Lignes directrices complémentaires

CRIPP

Cadre de Référence International des Pratiques Professionnelles de l'audit interne

GTAG®

Global Technology Audit Guide

L'audit des appareils intelligents

Guide destiné aux auditeurs internes : comprendre et auditer les appareils intelligents

The Institute of Internal Auditors | Global

Table des matières

Synthèse ... 3
Introduction ... 4
Risques liés aux appareils intelligents ... 5
- Risques liés à la conformité ... 5
- Risques liés à la protection des données personnelles ... 5
- Risques liés à la sécurité ... 5
  - Risques liés à la sécurité physique ... 5
  - Risques liés à la sécurité de l'information ... 6

Contrôles concernant les appareils intelligents ... 7
- Contrôles liés à la sécurité des appareils intelligents ... 7
- À propos du contrôle des politiques SI ... 8

L'audit des appareils intelligents ... 11
- Planification de la mission ... 11
- Objectifs de la mission ... 11
- Champ de la mission et ressources allouées à la mission ... 12
- Programme de travail de la mission ... 12

Annexe A. Normes et lignes directrices de l'IIA ... 14
Annexe B. Définitions des concepts clés ... 17
Annexe C. Programme d'audit des appareils intelligents ... 20
Auteurs/Contributeurs ... 25

Synthèse

Les appareils intelligents (téléphones portables et autres tablettes) offrent des options de mobilité propices au travail à distance. Néanmoins, comme toute nouvelle technologie ou en expansion, ils sont synonymes de nouveaux risques pour les organisations.

La démarche de l'audit interne en matière d'évaluation des risques et des contrôles liés aux appareils intelligents évolue au fur et à mesure de l'apparition de nouvelles technologies et de la diversification des appareils. Pour répondre à ces enjeux, les auditeurs internes sont tenus de :

- comprendre la stratégie de l'organisation relative aux appareils intelligents ;
- évaluer les effets de cette technologie sur l'organisation ;
- donner une assurance sur l'environnement des appareils intelligents en :
  - identifiant et en évaluant les risques émanant de l'utilisation de ces appareils ;
  - déterminant l'adéquation des processus de gouvernance, de management des risques et de contrôles relatifs aux appareils intelligents ;
  - révisant la conception et l'efficacité des contrôles associés.

Les responsables de l'audit interne devraient approfondir leur compréhension des opportunités et des menaces que représentent les appareils intelligents pour l'organisation et l'activité d'audit interne. L'audit interne peut accompagner les activités de maîtrise des risques du management concernant l'utilisation d'appareils intelligents.

Ce guide devrait aider les auditeurs internes à mieux comprendre les technologies, les risques et les contrôles relatifs aux appareils intelligents. L'annexe C propose un programme de travail incluant une évaluation des risques, conçu spécifiquement pour analyser le management des risques et les contrôles liés aux appareils intelligents.

Introduction

Appareils intelligents – Les appareils électroniques programmés et contrôlés à l'aide de technologies informatiques ont révolutionné la vie des collaborateurs et donné une nouvelle dimension au concept de « travailleur mobile ». Autrefois, travailler à distance se limitait à se connecter au réseau de l'organisation *via* un ordinateur portable fourni par cette dernière ; aujourd'hui, les possibilités sont multiples : les téléphones et les tablettes utilisent des applications *(apps)* et des dispositifs conçus spécialement pour véritablement travailler en mobilité.

Grâce aux appareils intelligents, les utilisateurs profitent d'une puissance informatique portable et d'une connexion à Internet n'importe où, pourvu qu'il y ait un réseau Wi-Fi ou cellulaire. Ils peuvent également disposer d'un appareil 2 en 1 : à usage personnel et professionnel. Il existe une grande variété d'appareils intelligents et autant de systèmes d'exploitation, de mécanismes de sécurité, d'applications et de réseaux. Citons par exemple les *smartphones,* les tablettes, les assistants numériques personnels (PDA), les appareils portables (montres et lunettes) et les consoles de jeux portables.

Les appareils intelligents se caractérisent notamment par :

- le format (tablette, à clapet, accessoirisé) ;
- le système d'exploitation (Apple iOS, Android, Windows Mobile, Blackberry OS) ;
- les réseaux voix et données ;
- la vidéo et la photo ;
- le stockage de données (intégré ou non);
- les services de localisation tels que le GPS *(Global positioning system)* ;
- les applications grand public ou professionnelles (pré-installées ou téléchargées).

Dans certaines organisations, les collaborateurs peuvent être contraints, ou invités, à travailler sur leurs propres appareils, une pratique baptisée *bring your own device* (*BYOD* - apportez votre propre appareil). Qu'ils soient propriété de l'organisation ou du collaborateur, les appareils intelligents, comme n'importe quelle autre nouvelle technologie ou en expansion, s'accompagnent d'une myriade de risques qui remettent en question la gestion traditionnelle des risques de la direction des systèmes d'information (DSI).

L'audit interne peut soutenir les activités de maîtrise des risques du management concernant l'utilisation des appareils intelligents. Selon la Norme 2120.A1 et la Norme 2130.A1, l'audit interne doit évaluer les risques afférents à la gouvernance, aux opérations et aux systèmes d'information de l'organisation ainsi que la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques[1]. Ce GTAG propose une description détaillée des risques liés à l'utilisation des appareils intelligents, des contrôles qui peuvent être effectués pour maintenir ces risques à un niveau acceptable, et un programme de travail auquel se référer pour évaluer de façon efficace la gouvernance, le management des risques et les contrôles liés aux appareils intelligents.

[1] Voir l'Annexe A pour le texte complet de ces normes et d'autres normes pertinentes de l'IIA.

Risques liés

Les risques liés aux appareils intelligents peuvent être classés par catégories : conformité, données personnelles, sécurité physique ou sécurité de l'information.

Risques liés à la conformité

Avec le BYOD, les organisations sont amenées à compter essentiellement sur les utilisateurs pour respecter les politiques et procédures applicables, telles que les instructions relatives à la mise à jour des logiciels et aux systèmes d'exploitation. Les utilisateurs qui estiment que ces mises à jour sont trop intrusives ou nuisent à la performance de leur appareil peuvent choisir de ne pas les installer ou de contourner les mesures de contrôle. Dans un environnement BYOD, il convient de renforcer les compétences et les capacités des services support de la DSI. L'augmentation du nombre et de la diversité des appareils étend l'exposition de l'organisation à toute une gamme de vulnérabilités. La gestion des différentes versions de matériels et de logiciels habilitées à accéder et à stocker les données d'un format propriétaire peut s'avérer complexe, notamment en l'absence de politiques, procédures et protocoles.

Risques liés à la protection des données personnelles

Les pratiques de BYOD peuvent soulever des questions en matière de protection des données personnelles tant du point de vue de l'organisation que des collaborateurs. Par exemple, une organisation peut rencontrer des difficultés pour protéger la vie privée de ses parties prenantes dont les données d'identification personnelle *(personally identifiable information-PII)* sont accessibles ou stockées sur un appareil intelligent : une situation de plus en plus fréquente. *A contrario,* les collaborateurs peuvent craindre une surveillance intrusive *via* leur appareil intelligent, ou la suppression accidentelle de leurs données personnelles (photos et contacts) en même temps que celle des données de l'organisation. Un risque supplémentaire existe quand des tiers (fournisseurs, invités ou visiteurs, par exemple) ont accès aux réseaux et systèmes de l'organisation depuis leur propre appareil intelligent.

Risques liés à la sécurité

Les informations stockées sur les appareils intelligents concernent des données personnelles et celles de l'organisation. Ces informations peuvent être compromises si l'appareil intelligent est perdu ou volé, si l'utilisateur quitte l'organisation sans supprimer de l'appareil les données de cette dernière ou si les contrôles de sécurité adaptés ne sont pas effectués comme ils le devraient. Avant d'élaborer un programme d'audit pour les appareils intelligents, les auditeurs doivent bien comprendre les particularités de différentes catégories de risques liés à la sécurité.

Risques liés à la sécurité physique

Les appareils intelligents sont en permanence exposés aux risques de sécurité physique. En raison de leur nature mobile, les appareils intelligents, utilisés dans différents lieux, sont susceptibles d'être perdus ou volés. Les données sensibles de l'organisation qui y sont stockées sont alors en

danger. Les organisations doivent se doter de procédures strictes en cas de perte ou de vol ou d'incidents de sécurité, et avoir la possibilité, par exemple, d'effacer à distance les données stockées sur l'appareil concerné.

Risques liés à la sécurité de l'information

Stockage et sauvegarde des données

Les données personnelles et celles de l'organisation stockées sur les appareils intelligents peuvent être compromises si des mesures de sécurité adaptées, telles que le chiffrement, ne sont pas mises en place. Après une panne de l'appareil ou du système, la récupération des données peut être problématique si ces dernières n'ont pas été correctement sauvegardées.

Systèmes d'exploitation

En termes de sécurité, chaque système d'exploitation (operating system : OS) présente des caractéristiques et des risques qui doivent être gérés, configurés et sécurisés différemment. Quand les utilisateurs contournent les restrictions d'origine des systèmes d'exploitation par le débridage ou le déverrouillage de l'OS *(jailbreaking* pour l'OS d'Apple, *rooting* pour l'OS d'Android), les contrôles de sécurité installés d'origine sur l'appareil sont désactivés et de nouvelles failles de sécurité apparaissent. De plus, la diversité des plateformes complique la suppression des données par les organisations en cas de remplacement de l'appareil ou de changement d'opérateur.

Connexions au réseau

Les appareils intelligents se connectent à Internet *via* des réseaux sans fil ou cellulaires, qui ne sont pas toujours fiables. Les réseaux non fiables (par exemple, les réseaux sans fil non sécurisés ou le Bluetooth…) suscitent différents risques de sécurité susceptibles de compromettre les données transmises : détournement de session *(hijacking,* exploitation d'une session réseau valide à des fins non autorisées), écoutes illégales et attaques de l'homme du milieu *(eavesdropping* et *man-in-the-middle attacks*, stratégie d'attaque au cours de laquelle l'assaillant intercepte le flux de communications entre deux parties du système attaqué et remplace les données échangées par ses propres données, prenant finalement le contrôle de la communication).

Applications

Un grand nombre d'applications disponibles depuis les catalogues d'applications mobiles *(app stores)* sont téléchargeables directement sur les appareils intelligents. Ces applications sont généralement développées par des tiers, qui sont de grands éditeurs de logiciels ou de simples particuliers. Les virus, chevaux de Troie et autres logiciels malveillants peuvent infecter les appareils intelligents si les plateformes pour appareils mobiles et les *app stores* n'imposent pas un minimum de règles de sécurité à la publication d'applications mobiles par des tiers.

Localisation

Il est possible d'utiliser un système comme le GPS pour se localiser, pour suivre les appareils intelligents, surveiller le comportement d'un utilisateur et programmer des cyberattaques. La localisation et les caractéristiques personnelles d'un individu sont déterminées en comparant les données

de différentes sources, telles que les médias sociaux, les moteurs de recherche, les applications de navigation. D'autres indices de localisation peuvent être déduits à partir des photos embarquées du GPS.

Contrôles associés aux appareils intelligents

Contrôles associés à la sécurité des appareils intelligents

En termes de sécurité, les appareils intelligents offrent un grand nombre de caractéristiques que les organisations peuvent mettre à profit pour réduire les risques.

Authentification – L'authentification, qui constitue la première étape de sécurisation des appareils intelligents, empêche les utilisateurs non autorisés d'accéder aux applications et aux données de l'appareil. Les appareils intelligents utilisent au moins l'une des méthodes d'authentification suivantes : mot de passe, schéma de déverrouillage, biométrie, questions de sécurité ou code PIN *(personal identification number)*. Le code PIN est un code à chiffres, la forme la plus simple d'authentification. Un mot de passe utilise une combinaison de chiffres, lettres et symboles. Autre méthode d'authentification, le schéma de déverrouillage, qui nécessite que l'utilisateur glisse son doigt sur une combinaison de points sur l'écran d'accueil. Enfin, la ou les questions de sécurité, prédéfinies, auxquelles doit répondre l'utilisateur. Ces méthodes sont à la discrétion de l'utilisateur, qui choisit son code ou son schéma.

Pour limiter le risque que l'utilisateur ne choisisse un code PIN ou un mot de passe avec un faible niveau de sécurité, les DSI peuvent imposer des paramètres renforcés *via* des solutions de gestion de terminaux mobiles ou MDM *(mobile device management)* ou demander une seconde authentification avant d'accéder aux applications de l'organisation. Les questions de sécurité sont souvent utilisées comme authentification de deuxième niveau sur les appareils intelligents (par exemple, quand l'utilisateur a oublié son mot de passe, les questions de sécurité permettent de l'identifier). La méthode d'authentification la plus sûre reste la biométrie, avec le recours à des technologies telles que la reconnaissance faciale ou la lecture d'empreintes digitales.

Effacement à distance – C'est la possibilité offerte à l'utilisateur ou à l'administrateur d'effacer les données et les applications *via* le réseau, sans être en possession de l'appareil. Cette technique permet également de restaurer une configuration par défaut et de verrouiller des données cryptées pour en empêcher l'accès ultérieur. Pour les appareils intelligents appartenant à l'organisation, les administrateurs de la DSI peuvent déployer des solutions MDM ou alternatives, telles que Microsoft Exchange ActiveSync, afin d'effacer les données à distance.

Notons toutefois que l'effacement à distance ne supprime pas complètement les données de l'appareil intelligent. Certains outils de MDM ne sont pas capables d'effacer les cartes SD *(secure digital)* à distance. Cette technique ne concerne pas les données sauvegardées, par ailleurs, sur un ordinateur ou dans le *cloud*. Enfin, le *jailbreaking* ou le *rooting* (déverrouillage des systèmes d'exploitation) peuvent interférer avec l'effacement à distance.

Chiffrement matériel ou d'appareil – En règle générale, les appareils intelligents supportent le chiffrement matériel. Lorsque cette option est activée, les données et les applications restent crytpées tant qu'un code secret n'a pas été saisi. Les clés de chiffrement sont générées en utilisant un code unique prédéfini à la fabrication et un code secret choisi par l'utilisateur. Le chiffrement matériel constitue un contrôle clé dans la protection des données sur les appareils intelligents.

Chiffrement logiciel – Incontournable, pour l'ensemble des applications de l'organisation, notamment les e-mails. Pour les appareils intelligents qui ne supportent pas le chiffrement matériel, le chiffrement logiciel, qui nécessite de renseigner un deuxième mot de passe pour accéder à une application, peut être utilisé pour protéger les applications et les données de l'organisation. Contrairement au chiffrement matériel, qui crypte l'ensemble des données de l'appareil, le chiffrement logiciel ne crypte que les données relatives à l'application qui utilise l'algorithme de chiffrement. Le niveau de chiffrement utilisé par le développeur de l'application doit être évalué afin de s'assurer qu'il répond aux normes minimum de l'organisation.

Chiffrement des flux de données – La plupart des appareils intelligents supportent le protocole TLS *(Transport Layer Security)* pour le chiffrement des e-mails, de la navigation sur Internet et des réseaux privés virtuels ou VPN *(virtual private networks)*.

À propos du contrôle des politiques SI

En plus des contrôles au niveau de l'appareil, la sécurité peut être instaurée au niveau des politiques et des procédures.

Programme anti-logiciel malveillant – Ce programme détecte et supprime les logiciels malveillants *(malwares)* qui s'immiscent dans les appareils intelligents et ouvrent l'accès aux données personnelles. Pour une protection efficace, les utilisateurs doivent :

a. Installer un programme anti-logiciel malveillant et s'assurer que l'ensemble des appareils intelligents sont bien protégés.
b. Mettre régulièrement à jour les systèmes d'exploitation. Les fabricants d'appareils intelligents mettent à jour très souvent leur système d'exploitation pour renforcer la sécurité ou les mécanismes de défense qui combattent les logiciels malveillants identifiés et les failles de sécurité.
c. Télécharger des applications, uniquement depuis des *app stores* connus. Les organisations peuvent développer leur propre catalogue d'applications d'entreprise, sécurisé, pour leurs collaborateurs.
d. Mettre régulièrement à jour les applications, car les développeurs renforcent constamment la sécurité de leurs applications mobiles.
e. Éviter le déverrouillage des systèmes d'exploitation *(jailbreaking/rooting)*. L'altération du système d'exploitation et la suppression des contrôles et des restrictions intégrés à l'origine par le fabricant contournent les outils de sécurité et rendent l'appareil vulnérable aux menaces. Si ces pratiques sont légales dans certains pays, elles peuvent tomber sous le coup de législations locales sur la propriété intellectuelle et annuler la garantie constructeur de l'appareil. Les organisations doivent interdire l'utilisation d'appareils intelligents débridés.

Politique en matière de BYOD – Pour les cas où les collaborateurs sont autorisés à utiliser leur appareil intelligent personnel dans le cadre de leur activité, une politique complète doit être mise en œuvre à ce sujet. Ces instructions doivent prévoir, entre autres :

a. Les appareils autorisés et les systèmes d'exploitation recevables (par exemple, iOS, Android) et les responsables de leur maintenance.
b. Les attentes et les responsabilités liées aux données personnelles et à celles de l'organisation stockées dans l'appareil intelligent. Par exemple, l'organisation peut limiter les téléchargements ou des transferts de données et, dans ce cadre, le collaborateur aura la responsabilité de ne pas partager l'appareil avec des membres de sa famille si des données confidentielles y sont stockées.
c. Un minimum d'exigences de sécurité, tels que des mots de passe complexes et la mise à jour des systèmes d'exploitation.
d. La remontée, en temps opportun, de toute faille dans la sécurité et de la perte ou du vol de l'appareil.
e. L'accès aux données, applications mobiles et ressources réseaux de l'organisation, y compris la liste des personnes autorisées à accéder aux applications et par quels moyens (par exemple, depuis le web, le VPN ou les applications mobiles).
f. Les sauvegardes et les transferts, notamment les modalités et lieux de sauvegarde des données de l'organisation ainsi que ce qui peut être transféré sur d'autres appareils. Par exemple, un collaborateur peut-il transférer ou sauvegarder des données de l'organisation sur un ordinateur personnel ou vers un service public d'hébergement de données ? Ces décisions peuvent avoir des conséquences sur la sécurité des données et sur la conformité avec certaines obligations de confidentialité, règlementaires et contractuelles (par exemple, aux États-Unis, la loi sur la responsabilité et la portabilité des données de santé *(Health Insurance Portability and Accountability Act*, HIPAA), la loi Sarbanes-Oxley de 2002, la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et le concept de données d'identification personnelle *(PII-personally identifiable information)*.
g. L'effacement à distance. Les utilisateurs doivent activer l'option d'effacement à distance et identifier les applications concernées. Le problème est que l'effacement à distance peut avoir des répercussions tant sur les données d'identification personnelle (PII) que sur les données de l'organisation. Il convient donc de déterminer si l'organisation peut avoir accès à l'ensemble des données (et éventuellement les supprimer) ou juste aux données de l'organisation. Les organisations dotées d'une politique BYOD doivent consulter leur service juridique avant de développer et de mettre en place les politiques et procédures relatives à l'effacement à distance.
h. Les processus concernant les appareils intelligents en fin de cycle. Plusieurs possibilités : revente, échange, don, ou mise au rebut.
i. Reconnaissance et signature, par les collaborateurs, de l'ensemble des politiques et procédures applicables.

Téléchargement de données/pièces jointes – Le téléchargement de données sensibles sur un appareil intelligent est à déconseiller. Des applications mobiles restrictives offrent aux utilisateurs la possibilité de consulter les pièces jointes sensibles sur leur appareil intelligent sans les télécharger sur une carte SD. De la même façon, il est important d'envisager le contrôle de la capacité à faire des captures d'écran.

Sauvegarde des données – La mise en place de sauvegardes sécurisées des données présentes sur les appareils intelligents permet de restaurer, sur un nouvel appareil, des données perdues, endommagées ou effacées à distance. La plupart des appareils intelligents proposent d'origine de sauvegarder les données sur un ordinateur de bureau ou portable, ou dans le *cloud*. Les données et les applications de l'organisation doivent être sauvegardées sur le centre de données de l'organisation, contrôlé par l'administrateur de la DSI, contrairement à la sauvegarde d'origine, contrôlée par l'utilisateur. Les systèmes de sauvegarde doivent être correctement sécurisés.

Gestion d'application mobile ou MAM *(Mobile Application Management)* – Les logiciels MAM permettent de gérer et de protéger les données sur des applications spécifiques. Pour ce faire, les points clés sont les modalités de conception, de gestion, de modification et de transfert de l'application vers un appareil intelligent, ainsi que les contrôles de sécurité déployés pour protéger les données utilisées par l'application.

Gestion des terminaux mobiles ou MDM *(Mobile Device Management)* – Les logiciels MDM s'avèrent plus efficaces quand des solutions MDM sont installées tant sur l'appareil que sur le réseau de l'organisation. Ce type de logiciel protège les données critiques en assurant l'interface avec les contrôles de sécurité installés sur le système d'exploitation de l'appareil intelligent.

Le logiciel MDM peut :

- Déployer et gérer de façon centrale les contrôles SI, tels que les mots de passe complexes, les niveaux de chiffrement, l'effacement à distance et autres options de sécurité.
- Répertorier, fournir, installer, mettre à jour et supprimer des applications.
- Contrôler les appareils, informer l'utilisateur et le management en cas d'infraction à une politique de contrôle et même désactiver les appareils intelligents qui ne respectent pas ces instructions.

Restrictions Wi-Fi – Ces restrictions restreignent l'utilisation des réseaux Wi-Fi, sécurisés conformément aux meilleures pratiques du secteur. Les solutions VPN sont à privilégier pour accéder aux applications et aux données de l'organisation depuis des appareils intelligents.

Toutes les politiques, procédures et technologies mises en place pour gérer les appareils intelligents ne sauraient être efficaces sans une bonne compréhension, de la part de l'utilisateur, des risques associés et de la façon d'adopter des mesures de protection. Tous les collaborateurs accédant aux données et applications de l'organisation depuis un appareil intelligent (personnel ou fourni par l'organisation) doivent recevoir régulièrement une formation, adaptée à leur rôle au sein de l'organisation, sur l'utilisation adéquate des appareils intelligents.

L'audit des appareils intelligents

Un programme de travail présente les objectifs et le périmètre d'intervention de la mission d'audit, ainsi que les risques et les contrôles correspondants liés aux appareils intelligents et les procédures d'audit à mettre en place.

L'engagement de l'audit interne dans l'évaluation de l'environnement de contrôle sensibilise davantage l'organisation aux risques associés à l'utilisation des appareils intelligents. Ce qui devrait se traduire par des contrôles de sécurité renforcés. Dans le cadre de la réalisation des missions d'assurance sur les systèmes d'information, conformément aux Normes 2120.A1 et 2130.A1. Il est prudent que l'audit interne évalue les expositions aux risques et examine l'adéquation et l'efficacité du management des risques et des contrôles liés au stockage et à l'utilisation des données critiques d'une organisation par les appareils intelligents, dans les systèmes d'exploitation et dans les applications mobiles.

Planification de la mission

La Norme 2200 énonce que les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le périmètre d'intervention, le calendrier de la mission, ainsi que les ressources allouées. Pour l'audit interne, un élément essentiel lors de cette planification consiste à déterminer si l'organisation dispose d'une structure de gouvernance unifiée et cohérente, notamment des politiques et des procédures, à partir desquelles des instructions claires et homogènes peuvent être diffusées dans l'ensemble de l'organisation. Un modèle robuste de gouvernance s'accompagnera de politiques, processus et outils nécessaires à la gestion de l'environnement et au contrôle des risques liés aux appareils intelligents et aux applications mobiles, autant d'activités indispensables à une protection adéquate des données de l'organisation. Il arrive que plusieurs fonctions soient chargées d'une partie de la stratégie relative aux appareils intelligents (par exemple, la DSI est chargée de la sécurité et le service juridique de la confidentialité). Néanmoins, la clé de succès d'une bonne gouvernance consiste à désigner un responsable unique qui devra assurer la cohérence des normes et des procédures, la collaboration entre les fonctions, l'intégration des objectifs métier et l'optimisation des ressources.

Objectifs de la mission

Sur un marché très concurrentiel, un accès rapide aux données et aux ressources de l'organisation est crucial. Cependant, les risques associés et leurs conséquences potentielles sur l'organisation doivent être bien compris du management et l'audit interne devrait contribuer à cette compréhension.

Les auditeurs internes établissent les objectifs de la mission en fonction des risques liés à l'activité à auditer. Une analyse des risques devrait être réalisée pour déterminer les objectifs initiaux et identifier d'autres domaines à enjeux significatifs.

Champ de la mission et ressources affectées à la mission

Les procédures à mettre en place ainsi que le périmètre d'intervention de la mission (nature, calendrier et étendue) doivent être déterminés après l'identification des risques. Selon la Norme 2220.A1, « le périmètre d'intervention de la mission doit couvrir les systèmes, les données, les personnes et les biens concernés, y compris ceux qui se trouvent sous le contrôle de tiers ».[2]

L'utilisation d'appareils intelligents expose les organisations à une myriade de risques qui nécessitent la mise en place de contrôles à différents niveaux de l'architecture informatique. La mission d'audit devra concerner également la stratégie et la gouvernance, y compris les politiques, les normes et les procédures relatives aux appareils intelligents, la sensibilisation et la formation des collaborateurs, la gestion des appareils intelligents et des applications mobiles, et la protection des données.

L'activité d'audit interne doit déterminer quelles sont les compétences nécessaires pour mener à bien la mission ainsi que l'effectif requis. L'équipe d'audit interne doit posséder les niveaux d'expertise, de connaissance et de qualification appropriés pour la réalisation de la mission. Dans le cas contraire, des ressources externes qualifiées devraient être mobilisées.

Programme de travail de la mission

Avant de commencer une mission d'audit des appareils intelligents, l'audit interne doit comprendre qui possède ces appareils et comment ils sont utilisés au sein de l'organisation. Conformément à la Norme 2240.A1 Programme de travail de la mission, « les programmes de travail doivent faire référence aux procédures à appliquer pour identifier, analyser, évaluer et documenter les informations lors de la mission ».

Un programme de travail relatif aux appareils intelligents peut comprendre les questions suivantes :

- Le réseau de l'organisation est-il accessible depuis des appareils intelligents ?
- L'accès au réseau est-il limité à la messagerie ou concerne-t-il aussi les données de l'organisation ?
- L'organisation fournit-elle des appareils intelligents à ses collaborateurs ?
- Les collaborateurs sont-ils autorisés à utiliser leur propre appareil pour leur activité professionnelle ?
- Comment la technologie des appareils intelligents s'intègre-t-elle dans l'organisation et dans la base d'utilisateurs ?
- Qui est responsable de la stratégie relative aux appareils intelligents et qui s'assure du respect des politiques et des procédures dans ce domaine ?
- Comment les données en interface avec le serveur *(back-end)* sont-elles stockées et gérées ?
- Comment l'organisation se protège-t-elle contre les pertes et la corruption de données, les failles de sécurité, les pannes de réseau et la perte ou le vol d'appareils ?
- Les appareils intelligents sont-ils protégés comme des actifs ou des outils de l'organisation nécessaires à l'atteinte des objectifs métiers ?
- L'organisation respecte-t-elle toujours les politiques juridiques et règlementaires ?

[2] NdT : Traduction des *Normes* en vigueur à la date de parution de la version française du GTAG. Les *Normes* sont régulièrement mises à jour. Pour une version actualisée, consulter les sites internet de l'IIA ou de l'IFACI.

L'annexe C propose un exemple de programme de travail d'audit sur la sécurité des appareils intelligents, y compris une évaluation des risques.

Annexe A. Normes et lignes directrices de l'IIA[3]

Selon la Norme 2110, Gouvernance
L'audit interne doit évaluer et formuler des recommandations appropriées en vue d'améliorer les processus de gouvernance de l'organisation pour :

- les prises de décisions stratégiques et opérationnelles ;
- la surveillance des processus de management des risques et de contrôle ;
- la promotion des règles d'éthique et des valeurs appropriées au sein de l'organisation ;
- une gestion efficace des performances de l'organisation, assortie d'une obligation de rendre compte ;
- la communication aux services concernés des informations relatives aux risques et aux contrôles ;
- la coordination des activités et la communication des informations entre le Conseil, les auditeurs externes, les auditeurs internes, les autres prestataires d'assurance, et le management.

Selon la Norme 2120, Management des risques
L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration.

2120.A1 – L'audit interne doit évaluer les risques afférents à la gouvernance, aux opérations et aux systèmes d'information de l'organisation au regard de :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

Selon la Norme 2130, Contrôle
L'audit interne doit aider l'organisation à maintenir un dispositif de contrôle approprié en évaluant son efficacité ainsi que son efficience et en encourageant son amélioration continue.

2130.A1 – L'audit interne doit évaluer la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs à la gouvernance, aux opérations et systèmes d'information de l'organisation. Cette évaluation doit porter sur les aspects suivants :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

[3] NdT : Traduction des Normes en vigueur à la date de parution de la version française du GTAG. Les *Normes* sont régulièrement mises à jour. Pour une version actualisée, consulter les sites internet de l'IIA ou de l'IFACI.

Selon la Norme 2200, Planification de la mission
Les auditeurs internes doivent concevoir et documenter un plan pour chaque mission. Ce plan de mission précise les objectifs, le périmètre d'intervention, le calendrier de la mission, ainsi que les ressources allouées. Ce plan doit prendre en considération la stratégie, les objectifs, et les risques de l'organisation pertinents au regard de la mission.

Selon la Norme 2201, Considérations relatives à la planification
Lors de la planification de la mission, les auditeurs internes doivent prendre en compte :

- la stratégie, les objectifs de l'activité auditée et la manière dont elle pilote sa performance ;
- les risques significatifs liés aux objectifs de l'activité, à ses ressources et à ses opérations, ainsi que les moyens par lesquels l'impact potentiel des risques est maintenu à un niveau acceptable ;
- la pertinence et l'efficacité des processus de gouvernance, de management des risques et de contrôle de l'activité, en référence à un cadre ou un modèle approprié ;
- les opportunités d'améliorer de manière significative les processus de gouvernance, de management des risques et de contrôle de l'activité.

2201.C1 – Les auditeurs internes doivent conclure avec le client donneur d'ordre un accord sur les objectifs et le périmètre d'intervention de la mission de conseil, les responsabilités de chacun et plus généralement sur les attentes du client donneur d'ordre. Pour les missions importantes, cet accord doit être formalisé.

Selon la Norme 2210, Objectifs de la mission
Les objectifs doivent être précisés pour chaque mission.

2210.A1 – Les auditeurs internes doivent procéder à une évaluation préliminaire des risques liés à l'activité soumise à l'audit. Les objectifs de la mission doivent être déterminés en fonction des résultats de cette évaluation.

2210.A3 – Des critères adéquats sont nécessaires pour évaluer la gouvernance, le management des risques et le dispositif de contrôle. Les auditeurs internes doivent déterminer dans quelle mesure le management et/ou le Conseil a défini des critères adéquats pour apprécier si les objectifs et les buts ont été atteints. Si ces critères sont adéquats, les auditeurs internes doivent les utiliser dans leur évaluation. S'ils sont inadéquats, les auditeurs internes doivent identifier, à travers une discussion avec le management et le Conseil, les critères d'évaluation appropriés.

Selon la Norme 2220, Périmètre d'intervention de la mission
Le périmètre d'intervention doit être suffisant pour atteindre les objectifs de la mission.

2220.A1 – Le périmètre d'intervention de la mission doit couvrir les systèmes, les données, les personnes et les biens concernés, y compris ceux qui se trouvent sous le contrôle de tiers.

Selon la Norme 2230, Ressources affectées à la mission
Les auditeurs internes doivent déterminer les ressources appropriées et suffisantes pour atteindre les objectifs de la mission. Ils s'appuient sur une évaluation de la nature et de la complexité de chaque mission, des contraintes de temps et des ressources disponibles.

Selon la Norme 2240, Programme de travail de la mission
Les auditeurs internes doivent élaborer et documenter un programme de travail permettant d'atteindre les objectifs de la mission.

> **2240.A1 –** Les programmes de travail doivent faire référence aux procédures à appliquer pour identifier, analyser, évaluer et documenter les informations lors de la mission. Le programme de travail doit être approuvé avant sa mise en œuvre. Les ajustements éventuels doivent être approuvés rapidement.

Selon la Norme 2310, Identification des informations
Les auditeurs internes doivent identifier les informations suffisantes, fiables, pertinentes et utiles pour atteindre les objectifs de la mission.

Autres lignes directrices de l'IIA sur le sujet

Guide pratique *« L'audit des risques d'atteinte à la vie privée, 2ème édition »*
« GTAG : Les risques et les contrôles des systèmes d'information, 2ème édition »
« GTAG : Information Security Governance »

Annexe B. Définitions des concepts clés

Audit interne – Fonction assurée par un service, une division, une équipe de consultants ou tout autre praticien, c'est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. L'audit interne aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernance, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité.[4]

Apportez votre propre appareil (BYOD) – Stratégie alternative permettant aux collaborateurs, aux partenaires commerciaux et aux autres intervenants d'utiliser un appareil qu'ils ont choisi et acheté pour y faire fonctionner des applications de l'organisation et accéder à ses données. Généralement, cette pratique concerne les *smartphones* et les tablettes mais elle peut aussi s'appliquer aux ordinateurs. Une subvention peut être prévue.[5]

Back-end – Côté serveur d'un système client/serveur.[6]

Catalogues d'applications mobiles – Offre aux utilisateurs mobiles des applications téléchargeables via une interface qui est soit intégrée dans l'appareil soit disponible sur le Web. Dans les catalogues publics, les applications sont réparties par catégories – jeux, voyages, productivité, loisirs, livres, services d'utilité publique, éducation, etc. et peuvent être gratuites ou payantes. Des catalogues privés peuvent être créés par les organisations pour leurs collaborateurs mobiles.[7]

***Cloud computing* (informatique dans les nuages) –** Concept reposant sur la technologie Internet et consistant à proposer un service de stockage à la capacité modulable.[8]

***Jailbreak* (débridage ou déverrouillage) –** Processus permettant aux utilisateurs d'appareils fonctionnant sous le système d'exploitation mobile d'Apple iOS d'obtenir un accès complet pour déverrouiller toutes les fonctionnalités du système d'exploitation, éliminant ainsi les restrictions et sécurités du fabricant. Une fois iOS débridé, ses utilisateurs sont en mesure de télécharger des applications, des extensions ou des thèmes en-dehors de la boutique d'applications officielle d'Apple, l'App Store.[9]

Malware – Abréviation de *malicious software,* programme ou logiciel malveillant. Conçu pour infiltrer, endommager et obtenir des données d'un système informatique sans le consentement de son propriétaire. Un logiciel malveillant intègre souvent des virus informatiques, des vers, des chevaux de Troie, des logiciels espions et des logiciels de publicité. Les logiciels espions sont généra-

[4] The Institute of Internal Auditors, International Professional Practices Framework (IPPF) (Altamonte Springs: The Institute of Internal Auditors, Inc., 2013), 43.

[5] Glossaire informatique Gartner, http://www.gartner.com/it-glossary (consulté le 9 mars 2016).

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] « Jailbreak d'iOS » / « Débridage d'iOS » Wikipedia. Consulté le 05 octobre 2016 https://fr.wikipedia.org/wiki/Jailbreak_d%27iOS.

lement utilisés à des fins commerciales, en tant que tels, ils ne sont pas malveillants, bien qu'ils soient non désirés. Ils peuvent toutefois être utilisés pour collecter des informations dans le but d'usurper une identité ou à d'autres fins clairement illégales.[10]

MAM *(Mobile Application Management,* gestion d'applications mobiles) – Concerne les logiciels et services responsables de la fourniture et du contrôle de l'accès aux applications mobiles développées en interne et disponibles à la vente utilisées dans la configuration des paramètres sur les appareils fournis par l'organisation ou ceux des collaborateurs. Ils fournissent des contrôles précis au niveau de l'application permettant aux administrateurs de gérer et de sécuriser les données qu'elle utilise.[11]

MDM *(Mobile device management,* gestion de terminaux mobiles) – Intègre un logiciel qui assure les fonctions suivantes : distribution de logiciels, gestion de la politique, gestion des archives, gestion de la sécurité et gestion des services pour *smartphones* et tablettes. La fonction MDM est semblable à l'outil PCCLM de gestion du cycle de vie des configurations sur les ordinateurs ; toutefois, des conditions spécifiques aux plateformes mobiles sont souvent incluses dans les suites MDM.[12]

PII *(Personally identifiable information,* données d'identification personnelle) – toute représentation de l'information qui permet d'identifier, de façon directe ou indirecte, un individu auquel la donnée s'applique. Par ailleurs, une PII est définie comme une donnée : (i) qui permet l'identification directe d'un individu (nom, adresse, numéro de sécurité sociale, ou autre numéro ou code d'identification, numéro de téléphone, adresse e-mail, etc.) ou (ii) qui permet son identification indirecte, par exemple lorsqu'une agence utilise cette donnée pour identifier des individus spécifiques en lien avec d'autres éléments. Ces éléments peuvent être : le genre, l'origine, la date de naissance, une indication géographique ou toute autre description. À noter qu'une information permettant de contacter physiquement ou virtuellement un individu donné est considérée comme une PII. Cette information peut être conservée sous forme papier, électronique ou par tout autre moyen.[13]

***Rooted* ou *Rooting* (déverrouillé ou déverrouillage) –** Le fait d'autoriser les utilisateurs de smartphones, tablettes et autres appareils tournant sous le système d'exploitation mobile Android à effectuer une élévation des privilèges (connus sous le nom de droits SuperUtilisateur) sur le système Android. Comme Android est souvent dérivé du noyau Linux, déverrouiller *(rooter)* un appareil Android est similaire au fait d'accéder aux droits administrateurs sur Linux ou tout autre système d'exploitation de type Unix tels que FreeBSD ou OSX.[14]

---

[10] ISACA, « ISACA Glossary of Terms », 59. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (consulté le 9 mars 2016). Tous droits réservés. Reproduction autorisée.

[11] « Jailbreak d'iOS » / « Débridage d'iOS » *Wikipedia,* https://fr.wikipedia.org/wiki/Jailbreak_d%27iOS (consulté le 05 octobre 2016).

[12] Glossaire informatique Gartner (2012), http://www.gartner.com/it-glossary (consulté le 9 mars 2016).

[13] « Guidance on the Protection of Personal Identifiable Information », United States Department of Labor, http://www.dol.gov/dol/ppii.htm (consulté le 9 mars 2016).

[14] « Rooting », *Wikipedia*, https://fr.wikipedia.org/wiki/Root_d%27Android (consulté le 05 octobre 2016).

***Smartphone* –** téléphone mobile utilisant un système d'exploitation ouvert identifiable. Un système d'exploitation ouvert est supporté par des applications tierces mises au point par une importante communauté de développeurs. Les applications tierces peuvent être installées sur l'appareil et supprimées. Elles peuvent être créées pour le système d'exploitation et les interfaces de programmation applicatives (API) de l'appareil. Les développeurs peuvent accéder aux API *via* une couche discrète, Java par exemple. Le système d'exploitation supporte un environnement multitâches et une interface utilisateur qui peut prendre en charge plusieurs applications en même temps. Par exemple, il permet l'accès aux e-mails tout en diffusant de la musique.[15]

Stockage SD *(Secure Digital)* – Carte mémoire à insérer dans les appareils intelligents. Secure Digital fait référence à une norme mise en place en 1999 par SD Association.[16]

[15] Glossaire informatique Gartner (2012), http://www.gartner.com/it-glossary (consulté le 9 mars 2016).

[16] « Fact Sheet », SD Association, https://www.sdcard.org/about_sda/fact_sheet/ (consulté le 9 mars 2016).

Annexe C. Programme d'audit des appareils intelligents

Objectif 1 : Planifier et déterminer le périmètre d'intervention de la mission		
Activités d'audit		**Vérifications**
1.1 Définir les objectifs de la mission (Norme 2210) Les objectifs de la mission d'audit ou d'assurance décrivent les objectifs généraux de l'audit.		
1.2 Identifier et évaluer les risques (Norme 2210.A1) L'évaluation des risques permet de déterminer les points auxquels les auditeurs devront accorder le plus d'attention.		
1.2.1	Identifier les risques métier associés à l'informatique mobile qui peuvent intéresser les propriétaires et les parties prenantes clés.	
1.2.2	Vérifier que les risques métier sont alignés avec les risques SI identifiés.	
1.2.3	Évaluer le risque global que présente la réalisation de la mission.	
1.2.4	En fonction de l'évaluation des risques, identifier les changements à apporter au périmètre d'intervention de la mission.	
1.2.5	Discuter des risques avec le management, et ajuster l'évaluation des risques.	
1.2.6	En fonction de l'évaluation des risques, revoir le périmètre d'intervention de la mission.	
1.3 Définir le périmètre d'intervention de la mission (Norme 2220) Le périmètre de la mission doit être défini. L'auditeur interne devra connaître les appareils intelligents utilisés dans l'organisation, les données qui y transitent et les risques associés pour l'organisation.		
1.3.1	Obtenir une liste des appareils intelligents utilisés.	
1.3.2	Déterminer le périmètre d'intervention de la mission.	
1.4 Définir les critères de succès de la mission Les facteurs de succès doivent être identifiés et faire l'objet d'un accord.		
1.4.1	Identifier les leviers d'une mission d'audit réussie.	
1.4.2	Communiquer, pour validation, les critères de succès au propriétaire du processus ou à la partie prenante.	
1.5 Définir les ressources nécessaires à la réalisation de la mission (Norme 2230) Dans la plupart des organisations, les ressources de l'audit ne sont pas toujours disponibles pour l'ensemble des processus.		
1.5.1	Déterminer les compétences nécessaires à la réalisation de la mission.	
1.5.2	Estimer les ressources (nombre d'heures) et le calendrier (date de début et de fin) nécessaires pour la réalisation de la mission.	

1.6 Définir les livrables (Norme 2210.A3) Les livrables ne sont pas limités à la rédaction d'un rapport final. La communication entre les équipes d'audit et le propriétaire du processus est essentielle pour la réussite de la mission.		
1.6.1	Définir les livrables intermédiaires, y compris les premiers constats, les rapports d'étape, les projets de rapport, les dates limites pour les réponses ou les réunions, et le rapport final.	
1.7 Communiquer sur le processus. (Norme 2201.C1) Le processus d'audit doit être clairement communiqué au client.		
1.7.1	Organiser une réunion d'ouverture pour : • Discuter du périmètre d'intervention et des objectifs avec les parties prenantes. • Obtenir les documents et les informations relatifs à la sécurité nécessaires pour réaliser une mission efficace. • Communiquer le calendrier et les livrables.	

Objectif 2 : Identifier et obtenir les documents nécessaires (Norme 2310)

Activités d'audit	Vérifications
2.1 Revue des politiques relatives aux appareils intelligents (y compris BYOD) et à la sécurité.	
2.2 Revue des documents relatifs à l'architecture de l'infrastructure SI.	
2.3 Revue des procédures MAM et MDM.	
2.4 Revue des rapports produits à partir de MAM et MDM.	

Objectif 3 : Comprendre l'environnement des appareils intelligents

Activités d'audit	Vérifications
3.1 L'appareil appartient-il à l'organisation ou est-il apporté par le collaborateur (BYOD) ?	
3.2 Les données de l'organisation sont-elles bien distinctes des données personnelles ?	
3.3 L'usage personnel de l'appareil est-il autorisé (jeux, médias sociaux, etc.) ?	
3.4 Existe-t-il un accord par lequel le collaborateur accepte de se conformer aux politiques de sécurité de l'organisation ?	
3.5 Le collaborateur a-t-il donné son accord pour l'effacement à distance des données de l'appareil ?	
3.6 Le collaborateur accepte-t-il que ses conversations téléphoniques soient enregistrées et écoutées par l'organisation ?	
3.7 Des données confidentielles sont-elles stockées sur l'appareil intelligent ? Dans ce cas, quelles sont les procédures en place pour les contrôler ?	

3.8 Quels sont les types d'appareils intelligents et de systèmes d'exploitation autorisés ?
3.9 Existe-t-il des procédures et des stratégies de sauvegarde pour les appareils intelligents ?
3.10 L'appareil intelligent est-il connecté au réseau de l'organisation ? De quelle façon ?
3.11 Comment les applications mobiles sont-elles intégrées dans l'appareil ? L'organisation développe-t-elle ses propres applications ? L'organisation dispose-t-elle de son propre catalogue d'applications ?

Objectif 4 : Comprendre l'architecture informatique sur laquelle repose l'environnement de l'appareil intelligent

Activités d'audit	Vérifications
4.1 La solution MDM est-elle hébergée dans le *cloud* ou déployée en interne ?	
4.2 La solution est-elle hébergée par un tiers ou est-elle auto-gérée ?	
4.3 Existe-t-il un contrat de tiers avec le prestataire ?	

Objectif 5 : Comprendre les particularités de la sécurité des appareils intelligents

Activités d'audit	Vérifications
5.1 Vérifier si la politique concernant les mots de passe respecte les normes du secteur.	
5.2 Revoir les exigences de chiffrement (notamment pour les données confidentielles) et la façon dont le chiffrement est déployé.	
5.3 Existe-t-il une exigence de contrôle des ports d'un appareil (appareil photo, Bluetooth, Wi-Fi) ?	
5.4 Quelle est la procédure pour l'effacement/le verrouillage et déverrouillage à distance de l'appareil ?	
5.5 Quelle est la procédure en cas de perte de l'appareil ?	
5.6 Comment les appareils sont-ils localisés et surveillés ?	
5.7 Quelle configuration est présente en *mode push* sur l'appareil (VPN, e-mail, etc.) ?	
5.8 Comment est contrôlée l'installation des applications sur l'appareil ? Comment ces dispositifs sont-ils installés ?	
5.9 Quelles options de contrôle et d'audit sont activées ? Quels rapports sont générés ?	

Objectif 6 : Comprendre comment les appareils intelligents sont intégrés à la solution MDM	
Activités d'audit	**Vérifications**
6.1 L'organisation recourt-elle à l'auto-enregistrement ? Comment les utilisateurs enregistrent-ils leur appareil ?	
6.2 Comment les utilisateurs se ré-enregistrent-ils suite à l'achat d'un nouvel appareil ou après avoir remplacé un appareil existant ? Qu'advient-il de l'ancien appareil ? Les données sont-elles effacées de l'appareil ?	
6.3 Comment vérifier que les règles de sécurité adéquates sont bien actives sur l'appareil ?	

Objectif 7 : Comprendre comment les appareils intelligents sont configurés pour les e-mails, les contacts et les carnets d'adresse ?	
Activités d'audit	**Vérifications**
7.1 Comment les e-mails sont-ils synchronisés avec les serveurs de l'organisation ? Sont-ils encodés ?	
7.2 Quand et comment l'anti-virus se déclenche-t-il ?	

Objectif 8 : Comprendre comment les applications sont installées sur les appareils intelligents	
Activités d'audit	**Vérifications**
8.1 Revoir les applications utilisées et la façon dont elles sont stockées et encodées sur les appareils.	
8.2 Revoir le déploiement des applications.	
8.3 Revoir la procédure d'authentification pour les applications. Comment les mots de passe sont-ils authentifiés ? Existe-t-il une procédure d'autorisation pour les collaborateurs utilisant les données de l'organisation ?	

Objectif 9 : Comprendre comment les appareils intelligents sont connectés au réseau de l'organisation	
Activités d'audit	**Vérifications**
9.1 Quel type de connexion à distance est utilisé ?	
9.2 Quelle authentification est utilisée avant l'autorisation d'accès au réseau de l'organisation ?	
9.3 Quels protocoles de chiffrement sont utilisés pour les connexions à distance ?	

Objectif 10 : Comprendre les exigences réglementaires et de conformité liées aux appareils intelligents	
Activités d'audit	**Vérifications**
10.1 Quels rapports et contrôles sont utilisés pour respecter les exigences en termes réglementaire et de conformité (HIPAA, Sarbanes-Oxley, PCI, PII et autres) ?	

Objectif 11 : Comprendre les rapports de gestion liés aux appareils intelligents	
Activités d'audit	**Vérifications**
11.1 Quels rapports sont revus par le management ?	
11.2 Quelles statistiques clés sont contrôlées et revues ?	

Auteurs / Contributeurs

Brad Ames, CRMA, CISA

Frederick Brown, CISA, CRISC

John Bogert, CISA

Michelle Creer, CISA

Jacques Lourens, CIA, CISA, CGEIT, CRISC

Raj Patel, CISA, CISM, CRISC

Sajay Rai, CISM, CISSP

Steve Stein, CIA, CISA

Réviseurs de la traduction :

Bouchra Bajjou

José Bouaniche,

Béatrice Ki-Zerbo, CIA

À propos de l'Institute of Internal Auditors

Porte-parole mondial de la profession d'audit interne, l'Institute of Internal Auditors (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA compte actuellement quelque 185 000 membres dans plus de 170 pays et territoires. Son siège se situe à Lake Mary (Floride) aux États-unis. Plus d'informations sont disponibles sur le site www.globaliia.org ou www.theiia.org.

À propos des lignes directrices complémentaires

Les lignes directrices complémentaires font partie intégrante du Cadre de référence international des pratiques professionnelles (CRIPP) et proposent des recommandations supplémentaires (facultatives) pour la réalisation des activités d'audit interne. Si elles reflètent les *Normes internationales pour la pratique professionnelle de l'audit interne* (les *Normes*), ces lignes directrices complémentaires ne visent pas directement la mise en conformité aux dites *Normes*. Elles couvrent au contraire des domaines particuliers, ainsi que des questions sectorielles, et contiennent des procédures et processus détaillés. Ces lignes directrices ont été officiellement révisées et approuvées par l'IIA.

Guides pratiques

Les guides pratiques constituent un type particulier de lignes directrices complémentaires et détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Dans le cadre des dispositions du CRIPP, la conformité aux guides pratiques est recommandée (mais non obligatoire). Ces guides pratiques ont été officiellement révisés et approuvés par l'IIA.

Le Global Technologies Audit Guide (GTAG) est un type de guide pratique qui aborde, dans un langage courant, une question d'actualité liée à la gestion, au contrôle ou à la sécurité des systèmesd'information.

Pour de plus amples informations sur les documents de référence proposés par l'Institute, vous pouvez consulter notre site Web, www.globaliia.org/standards-guidance ou www.theiia.org/guidance ou www.ifaci.com.

Avertissement

L'Institute of Internal Auditors publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et doit uniquement servir de guide. À ce titre, il doit être utilisé uniquement à des fins d'orientation. L'Institute of Internal Auditors vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'Institute dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

Copyright

Le copyright de ce guide pratique est détenu par l'Institute of Internal Auditors et par l'IFACI pour sa version française.

Pour l'autorisation de reproduction, prière de contacter l'Institute of Internal Auditors à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com.

Avril 2017 - ISBN 978-2-915042-80-1