Protection de L'Information

KPMG France

Un élément des
Règles Globales de Sécurité de l'Information

Mars 2018

Sommaire

1 Introduction

KPMG[1] considère ses informations, celles de ses clients, et son système d'information comme des biens précieux. Ces biens sont fondamentaux pour l'activité de KPMG et sont conservés et protégés comme tels. KPMG considère qu'il est important de protéger l'information contre des menaces en évolution permanente et travaille continuellement à améliorer les programmes de protection de l'information[2] déjà en place.

KPMG adopte une approche holistique de la protection de l'information, impliquant des mesures techniques (basées sur des règles et standards techniques ou de sécurité) et des mesures non techniques (basées sur les référentiels mondiaux de KPMG que sont le "Manuel de Gestion de la Qualité et des Risques", le "Code de Conduite" et les "Règles de Sécurité Informatiques pour les utilisateurs finaux"). Chacun des collaborateurs de KPMG a un rôle à tenir dans la protection de l'information.

Dans ce document, 'systèmes critiques' désigne les systèmes et équipement de stockage de fichiers ou de documents, de gestion interne, de messagerie, les systèmes globaux auxquels les clients ont accès ou qui participent directement à la fourniture d'un service aux clients, tout autre système considéré comme critique par un cabinet membre de KPMG ainsi que les systèmes hébergé par un cabinet membre de KPMG pour son compte ou celui d'un autre cabinet membre dont une indisponibilité supérieure à 5 jours ouvrés aurait un impact élevé sur l'activité de KPMG.

1.1 Le réseau KPMG de cabinets membres

KPMG International Cooperative ('KPMG International' or 'KPMGI') est une entité de droit suisse. C'est à cette entité que tous les cabinets membres du (collectivement désignés par 'KPMG') adhèrent. KPMG International ne fournit aucun service aux clients. Les services sont exclusivement fournis aux clients par les cabinets membres.

KPMGI et les cabinets membres sont des entités légales indépendantes les unes des autres. Aucun cabinet membre ne peut engager KPMGI ou un quelconque autre cabinet membre vis-à-vis des tiers de même que KPMGI ne peut engager aucun cabinet membre.

[1] Dans ce document, 'KPMG', et 'cabinets membres' désigne le résau des cabinets membres indépendants exerçant sous le nom KPMG et adhérant à KPMG International Cooperative ('KPMG International'), ou à une ou plus de ces entités. 'Règles globales' désigne les règles de KPMG International. KPMG International est une entité de droit. KPMG International ne fournit aucun service aux clients. Les services sont exclusivement fournis aux clients par les cabinets membres.

[2] A travers ce document, 'information protection' doit englober tout ou partie des éléments suivants: risque et sécurité de l'information, protection des données, confidentialité des données, confidentialité du client, sécurité de l'information.

2 Conception de la protection de l'information

La protection de l'information a toujours été une priorité pour KPMG, et est devenue désormais l'un des éléments les plus importants des programmes technologiques de KPMG. La protection de l'information est au cœur même des développements informatiques et des activités métiers de KPMG.

L'utilisation croissante de fonctionnalités d'analyse de données, d'intelligence artificielle, de processus automatisés et d'autres fonctionnalités digitales font que les données sont en permanence au cœur de l'activité de KPMG. Les données sont à la fois un atout essentiel pour la croissance de KPMG et un outil mis au service de ses clients pour résoudre des problématiques métiers complexes. Compte-tenu de ce rôle essentiel, il est primordial que le maintien d'un niveau de sécurité stable prenant en compte les évolutions liées à l'utilisation de services cloud ou mobiles fasse partie des priorités de KPMG.

KPMG ayant la responsabilité d'assurer la sécurité de ses données et de celle de ses clients, a défini des règles (par exemple les règles globales de protection de l'information), établi un Centre Opérationnel de Sécurité Global (GSOC) ainsi que d'autres services de sécurité et est tenu par ses obligations contractuelles. Ces dispositions sont les éléments fondamentaux mis en œuvre par KPMG pour accompagner ses équipes dans la fourniture de services à ses clients. KPMG planifie ses actions de protection de l'information pour assurer le respect de ses obligations et tirer le meilleur profit des services de sécurité fournis notamment par le GSOC.

2.1 Une approche basée sur 4 piliers

KPMGI a adopté une approche selon 4 piliers, commençant par la prévention des menaces, passant par nos facultés à détecter et réagir aux incidents et conduisant à notre amélioration par le biais de la prédiction de l'évolution des menaces. Ces 4 piliers sont présentés ci-après.

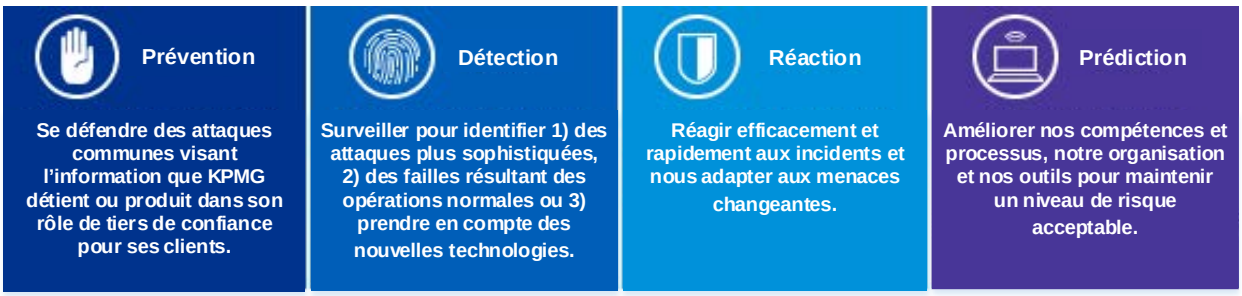

Figure 1: Les 4 piliers

2.1.1 Prévention

— **Une protection contre les attaques ciblées** est mise en œuvre sous la forme d'un service externalisé de filtrage de contenu.

— **Un service global de gestion des firewalls** (MSFS) est opéré par le GSOC.

— Les **Règles et Standards de Sécurité** sont alignés sur ISO 27000.

— **Certification ISO 27001:** certains cabinets membres sont certifiés ISO 27001 et l'extension de la certification à d'autres cabinets membres et à KPMGI est prévue.

2.1.2 Détection

— **Surveillance de la Sécurité dans le Cloud**, analyse comportementale et surveillance des applications clés (services fournis par le GSOC).

— Extension des détections automatiques de vulnérabilités aux équipements des réseaux internes des cabinets membres.

— Développer le périmètre du GSOC en activant **la surveillance des sessions internet et utilisateurs** via MSFS et mettre en œuvre une surveillance continue pour mieux assister les cabinets membres dans l'administration de leurs environnements techniques.

2.1.3 Réaction

— **Processus Global de Gestion des Incidents de Sécurité** et organisation de simulations de cyber-attaques.

2.1.4 Prédiction

— Analyse des menaces et veille permanente basées sur des sources interne et externes.

— Suivi des profils de risques opérationnels et techniques des cabinets membres.

3 Protection de l'Information

3.1 Organisation

3.1.1 KPMG International

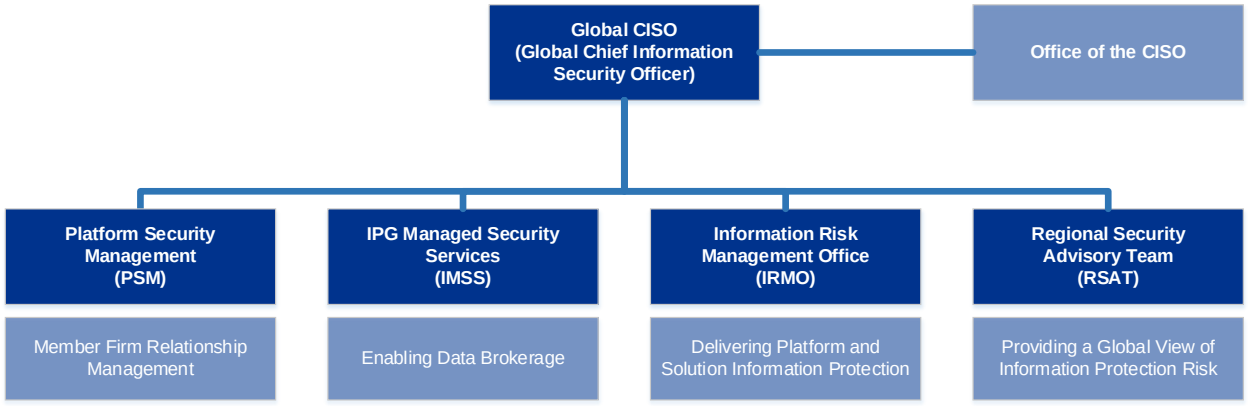

Figure 2: KPMG International — Global Information Protection Group (IPG)

Le « Global Information Protection Group » (IPG) de KPMG International dépend du « Global Chief Information Security Officer » (Global CISO), et informe un comité global de gouvernance des risques ainsi qu'un comité global de pilotage des systèmes d'information. Le premier comité est constitué par des représentants des équipes de sécurité de l'information et des représentants des équipes de gestion des risques professionnels de KPMG. Ce comité est l'approbateur final des règles de sécurité de l'information et supervise un programme de conformité validant l'efficacité des contrôles mis en œuvre. Dans le cas où une règle de sécurité concernerait une technologie spécifique ou de manière plus générale la stratégie informatique, l'approbation du comité global de pilotage des systèmes d'information est également requis.

Ce comité global de pilotage des systèmes d'information comprend des CISOs représentant les cabinets membres les plus importants et des responsables informatiques internationaux. Si l'approbation initiale des exigences de sécurité de l'information dépend du comité global de gouvernance des risques décrit plus haut, l'approbation des standards techniques de sécurité et d'architecture en découlant est du ressort de ce comité de pilotage des systèmes d'information, également responsable de la supervision de la gestion des incidents de sécurité de l'information.

Le « Global Head of Technology and Knowledge » informe régulièrement une équipe de direction générale dépendant du « Global Board » de KPMGI. Le « Global Chairman » de KPMGI a demandé à chaque cabinet membre de prendre en compte l'importance de la protection de l'information et a approuvé un programme visant à développer les initiatives de sécurité, faisant ainsi preuve de l'engagement de KPMGI à renforcer les mesures de sécurité contre des menaces en évolution permanent et à développer la sensibilisation à ces sujets des instances dirigeantes des cabinets membres.

Les règles de sécurité globales stipulent que les rôles clés au sein des départements informatiques doivent

être isolés de telle sorte qu'un individu ne puisse à lui seul concevoir, développer et mettre en œuvre une modification d'un système informatique. Lorsque cette séparation ne peut être mise en œuvre, des contrôles compensatoires sont requis.

IPG définit avec de nombreuses parties prenantes les règles et procédures globales de sécurité de KPMGI et entretient un programme global de conformité de la sécurité de l'information. Si IPG définit les standards minimum à respecter dans le réseau de cabinets membres, il est de la responsabilité des équipes de sécurité de chaque cabinet membre d'assurer la conformité au niveau de ses collaborateurs.

Le programme de protection de l'information de KPMGI est basé sur un ensemble cohérent de règles, standards et recommandations de sécurité basés sur ISO 27000. De plus amples détails sont fournis au paragraphe 3.2 (Règles de sécurité).

3.1.2 Cabinets membres

Chaque cabinet membre doit désigner un « National IT Security Officer » (NITSO) faisant office de contact principal pour les questions de sécurité de l'information agissant en coordination notamment avec les départements en charge de la sécurité physique, du juridique, de la gestion des risques, de la protection des données personnelles. Le NITSO est le point de contact principal entre KPMGI et le cabinet membre pour les sujets de protection de l'information.

Les schémas suivant décrivent les relations entre IPG et les cabinets membres, les services couverts par le programme de protection de l'information ainsi que l'organisation des cabinets membres pour l'informatique et la gestion des risques.

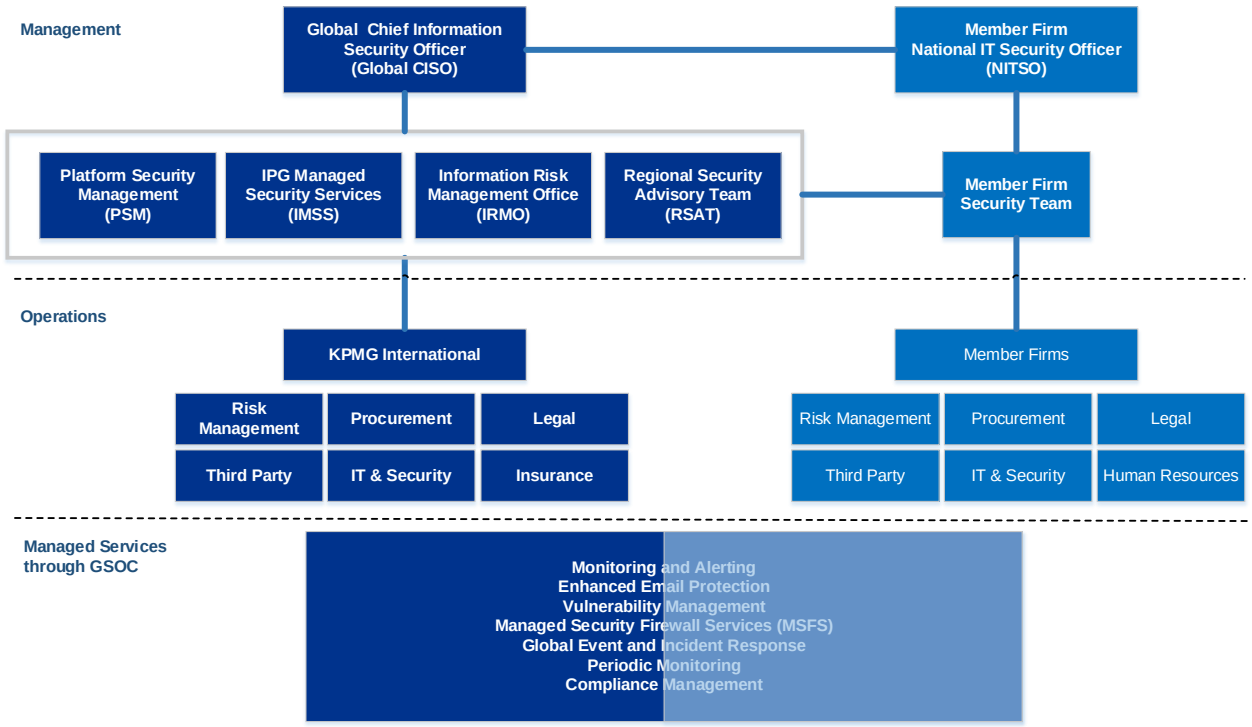

Figure 3: Relations entre IPG et les cabinets membres

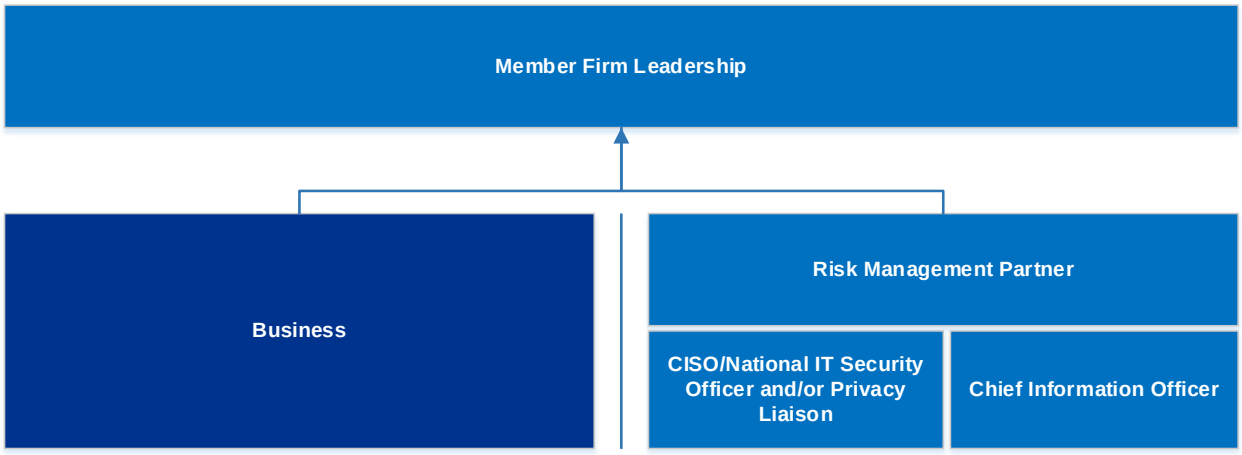

Figure 4: La gouvernance IT des Member firms et structure de la gestion du risque

Certains cabinets membres n'ont pas désigné de « Chief Information Officer ». Dans certains cas, les personnes assurant les rôles de « Risk Management Partner », « CISO/National IT Security Officer » et/ou « Privacy Liaison » peuvent également exercer d'autres rôles au sein du cabinet membre.

3.2 Règles de sécurité

KPMGI publie des règles et standards de sécurité et chaque cabinet membre est en charge de leur application locale, de leur respect et du respect des lois et réglementations locales pouvant s'appliquer. KPMGI, les cabinets membres et leurs personnels doivent se conformer à des règles relatives à l'utilisation des moyens informatiques, à la sécurité de l'information, la protection des données et la confidentialité des clients. Ces règles font l'objet d'une revue régulière et sont modifiées en fonction des besoins.

Les cabinets membres peuvent adopter des règles complémentaires notamment pour assurer la conformité avec des lois et règlements locaux. Dans l'éventualité d'un conflit entre les lois et règlements locaux et les règles de KPMG, la loi locale prévaut. Sauf indication contraire, les règles décrites plus bas reflètent les règles et spécifications de sécurité globales auxquelles les cabinets membres doivent se conformer à minima. Dans certains cas, il peut exister des exceptions. Ces exceptions sont soumises à un processus formel d'autorisation comprenant une analyse de risque, et l'évaluation du contexte et des mesures compensatoires.

Les règles de sécurité de KPMG sont communiquées aux membres de son personnel par l'intermédiaire de différents moyens comme l'intranet, les formations annuelles obligatoires et la procédure annuelle de confirmation d'indépendance et de respect des règles éthiques.

3.2.1 Règles de sécurité informatique pour les utilisateurs finaux

La politique d'utilisation autorisée (Global Acceptable Use Policy / AUP) décrit le comportement qui est attendu de la part des membres du personnel de KPMG ou de tiers autorisés lorsqu'ils utilisent les moyens informatiques qui sont mis à leur disposition par KPMG. Les cabinets membres doivent adopter ces règles globales ou mettre en œuvre une politique locale équivalente en respectant à minima toutes les dispositions sauf conflit avec la législation.

Les membres du personnel de KPMG doivent faire preuve de jugement personnel et respecter les principes suivants.

- Les utilisateurs des moyens informatiques de KPMG doivent respecter les lois, règlementations, standards professionnels et l'ensemble des règles de KPMG.
- Les membres du personnel de KPMG ne doivent rien faire qui puisse compromettre la marque KPMG, sa réputation, ses relations avec ses clients ou gêner KPMG ou ses clients.
- Les collaborateurs de KPMG accédant à Internet par des moyens fournis par KPMG ne doivent ni accéder, ni télécharger ni diffuser des contenus illégaux ou inappropriés.
- Les membres du personnel de KPMG doivent, conformément aux règles et usages approuvés, prendre toutes les mesures raisonnables pour protéger les moyens informatiques de KPMG ainsi que les données de KPMG et de ses clients qui sont sous leur contrôle, de tout vol, perte, usage inapproprié, divulgation, modification, duplication, altération et destruction.
- L'information confidentielle de KPMG doit être protégée des accès non autorisés et des divulgations involontaires. Les informations confidentielles ou à caractère personnel ne doivent pas être partagées avec une personne n'ayant pas un motif métier valide de les connaitre. Ceci s'applique à toute forme de communication, orale, écrite ou électronique.
- Les membres du personnel de KPMG doivent respecter les règles de KPMGI relatives à la classification de l'information.
- Il est interdit aux membres du personnel de KPMG d'usurper l'identité d'une autre personne, par quelque moyen que ce soit, dans leurs relations avec d'autres collaborateurs de KPMG, de ses clients ou d'autres tiers.

3.2.2 Règles de sécurité de l'information

Les règles de sécurité de l'information de KPMG sont alignées avec le standard ISO 27000. Elles s'adressent aux responsables des services informatiques et de sécurité, afin d'établir un socle commun de règles et contrôles pour l'ensemble de KPMG.

3.2.3 Confidentialité des clients et protection des données

Les membres du personnel de KPMG et les cabinets membres sont soumis à des règles encadrant l'usage et la divulgation des informations de leurs clients. Ces règles mettent en œuvre les principes établis par le « Code of Ethics for Professional Accountants » publié par l' « International Ethics Standards Board for Accountants » (IESBA). Les cabinets membres de KPMG doivent également se conformer aux législations et règlementations locales ainsi qu'aux standards professionnels applicable à la protection de la confidentialité des informations et données personnelles de leurs clients.

De plus, la Politique de Confidentialité de KPMGI établit les principes minimaux à respecter pour le

traitement des données à caractère personnel. Les cabinets membres doivent adopter cette politique ou mettre en œuvre un politique local équivalente en respectant à minima toutes les dispositions, en accord avec la législation locale. KPMG dispose d'un cadre juridique pour le transfert de données à caractère personnel entre les cabinets membres conforme aux dispositions de la directive UE 95/46/EC et au Règlement Général sur la Protection des Données (RGPD) entré en vigueur en Mai 2018. Les données à caractère personnel des clients peuvent également être soumises à des termes, conditions ou restrictions complémentaires, tels que stipulés dans les conditions d'intervention.

Dans les cas où KPMG travaille avec des tiers, les dispositions adéquates sont incluses dans les contrats, y compris concernant la protection de confidentialité des informations. KPMG peut également être amené à divulguer des informations sur un client lorsque cela est requis par une disposition impérative d'une loi, ou d'une règlementation, y compris dans le cadre d'une citation à comparaître ou similaire.

3.3 Ressources Humaines

KPMG opère des contrôles préalables à l'embauche selon une approche basée sur le risque, conformément à la loi et tenant compte du poste et de la sensibilité des informations à traiter. Les membres du personnel de KPMG sont soumis à une procédure affidavit annuelle incluant un engagement de respect des règles de confidentialité et de sécurité de l'information.

Les règles globales stipulent que les cabinets membres doivent obtenir des membres de leur personnel la confirmation de respect du « Global Code of Conduct » (code de conduite) et du « Global AUP » (politique d'usage autorisé). Les membres du personnel d'un cabinet membre peuvent également avoir à confirmer le respect de règles et politiques locales complémentaires. Le non-respect volontaire ou par négligence flagrante des règles de sécurité par un membre du personnel peut faire l'objet de sanctions disciplinaires.

Les règles globales stipulent également que les cabinets membres doivent appliquer un processus, défini conjointement par le service informatique et le service Ressources Humaines, pour traiter les événements de fin d'emploi ou de changement de responsabilités. En cas de fin d'emploi, les droits d'accès doivent être supprimés ou désactivés dans les meilleurs.

Les cabinets membres doivent se conformer aux dispositions du « Global People, Performance and Culture manual » décrivant les règles, processus et programmes obligatoires en termes de Ressources Humaines.

Les cabinets membres doivent assurer régulièrement la formation de leur personnel aux sujets de la protection de l'information et doivent également entretenir un programme annuel de sensibilisation. Completion of these trainings is mandatory for KPMG personnel. Les politiques et autres documentations pertinentes sont disponibles sur l'intranet de KPMG.

3.4 Gestion des actifs

3.4.1.1 Inventaire des actifs

Les règles globales requièrent que tous les actifs informatiques critiques soient identifiés et répertoriés dans un inventaire tenu à jour et révisé régulièrement. Ces actifs informatiques critiques ont un propriétaire identifié responsable d'en déterminer la classification, l'usage et les accès appropriés et d'en assurer la gestion au cours de son cycle de vie. Un processus de restitution des équipements informatiques et des informations client lors du de la fin d'emploi d'un collaborateur doit être établi conjointement par le service du personnel et le service informatique. Ce processus doit inclure la confirmation écrite par le collaborateur qu'il a bien restitué tous les matériels et informations en sa possession avant de quitter un cabinet membre.

3.4.1.2 Traitement de l'information

Tous les documents créés ou reçus par KPMG doivent être traités conformément aux règles de KPMGI et à leurs niveaux de confidentialité.

3.4.1.3 Rétention

Les cabinets membres doivent établir des processus pour conserver et protéger l'information conformément aux lois, règlementations et standards professionnels applicables, aux exigences relatives à la conservation des documents (par ex. concernant la gestion des litiges ou les enquêtes règlementaires) et aux manuels fonctionnels de KPMGI afférents.

3.4.1.4 Destruction

Les supports contenant des informations sensibles non sujettes à des exigences de rétention ou conservation doivent être recyclés de telle sorte que les informations ne puissent être reconstituées après coup. Les supports contenant des informations sensibles et qui ne peuvent être effacés de manière sécurisée doivent être détruits physiquement.

3.4.1.5 Supports de données

Les supports amovibles contenant des informations de KPMG ou de ses clients doivent être chiffrés (voir également section 3.6 Cryptographie). Les supports utilisés dans le cadre d'une mission doivent être recyclés de manière sécurisée lorsqu'ils ne sont plus nécessaires à l'activité ou aux besoins de rétention. Les medias contenant des informations de KPMG doivent être protégés de manière appropriée (protection par chiffrement et authentification) contre la perte, le vol ou la divulgation involontaire lorsqu'ils sont transportés hors des locaux de KPMG.

3.5 Contrôle d'accès

Les règles globales requièrent que les exigences de contrôle d'accès aux applications soient définies par leurs propriétaires métier selon les principes du besoin d'en connaitre et du moindre privilège (seules les autorisations nécessaires à sa fonction sont attribuées à un utilisateur). La création et l'utilisation de comptes à privilèges sont réduites au minimum.

Les règles globales requièrent également que les connexions réseau à distance soient identifiées, gérées

centralement et protégées par une authentification à double facteur. Le personnel se connectant au réseau de KPMG à distance doit utiliser les solutions approuvées de VPN et une authentification forte à double facteur.

Les serveurs se connectant à des réseaux externes ou accessibles depuis des réseaux externes doivent être isolés logiquement du réseau interne KPMG.

3.5.1 Cabinet membres

Les exigences minimales à respecter par les cabinets membres sont:

- Mise en œuvre d'un processus opérationnel de création/suppression des comptes utilisateurs, incluant des procédures d'autorisation, des contrôles périodiques, et la suppression des comptes redondants ou désactivés.
- Processus de revue périodique des droits d'accès.
- Utilisation d'un identifiant utilisateur unique par chaque personne accédant aux ressources informatiques de KPMG et d'un mot de passe conforme aux exigences de complexité définie par KPMG.
- Définition d'un délai d'inactivité et des mesures de verrouillage associées.
- Les mots de passe doivent respecter des critères de complexité et de longueur minimum.
- Les utilisateurs doivent être en mesure de choisir et changer eux-mêmes leur mot de passe.
- La création et l'utilisation de comptes à privilèges doivent être réduites au minimum. Les collaborateurs nécessitant de tels comptes pour des motifs métiers valides doivent être identifiés explicitement. L'affectation et la révocation des comptes à privilèges doivent être documentés

3.6 Cryptographie

3.6.1 KPMG International et cabinets membres

Les règles globales imposent que les cabinets membres mettent en œuvre des contrôles cryptographiques pour assurer la confidentialité, l'authenticité et/ou l'intégrité de l'information conformément aux règles de Classification de l'Information. Des processus de gestion des clés cryptographiques doivent être définis pour assurer la protection des systèmes de chiffrement contre d'éventuelles compromissions.

3.6.1.1 Services de certificats

KPMGI opère un service global de certificats basé sur les « Certificate Practice Statements » pour les services interne de cryptographie de KPMG. Ce service est consommé par les services informatiques globaux, régionaux et nationaux incluant des services mobiles.

Pour protéger les échanges de messages électroniques entre les cabinets membres et leurs clients, KPMGI propose un service de chiffrement TLS obligatoire. Le chiffrement TLS obligatoire permet de chiffrer tous les messages électroniques depuis les passerelles de messagerie de KPMG jusqu'aux passerelles de messagerie des clients. Lorsque le chiffrement TLS obligatoire n'est pas activé, un chiffrement TLS opportuniste est appliqué assurant ainsi un chiffrement des messages électroniques lorsque cela est possible.

3.6.2 Cabinets membres

Les cabinets membres doivent mettre en œuvre les contrôles cryptographiques suivants.

- Chiffrement des disques durs des ordinateurs de bureau et portables à l'aide des technologies de chiffrement approuvées par KPMGI.
- Chiffrement des medias amovibles.
- Chiffrement des terminaux mobiles conformément aux exigences de sécurité définies.

3.7 Sécurité physique et environnementale

3.7.1 KPMG International et cabinets membres

Les règles globales de sécurité relatives aux locaux où sont traitées des informations de KPMG ou de ses clients requièrent les éléments suivants.

- L'accès aux locaux est réservé aux seules personnes autorisées.
- Revue régulière du personnel ayant accès aux locaux techniques informatiques.
- Tous les visiteurs doivent être accompagnés et leurs accès doivent faire l'objet d'un enregistrement.
- Le personnel de KPMG personnel doit porter de manière apparente son badge d'accès.
- Les accès aux datacenters doivent faire l'objet d'une revue formelle trimestrielle.
- Des mesures de sécurité adaptées contre le feu, les fumées et l'inondation doivent exister. Les autres facteurs de risque existants doivent être évalués et faire l'objet de mesures de protection adéquates.

Les règles exigent également que les matériels informatiques:

- Essentiels aux opérations (traitement, transmission, stockage) de KPMG soient protégés efficacement contre les menaces environnementales
- Soient protégés de la même manière lorsqu'ils sont transportés hors des locaux de KPMG.

3.8 Sécurité des opérations

3.8.1 KPMG International et cabinet membres

Les exigences suivantes s'appliquent aux cabinets membres.

- Protection contre les logiciels malveillants:
  - Maintenir un système anti-virus mettant à jours les ordinateurs individuels et les serveurs au moins une fois par jour
  - Programmer une analyse antivirale complète hebdomadaire sur l'ensemble des ordinateurs individuels et des serveurs et avoir un processor pour identifier les mises à jour et analyses défectueuses
- Mener une analyse mensuelle des vulnérabilités pour tous les systèmes et applications exposées à internet.
- Protéger chaque connexion à un réseau tiers par un firewall.
- Consigner le trafic réseau en incluant les tentatives infructueuses de connexion, la désactivation des traces d'audit, les changements effectués, l'horodatage et les adresses IP.
- Mettre en place un processus d'approbation visant à s'assurer que seul le trafic nécessaire à des besoins métiers valides est autorisé sur le réseau.
- Concevoir, documenter, maintenir et publier des procédures opérationnelles pour toutes les activités quotidiennes des systèmes informatiques stockant, traitant ou transmettant des informations de KPMG ou de ses clients.
- Isoler et protéger adéquatement les réseaux hébergeant des systèmes contenant des informations très sensibles.
- Suivre un processus formalisé de gestion des changements sur les systèmes informatique en production pour s'assurer que tous les changements opérés soient autorisés et puissent être audités.
- Mettre en œuvre u processus d'application des correctifs de sécurité sur les systèmes gérés par ou pour le compte de KPMG. Ce processus doit prendre en compte des niveaux de sévérité des vulnérabilités et des délais de correction correspondant à ces niveaux.
- Séparer de manière logique (et idéalement physiquement) les environnements de développement, de test et de production.
- Sauvegarder les données et les systèmes pour assurer la continuité de service et la disponibilité des systèmes critiques de KPMG. Les sauvegardes des systèmes critiques et des informations sensibles doivent être chiffrées et leur fréquence convenue conjointement entre le service informatique et le propriétaire du système, conformément à sa criticité.

3.9 Sécurité des communications

3.9.1 KPMG International et cabinets membres

Les réseaux internes de KPMG et les réseaux externes dument autorisés employés doivent:

- Être justifies par un besoin métier valide
- être opérés et administrés efficacement
- être robustes et fournir un service fiable et résilient
- être protégés des menaces internes et externes et assurer la sécurité et l'intégrité de l'information qui y circule.

Seuls les systèmes de communication approuvés par KPMGI peuvent être installés et utilisez par les cabinets membres.

Les communications entre 2 parties ou plus (internes ou externes) doivent se faire selon des méthodes approuvées garantissant la confidentialité, l'intégrité, 'exactitude et l'intégralité de l'échange.

3.10 Acquisition, développement et maintenance de systèmes

3.10.1 KPMG International

Une application – qu'elle soit développée par KPMGI, qu'elle soit un logiciel standard du marché ou encore fournie selon le modèle « software as a service » - mise à la disposition des cabinets membres par KPMGI doit faire l'objet d'une évaluation de risque, incluant des tests de sécurité, préalablement à sa mise en production. Des contrôles et mesures de sécurité adaptés doivent être mis en place conformément au risque et au service rendu.

3.10.2 Cabinets membres

Chaque cabinet membre opère un processus formel de revue de ses applications locales.

Un processus formalisé de gestion du changement doit être suivi pour les systèmes critiques en production pour s'assurer de ne pas introduire d'effets indésirables sur les systèmes ou applications.

3.11 Relations avec les fournisseurs

3.11.1 KPMG International et cabinets membres

Des revues de sécurité et de confidentialité des tiers doivent être menées avant de recourir à leurs services. En outre, KPMG ne peut octroyer l'accès à des systèmes critiques à des tiers qu'après avoir mené une évaluation de risque.

Le propriétaire métier de chaque service fourni par un tiers est responsable de la gestion des contrats en vue de garantir que les services fournis sont conformes à ceux attendus.

3.12 Gestion des incidents de sécurité

3.12.1 KPMG International et cabinets membres

Le processus global de réponse à incidents (« Global Events & Incidents Response » / GEIR) définit les responsabilités des KPMG International et des cabinets membres. Dans le cas où un incident implique des données d'un client, l'associé en charge du client et le service de Risk Management doivent être informés sans délai.

3.12.2 Cabinet membre

Chaque cabinet membre doit mettre en place un processus local de gestion des incidents de sécurité. Celui-ci concerne par exemple les incidents de sécurité physique, les violations de données, les pertes de confidentialité et doit définir un processus d'escalade national et international. Le processus local doit être aligné avec le processus « GEIR ».

Les cabinets membres peuvent avoir également à mettre en place des procédures complémentaires pour se conformer à des exigences réglementaires ou légales locales, spécialement quand des données d'un client de KPMG sont concernées.

3.13 Sécurité de l'Information et continuité d'activité

3.13.1 KPMG International et cabinets membres

3.13.1.1 Continuité d'activité

Le plan de continuité d'activité de KPMGI prévoit que chaque cabinet membre doit constituer une équipe de gestion de crise et des plans de reprise après sinistre concernant les sites et les services fournis par le cabinet membre. KPMGI dispose de plans d'urgence pour traiter les interruptions de ses opérations. Ces plans prévoient des mesures concernant les perturbations pouvant affecter des sites et des applications internes essentielles hébergées par KPMG dans ses datacenters. En cas de sinistre ou d'urgence, KPMGI et les cabinets membres ont défini des processus pour en minimiser les impacts sur les opérations et les services rendus par KPMG à ses clients.

De plus, dans le cadre de l'approche globale de gestion des risques d'entrepris, le « Global Quality & Risk Management » entretient un plan de gestion de crise pour réagir à toute situation qui menacerait ou affecterait le personnel, les locaux ou les opérations de KPMG.

3.13.1.2 Reprise après sinistre

Les règles globales requièrent que les cabinets membres établissent et communiquent à leur personnel un plan de reprise après sinistre traitant de la remise en service des systèmes critiques. Des tests de reprise doivent être conduits périodiquement conformément au niveau de risqué associé à chaque système critique.

Les cabinets membres doivent également mettre en œuvre des sauvegardes des données et systèmes critiques. Ces sauvegardes doivent être réalisées selon une planification conforme à la criticité des données et systèmes. Les procédures de sauvegarde doivent prévoir un stockage hors-site et des tests périodiques pour s'assurer de la possibilité de de restitution des informations sauvegardées lorsque cela est nécessaire.

3.14 Conformité

3.14.1 KPMG International et cabinets membres

L' « Information Protection Group » de KPMG International (IPG) a défini un programme de conformité visant à fournir un aperçu sur les pratiques de sécurité de l'information au sein du réseau des cabinets membres, à faciliter la gestion des risques informatiques qui pourraient affecter plus d'un cabinet membre et à promouvoir de saines pratiques de gestion des risques informatiques. A l'aide de revues de conformité, d'outils de surveillance permanente et de profils de risque de chaque cabinet membre le programme de conformité permet à chaque cabinet membre de mettre en place des bonnes pratiques de gestion des risques et de protéger leur environnement informatique conformément aux règles de sécurité globales de KPMG.

Chaque cabinet membre est responsable de la mise en œuvre, et de sa conformité avec, des règles de sécurité et de confidentialité globales de KPMG relatives à la protection de l'information. Chaque cabinet membre conduit un audit annuel indépendant sur ses contrôles en terme de protection de l(information pour déterminer son niveau de conformité avec les règles globales, identifier les zones de non-conformité ou les possibilités d'amélioration, et créer et maintenir un plan d'action de réduction des risques afin de les maintenir à un niveau acceptable pour le cabinet membre et pour tous les autres cabinets membres. Enfin, chaque cabinet membre est soumis à une revue de conformité exercée par l' « Information Protection Group » (IPG). Cette revue a lieu habituellement tous les 3 ans, cette fréquence pouvant être augmentée en fonction du profil de risque du cabinet membre concerné. Les résultats de cette revue sont communiqués aux instances dirigeantes du cabinet membre et de KPMG International.

Les résultats des audits internes et des revues de conformité sont confidentiels et communiqués uniquement en internet à KPMG. La communication externe (par exemple à des clients ou des tiers) est interdite.

Contact us

René Barrabes
National Information Security Officer
E fr-nitso@kpmg.fr

www.kpmg.fr