).

Interlocuteurs	RSSI, DSI
Points de contrôle	Vérification des sites bloqués

2) Mettre en place un anti-spam

Les méthodes utilisées par les *hackers* sont de plus en plus précises. L'envoi de mails en masse est remplacé par du hameçonnage plus spécifique où le corps du mail est travaillé de façon à augmenter sa crédibilité. La mise en place d'un anti-spam n'exclut pas de former les employés de l'entreprise à tout l'univers du *phishing* mais c'est un premier rempart qu'il ne faut pas négliger.

- **Je mets en place un anti-spam** afin de minimiser la surface d'attaque par de potentiels assaillants.
- **Je mets en place un antivirus mail** sur la messagerie.
- **Je forme les employés** afin qu'ils soient sensibilisés à la détection des mails frauduleux.

Interlocuteurs	RSSI, DSI
Points de contrôle	Vérification de la bonne réception des mails bien notés et du rejet des mails mal notés

Actions à moyen terme

1) Tenir un inventaire des points d'accès distants

Afin d'éviter toute faille de sécurité il est important de savoir quels sont les points d'accès au système. En cas de connaissance d'une vulnérabilité sur un type d'accès, il est ainsi plus facile de bloquer cet accès le temps de trouver une solution.

- Je construis **une cartographie des points d'accès distants par criticité**.
- Je m'assure de pouvoir agir en cas de compromission d'un point d'accès.

Interlocuteurs	RSSI, DSI
Points de contrôle	Vérification de la cartographie de façon régulière, vérification du fonctionnement du plan d'action, test régulier du niveau de sécurité

2) Mettre en place une authentification forte sur les accès à distance

Une authentification double voire triple facteurs peut être mise en place afin d'avoir accès à distance au SI. En cas de perte de matériel, si une double / triple authentification est en place, il sera plus compliqué pour une personne mal intentionnée d'utiliser le matériel perdu. L'utilisateur ne maîtrise pas toujours l'environnement dans lequel il se trouve.

- Je mets en place un **système d'authentification multi facteur**. Suivant le degré de confidentialité, le niveau du système peut être plus ou moins élevé.
- Je forme les collaborateurs sur les risques encourus en cas de perte de ses identifiants.

Interlocuteurs	RSSI, DSI
Points de contrôle	Contrôle du niveau d'authentification des connections existantes

Pour aller plus loin !

1) Mettre en place un cloisonnement réseau pour séparer les réseaux bureautiques et serveurs

Le cloisonnement permet de découper un environnement en plusieurs parties ne comportant pas les mêmes éléments et n'ayant pas les mêmes droits. Cela permet de limiter la compromission générale car si une sous-partie est compromise, la propagation sera moindre du fait des droits restreints de la sous-partie.

- Je définis le cloisonnement de mon réseau en identifiant les zones sensibles.
- Je renseigne les permissions de chaque sous-réseau.
- Je cloisonne les applications en fonction de leur activité.
- Je mets en place le cloisonnement.

Interlocuteurs	RSSI, DSI
Points de contrôle	Tester le cloisonnement par une simulation d'attaque ; revue des matrices de flux

CHAPITRE 6 / SENSIBILISATION

Par où commencer ?

1) Les sources incontournables

La sensibilisation est un élément clé de la stratégie de la cybersécurité. Rien ne sert d'avoir de bonnes solutions de sécurité si les collaborateurs n'ont pas compris leur rôle pour se protéger et protéger les actifs de la société.

La sensibilisation a donc pour but de faire prendre conscience à l'ensemble des collaborateurs de l'importance de leurs actions dans ou hors de la société. Notamment la sensibilisation doit leur permettre de comprendre les risques et de reconnaître les menaces afin d'adopter un bon comportement et le cas échéant d'y répondre de façon appropriée.

Il suffit souvent de transposer dans la vie réelle ce qui est fait dans le monde de la cyber pour comprendre les risques qui sont pris.

De nombreux guides autour de la sensibilisation existent sur Internet : fiches pratiques, infographies, MOOC, vidéos, conférences, etc. Ces informations sont accessibles à tous et peuvent permettre de décliner au sein de son organisation les bonnes pratiques en termes de cybersécurité : c'est le cas notamment du *Mois européen de la cybersécurité* qui a lieu tous les ans en octobre. De nombreux événements ont lieu partout en France et en Europe sur le thème de la cybersécurité.

On trouvera notamment au sein de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) un certain nombre de documentations qui pourraient être utilisées. Enfin, l'AFG met à disposition sur son site internet, un ensemble de fiches en libre accès pour tous les membres de l'association.

- ANSSI : https://www.ssi.gouv.fr
  http://www.ssi.gouv.fr/administration/bonnes-pratiques/
  https://www.secnumacademie.gouv.fr/ (MOOC)
  https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/
  https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2018/boite-a-outils/
- AFG : https://www.afg.asso.fr/ (accès "membre")
  https://www.afg.asso.fr/publications/fiches-thematiques-de-lafg/
  (fiches pédagogiques Cybersécurité)
- CIGREF : https://www.hack-academy.fr/home (campagne de prévention grand public lancée par le Club Informatique des Grandes Entreprises Françaises)

Interlocuteurs	Ensemble des collaborateurs, DSI, Direction générale, RH (plan de formation), Communication

Points de contrôle	Nombre de communications faites au sein de son organisation, sondages, news, tests de *phishing*, etc.

Actions à court terme

1) Un bon mot de passe

Un mot de passe est un moyen d'authentification, c'est-à-dire un moyen qui permet de prouver que je suis bien celui qui se connecte. Les moyens d'authentification peuvent être différents suivant la sensibilité de l'application accédée.

Un bon mot de passe doit respecter un certain nombre de critères de sécurité pour se connecter sur des ressources sensibles ou non sensibles.

Le mot de passe est secret et il ne doit pas être communiqué, ni à l'écrit, ni à l'oral.

- Si je reçois mon mot de passe par mail, je dois impérativement le changer à la première utilisation.
- Je dois également le changer régulièrement et dès lors que je suspecte une compromission.
- Afin que je puisse me protéger des différentes attaques "de force brute" ou "au dictionnaire", **il convient de respecter la robustesse de mon mot de passe** en utilisant au moins :
  - des lettres (majuscule + minuscule)
  - des caractères numériques
  - 1 ou plusieurs caractères spéciaux
  - une longueur adéquate (au moins 12 caractères)

De plus,

- Je mets en place des moyens mnémotechniques afin de faciliter l'apprentissage du mot de passe.
- **J'utilise un mot de passe différent par site.**

Un bon mot de passe est un mot de passe adapté à la sensibilité de l'actif auquel il doit accéder. Pour des actifs sensibles ou des comptes à privilèges, on sera également amené à faire le choix de mots de passe à usage unique (*One Time Password* – OTP)

Interlocuteurs	Ensemble des collaborateurs, Équipe DSI, Équipes applicatives
Points de contrôle	Couverture de l'activation d'un mot de passe, vérification de la robustesse d'un mot de passe par des tests

2) Se protéger du *phishing*

Le *phishing* – ou hameçonnage en français – est une pratique très répandue qui vise à piéger un utilisateur en lui adressant un mail pour récupérer ses accès via un lien malveillant ou une pièce jointe malveillante. 9 attaques sur 10 commencent pas un mail de ce type.

- Je dois respecter un certain nombre de bonnes pratiques afin de me prémunir d'un éventuel *phishing*.
- Pour cela, je mets en place des recommandations auprès des utilisateurs pour mieux détecter les *phishing*.

Il est utile de rappeler aux utilisateurs de bonnes pratiques lors de la réception d'un mail :

- Je prends un moment pour me demander : si je dois recevoir ce type de mail, ou si j'ai déjà reçu ce genre de message avant.
- Je regarde l'émetteur : son adresse complète, avec le domaine d'où il provient.
- Je cherche les erreurs d'orthographe, les signatures suspectes.
- Je vérifie le ton et le sujet du mail : les *phishing* sont souvent inquiétants, alarmistes, menaçants ou pressants en demandant une action rapide.
- **Si j'ai le sentiment que le seul moyen d'en savoir plus sera de cliquer sur le lien ou d'ouvrir le document, je ne le fais pas** et j'alerte les équipes sécurité afin qu'elles puissent faire des analyses et bloquer l'expéditeur si besoin.

Interlocuteurs	Équipe DSI, Conformité / Déontologie

Points de contrôle	Lancement de tests de campagne de *phishing* via des sociétés spécialisées comme par exemple *Getgophish*, *Lucysecurity*, *Insight*, *Wombatsecurity*, etc.

Actions à court terme (suite)

3) Incident de sécurité : qui contacter ?

Cette mesure fait référence à la mesure “Processus de gestion des incidents” du chapitre 1 / Gouvernance.

- Suivant la structure de ma société de gestion, lorsque je détecte un incident, **je définis qui contacter en cas d’incident** : cela peut être mon manager, mon équipe sécurité, la conformité, notamment dans le cadre de fuite d’information.
- **Pour cela je dois définir ce qu’est un incident de sécurité.** Cela peut être :
  - une fuite d’information ou la divulgation d’information ;
  - une usurpation d’identité (utilisation illégale de mots de passe, usurpation d’identité ou abus de droits) ;
  - une intrusion ou tentative d’intrusion pour exploiter des failles de sécurité ;
  - un piratage ciblé des postes de travail et vol de données ;
  - un virus / *malware* (exemples : chiffrement des données avec demandes de rançons, utilisation de la machine pour d’autres attaques…) ;
  - etc.
- **À chaque catégorie d’incident, j’associe un plan de réaction** qui va me permettre de répondre à chaque situation et qui doit notamment me permettre d’identifier la sévérité de l’incident et d’adapter ma façon de répondre, laquelle peut aller jusqu’à une gestion en mode crise. Je mets en place des tests pour m’assurer que les plans de réaction sont connus et appliqués.

Interlocuteurs	Conformité / Déontologie, DSI, DPO, Sécurité
Points de contrôle	Diagnostic et résolution des incidents

Actions à moyen terme

1) Entraîner les utilisateurs via un faux *phishing*

L'objectif du test faux *phishing* n'est pas de piéger les utilisateurs, mais de leur montrer, par l'intermédiaire de cet outil, les risques auxquels ils sont exposés de manière permanente à cause du non-respect de règles comportementales en matière de sécurité de l'information.

- Afin d'entraîner les utilisateurs via un faux *phishing*, je commence par établir une campagne de *phishing* en mettant en œuvre :
  - une cible (en définissant ma population) ;
  - un message ou scénario spécifique (typologie d'email malveillant : peu crédible, crédible) ;
  - une date et une heure d'envoi : période à laquelle mon message partira.

2) Mesurer le niveau de maturité

Les statistiques obtenues suite à une campagne vont me permettre de mesurer le niveau de maturité de mon entité, d'adapter les campagnes de sensibilisation à implémenter en fonction des résultats et de classer les populations visées suivant leur niveau en matière de cyberattaques.

- Valider les bonnes pratiques de votre entreprise face au *phishing*.
- Connaître l'attitude de vos salariés face à des emails non légitimes, les invitant à saisir leurs identifiants.

Interlocuteurs	DSI, Communication, Représentants du personnel

Points de contrôle	Nombre de personnes piégées / nombre de personnes ciblées ; nombre de personnes ayant donné l'alerte

Pour aller plus loin !

1) *Serious games*, simulation d'attaque "réelle" (piégeage de téléphone, site malveillant, *Red Team*, etc.)

- Je peux **renforcer les actions de sensibilisation** en mettant en place notamment des *serious games* qui mettent les collaborateurs dans une situation réelle : le collaborateur jouera alors son propre rôle ou le rôle d'une personne malveillante.

  Des *escapes games* permettent également de montrer de façon ludique une approche de la sensibilisation sur la cybersécurité.

- Je peux **organiser des tests de cellules de crise** afin de m'assurer que les comportements et les réactions de la direction et/ou des collaborateurs sont en adéquation avec les attentes : cela peut être une simulation d'attaque virale type rançongiciel, un déni de service, etc.

- Enfin, je peux **tester mes équipes de sécurité** en faisant appel à une *Red Team* qui testera les mesures de sécurité et mettra tout en œuvre afin d'atteindre l'objectif qui lui a été assigné (on parle de "trophée") : vol d'informations, mise en place de code malveillant, intrusion dans les systèmes. Ces experts spécialisés pourront aller jusqu'au piégeage par téléphone ou l'utilisation de faux sites malveillants pour piéger les utilisateurs et les sensibiliser au risque.
  Cette action permettra de valider le niveau de robustesse du dispositif de sécurité de votre société mais également de vous assurer que les moyens d'*alerting* et de surveillance sont opérationnels (on parle souvent de *Red Team versus Blue Team*).
  Dans tous les cas vous découvrirez les points forts et potentiellement les points à améliorer au sein de votre entité.

Interlocuteurs	Direction informatique, Production informatique, Équipe de support informatique, Équipe de développement, Équipe de réponse à incident
Points de contrôle	Résultat au test, nombre de vulnérabilités détectées/exploitées

LEXIQUE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DPO	*Data Privacy Officer* / Délégué à la Protection des Données
DRH	Direction des ressources humaines
DSI	Directeur / Direction des Systèmes d'information
IT	*Information Technology*
MDM	*Mobile Device Management* / Solution de gestion des appareils mobiles (configuration / sécurité)
OS	*Operating System* / Système d'exploitation
OTP	*One Time Password* / Mot de passe valable une seule fois
Parefeu	Équipement réalisant un filtrage des connexions réseau
PCA	Plan de continuité d'activité
Proxy	Équipement réalisant une rupture de flux pour contrôler l'accès à Internet
RCCI	Responsable Conformité et Contrôle Interne
RSSI	Responsable de la Sécurité des Systèmes d'Information
SIEM	*Security Incident and Event Management* / Système de centralisation des données de sécurité
SOC	*Security Operation Center* / Centre d'opération sécurité
SSI	Sécurité des Systèmes d'Information

L'AFG remercie les membres du Groupe de travail Cybersécurité qui ont participé à l'élaboration de ce Guide, et en particulier son président Wilfried LAUBER (AXA Investment Managers Paris).

Le Groupe de travail Cybersécurité est rattaché à la Commission Déontologie et Conformité présidée par Monique DIAZ (AXA Investment Managers Paris).

Valentine BONNET, Directrice Gouvernement d'entreprise et Conformité (AFG), a coordonné ces travaux.

41 rue de la Bienfaisance I 75008 Paris I Tél. +33 1 44 94 94 00
45 rue de Trèves I 1040 Bruxelles I Tél. +32 2 486 02 90
@AFG_France I www.afg.asso.fr

AFG
41 rue de la Bienfaisance
75008 Paris
T: +33 1 44 94 94 00

@AFG_France

45 rue de Trèves
1040 Bruxelles
T: +32 2 486 02 90

www.afg.asso.fr

association française de la gestion financière