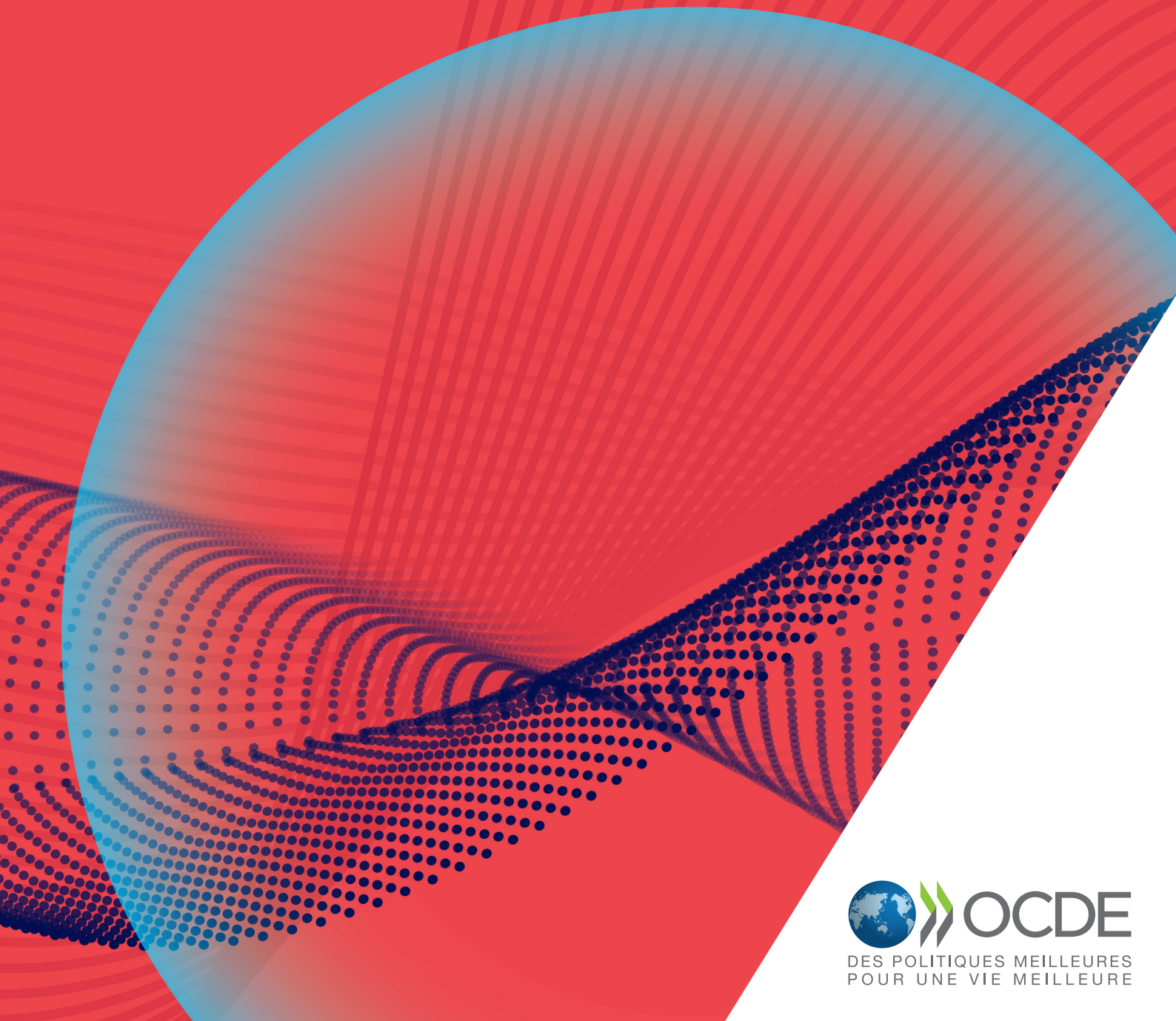
FORUM MONDIAL SUR
LA TRANSPARENCE ET L'ÉCHANGE DE RENSEIGNEMENTS À DES FINS FISCALES

Boîte à outils sur la confidentialité et la gestion de la sécurité de l'information



OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Cette boîte à outils a été préparée par le Secrétariat du Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales.

Table des matières

Table des matières

Abréviations et acronymes

BEPS	Érosion de la base d'imposition et transfert de bénéfices (Base erosion and profit shifting)
CMDB	Base de données de gestion de la configuration (Configuration Management Database)
DLP	Prévention de fuite de données (data loss prevention)
DMZ	Zone démilitarisée (delimitarised zone)
EAR	Échange automatique de renseignements
EF	Exigence fondamentale
Forum mondial	Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales
GSI	Gestion de la sécurité de l'information
OCDE	Organisation de Coopération et de Développement Économiques
PCA	Plan de continuité de l'activité
PDCA	Planifier ; Déployer ; Contrôler ; Agir
PUA	Politique d'utilisation acceptable
RSSI	Responsable de la sécurité des systèmes d'information
SE	Sous-exigence
SGSI	Système de gestion de la sécurité de l'information
DR	Disaster Recovery
DRP	Disaster Recovery Plan

Préface

Maria José Garde
Présidente du Forum mondial

Zayda Manatta
Cheffe du Secrétariat du Forum mondial

La confidentialité et la sécurité de l'information constituent un fondement de la relation entre administrations fiscales et contribuables partout dans le monde. Elles sous-tendent également l'échange de renseignements en matière fiscale entre États, l'un des piliers du système fiscal international et des efforts multilatéraux pour lutter contre les pratiques de fraude et d'évasion fiscales.

La communauté internationale n'aurait pas entériné la Norme d'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale, qui a permis une amélioration sans précédent de la discipline fiscale, sans ses dispositions détaillées en matière de confidentialité et de gestion de la sécurité de l'information.

Depuis 2014, le Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales (le Forum mondial) s'emploie à suivre, évaluer et aider ses membres à mettre en œuvre la norme d'échange automatique de renseignements. Vérifier le respect des exigences de confidentialité et aider les juridictions à s'y conformer est au cœur de ces travaux.

Les membres ont pris note du fait que les administrations fiscales du monde entier prennent la gestion de la sécurité de l'information très au sérieux. À la faveur du processus multilatéral d'examen et d'assistance, un panorama général se dégage des lois sur la confidentialité et des bonnes pratiques en matière de gestion de la sécurité de l'information déjà mises en place dans les juridictions membres, et de la façon dont leurs administrations fiscales intègrent les normes de confidentialité et de sécurité de l'information dans leurs activités.

À l'heure où nous nous efforçons de faire en sorte que davantage de pays en développement puissent bénéficier de l'échange automatique de renseignements, cette boîte à outils sur la confidentialité et la gestion de la sécurité de l'information vise à donner des orientations sur les bonnes pratiques de gestion de la sécurité de l'information qui forment l'épine dorsale des normes du Forum mondial dans ce domaine.

Nous espérons que toutes les administrations fiscales, et notamment celles des pays en développement qui souhaitent appliquer la norme d'échange automatique de renseignements et d'autres formes d'échange, feront bon usage de ces orientations afin de continuellement améliorer le traitement des données échangées et d'autres types de données.

À propos de cette boîte à outils

Cette boîte à outils sur la confidentialité et la gestion de la sécurité de l'information (la « boîte à outils ») a pour but d'aider les pays qui souhaitent participer à l'échange automatique de renseignements en s'assurant qu'ils se conforment aux bonnes pratiques en matière de confidentialité et de protection des données. Elle contient des orientations générales sur le déploiement de cadres juridiques et de gestion de la sécurité de l'information (GSI) propres à garantir la confidentialité des informations sur les contribuables, y compris celles échangées en vertu d'accords internationaux (« renseignements échangés »), conformément aux exigences de la Norme d'échange automatique de renseignements relatifs aux comptes financiers à des fins fiscales (norme EAR)[1]. La mise en œuvre de ses bonnes pratiques en matière de GSI intéresse aussi d'autres types d'échange, comme l'échange de renseignements sur demande, l'échange spontané et l'échange de déclarations pays par pays prévu par le standard de l'Action 13 du projet sur l'érosion de la base d'imposition et transfert de bénéfices.

Cette boîte à outils se divise en quatre parties, à savoir :

- La partie 1 décrit le contexte dans lequel s'inscrit la participation des pays en développement à l'échange automatique de renseignements, et présente les normes de confidentialité et de gestion de la sécurité de l'information en se référant aux « exigences fondamentales » des termes de référence qui régissent les examens par les pairs de la confidentialité et de la protection des données au regard de la norme d'échange automatique de renseignements.
- La partie 2 contient des orientations pour aider les juridictions à s'assurer que leur cadre juridique portant sur la confidentialité des informations des contribuables est approprié et garantit la confidentialité et le bon usage des renseignements échangés en vertu d'un accord international.
- La partie 3 livre des orientations pour aider les administrations fiscales des pays en développement à mettre en place les composantes d'un cadre GSI qui soit conforme aux normes ou aux bonnes pratiques reconnues à l'échelle internationale, ainsi que l'exige la norme d'échange automatique de renseignements. Cette section se divise en six domaines principaux de la GSI (« sous-exigences ») autour desquels s'organisent les exigences du Forum mondial.
- La partie 4 contient des orientations pour aider les juridictions et les administrations fiscales à s'assurer que des dispositions et des processus efficaces sont en place pour remédier aux atteintes à la confidentialité.

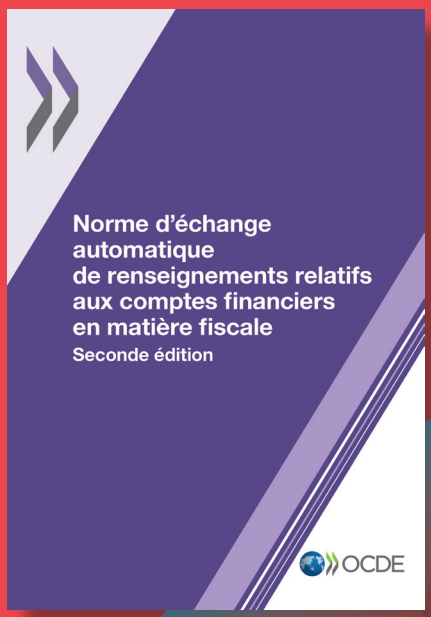
Les annexes contiennent un glossaire des principaux concepts abordés dans la boîte à outils, ainsi qu'une liste de ressources utiles.

1. www.oecd.org/fr/fiscalite/echange-de-renseignements-fiscaux/norme-d-echange-automatique-de-renseignement-relatifs-aux-comptes-financiers-en-matiere-fiscale-seconde-edition-9789264268050-fr.htm

Avertissement

Cette boîte à outils ne prétend pas réunir tous les éléments des normes reconnues internationalement en matière de GSI. En outre, son contenu ne reflète pas nécessairement toutes les options possibles qui s'offrent à une juridiction pour gérer la confidentialité et la sécurité de l'information dans le respect de ces normes. Cette boîte à outils vise uniquement à servir de guide général à la mise en œuvre des composantes fondamentales d'un cadre de confidentialité et de GSI adapté aux administrations fiscales qui participent aux échanges internationaux de renseignements. En définitive, il incombe aux juridictions de mettre en place le cadre juridique et de GSI adapté aux circonstances qui leur sont propres, sur la base des risques spécifiques qu'elles rencontrent en matière de confidentialité et de sécurité de l'information.

1. Introduction



LA CONFIDENTIALITÉ ET LA PROTECTION DES DONNÉES SONT LES PILIERS DE L'ÉCHANGE DE RENSEIGNEMENTS FISCAUX

Les contribuables apprécient l'équité générale qu'offrent la transparence et l'échange de renseignements à des fins fiscales. Dans le même temps, ils attendent des pouvoirs publics qui échangent leurs informations personnelles qu'ils traitent ces informations avec la plus grande diligence. Aussi, la norme d'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale[2], qui s'appuie sur la norme d'échange de renseignements sur demande[3], demande aux juridictions de mettre en place les mécanismes appropriés de confidentialité et de protection des données. Il s'agit pour elles d'établir un cadre juridique qui garantisse la confidentialité et le bon usage des renseignements échangés, ainsi qu'un cadre de gestion de la sécurité de l'information (GSI) qui respecte les normes ou bonnes pratiques reconnues à l'échelle internationale.

Peu après la mise au point de la norme d'échange automatique de renseignements (EAR) en 2014, le Forum mondial l'a entérinée et a déployé un processus destiné à assurer sa mise en œuvre mondiale, à travers un engagement politique collectif à l'appliquer selon un calendrier établi d'un commun accord. Tous les membres du Forum mondial, à l'exception des pays en développement qui n'abritent aucun centre financier, étaient invités à prendre l'engagement d'appliquer la norme d'EAR et de débuter les échanges avec tous les partenaires appropriés intéressés en 2017 ou 2018 (cette expression désigne les juridictions désireuses de recevoir des renseignements et qui se conforment aux exigences attendues en matière de confidentialité et de protection des données). Le Forum mondial a également élaboré un mécanisme d'examen par les pairs afin d'appuyer, de suivre et d'évaluer la mise en œuvre de la norme d'échange automatique de renseignements.

Dans ce contexte, le Forum mondial a mis en place un processus spécifique pour évaluer si les juridictions qui se sont engagées en faveur de l'EAR respectent les exigences en matière de confidentialité et de protection des données, condition préalable à l'obtention de données. Les évaluations sont menées par un groupe d'experts réunissant des praticiens de la GSI expérimentés, issus des administrations fiscales des pays partenaires (coordonnés par le Secrétariat du

2. Veuillez consulter les commentaires sur la section 5 concernant la confidentialité et les mécanismes de protection des données du Modèle d'accord entre autorités compétentes qui fait partie de la norme d'échange automatique de renseignements : https://read.oecd-ilibrary.org/taxation/norme-d-echange-automatique-de-renseignement-relatifs-aux-comptes-financiers-en-matiere-fiscale-seconde-edition_9789264268050-fr#page145

3. www.oecd.org/tax/transparency/documents/handbook-french-eoi-2016-2020.pdf

Forum mondial). Les évaluations de la confidentialité comportent trois volets :

- Une évaluation préalable aux échanges, avant que des données soient reçues pour la première fois (procédure entamée en 2015) ; et
- Une évaluation postérieure aux échanges, qui examine les mécanismes de sécurité portant sur les données échangées automatiquement, une fois celles-ci reçues et utilisées (procédure entamée en 2019).
- Un processus d'évaluations préalable et postérieure aux échanges qui concerne spécifiquement les juridictions pour lesquelles il n'y a pas de réciprocité, au regard du fait qu'elles envoient des données, mais n'en reçoivent pas.

Si des défaillances sont détectées, les juridictions sont invitées à procéder à des améliorations avant de conclure positivement l'évaluation et d'autoriser la réception de renseignements. Si nécessaire, le Secrétariat du Forum mondial fournit une assistance technique visant à apporter des améliorations.

Le risque que les données des administrations fiscales soient compromises ne pouvant être totalement exclu, les processus appliqués par le Forum mondial comportent également un mécanisme en cas de violation des données. Ce mécanisme prévoit un réexamen des dispositifs de sécurité instaurés par la juridiction victime de la violation pour s'assurer qu'ils restent adaptés, et une communication multilatérale pour informer toutes les parties prenantes concernées.

FAIRE EN SORTE QUE LES PAYS EN DÉVELOPPEMENT TIRENT ÉGALEMENT PROFIT DE L'ÉCHANGE AUTOMATIQUE DE RENSEIGNEMENTS

Les membres du Forum mondial qui sont des pays en développement dépourvus de centre financier n'étaient pas obligés d'appliquer la norme d'EAR et de procéder aux premiers échanges d'ici 2018. Bien qu'en principe, ces juridictions soient tenues d'adhérer à la norme en vertu de leurs obligations de membre, elles sont invitées à le faire en suivant un calendrier qui leur est propre (qui peut être établi avec l'aide du Secrétariat du Forum mondial).

Néanmoins, le Forum mondial souhaite que ses membres en développement bénéficient pleinement des avantages découlant de l'EAR afin d'améliorer leur discipline fiscale et de contribuer à mobiliser des ressources intérieures pour leur développement. Aussi le Secrétariat a-t-il mis en place un programme de renforcement des capacités et d'assistance technique pour aider les pays en développement à évaluer leur état de préparation pour l'EAR, la confidentialité et la protection des données étant au cœur du soutien apporté. Ce programme vise non seulement à aider les membres à mettre en place les composantes législatives et administratives essentielles de l'EAR, mais aussi à les préparer à répondre aux exigences de la norme d'EAR et de l'examen de confidentialité par le Forum mondial. Ce programme est décrit dans le Plan d'action du Forum mondial pour la participation des pays en développement à l'échange automatique de renseignements[4].

Le programme prévoit de mener une analyse des lacunes centrée sur la GSI des administrations fiscales par rapport aux exigences en matière de confidentialité et de protection des données pour l'EAR, et de fournir des orientations techniques et une assistance pratique pour y remédier. Disponible sur demande, ce programme d'assistance suppose que les pays qui souhaitent en bénéficier prennent l'engagement politique d'établir un calendrier pratique de déploiement de l'EAR, puis de s'y conformer.

UNE BOÎTE À OUTILS POUR AIDER LES ADMINISTRATIONS FISCALES DES PAYS EN DÉVELOPPEMENT À SE CONFORMER AUX EXIGENCES EN MATIÈRE DE CONFIDENTIALITÉ ET DE PROTECTION DES DONNÉES

Bien qu'une assistance sur mesure en matière de GSI soit proposée individuellement aux membres à leur demande, le Secrétariat du Forum mondial a également préparé cette boîte à outils afin d'aider les administrations fiscales de l'ensemble des pays en développement à établir ou améliorer les éléments fondamentaux de leur cadre de GSI et à gérer en toute sécurité les informations échangées en vertu d'accords fiscaux internationaux.

La structure de cette boîte à outils suit celle des sections consacrées à la confidentialité et à la protection des données de la norme d'EAR, telles qu'intégrées et décrites plus en détail dans les termes de référence pour les évaluations et dans le questionnaire d'évaluation[5]. Cette approche simplifiera la tâche des administrations fiscales amenées à procéder aux améliorations nécessaires de leur système de GSI, tout en les préparant systématiquement à leur évaluation de confidentialité par le Forum mondial.

4. www.oecd.org/tax/transparency/plan-action-aeoi-pays-en-developpement.pdf
5. Les termes de référence peuvent être consultés à l'adresse www.oecd.org/fr/fiscalite/transparence/documents/confidentialite-protection-des-donnees-tdr.pdf. Le questionnaire d'évaluation de la confidentialité et de la protection des données est transmis par le Secrétariat aux personnes autorisées des juridictions, sur demande.

LA NORME D'EAR ET LES EXIGENCES D'ÉVALUATION DU FORUM MONDIAL

La norme d'EAR impose aux juridictions de garantir la confidentialité et la protection des renseignements échangés, et de les utiliser conformément aux dispositions de l'accord d'échange de renseignements. Cette exigence a été intégrée en tant qu'exigence fondamentale (EF) 3 dans les termes de référence applicables à la procédure d'examen par les pairs relatif à l'EAR[6]. L'EF 3 se décline entre trois composantes essentielles (EF 1-3) qui doivent être mises en place, lesquelles se décomposent en plusieurs sous-exigences (SE) illustrées dans le tableau 1. Cette boîte à outils donne des orientations sur chacune des EF et SE.

Tableau 1. **Exigences fondamentales et sous-exigences des évaluations de la confidentialité**

EF 3.1 Les juridictions devraient disposer d'un cadre juridique qui garantisse la confidentialité et le bon usage des renseignements échangés	EF 3.2 Les juridictions devraient disposer d'un cadre de GSI qui soit conforme aux normes ou aux bonnes pratiques reconnues à l'échelle internationale	EF 3.3. Les juridictions devraient adopter des dispositions et des processus propres pour remédier aux atteintes à la confidentialité
• SE 3.1.1 Le cadre juridique interne des juridictions devrait contenir des dispositions suffisantes pour protéger la confidentialité des renseignements des contribuables, y compris des renseignements échangés, et définir les circonstances spécifiques et limitées dans lesquelles ces renseignements peuvent être divulgués et utilisés, ces circonstances étant conformes, s'agissant des renseignements échangés, aux termes de l'instrument d'échange international applicable (bilatéral ou multilatéral) en vertu duquel l'échange a eu lieu	• SE 3.2.1 Les organisations concernées devraient disposer d'un système complet approprié de gestion de la sécurité de l'information • SE 3.2.2 Les organisations concernées devraient établir des contrôles appropriés portant sur les ressources humaines • SE 3.2.3 Les organisations concernées devraient établir des contrôles d'accès physique et logique appropriés • SE 3.2.4 Les organisations concernées devraient établir un mécanisme approprié de sécurité des systèmes d'information • SE 3.2.5 Les organisations concernées devraient protéger l'information de façon adéquate • SE 3.2.6 Les organisations concernées devraient établir un cadre approprié de gestion des opérations, englobant des mécanismes de gestion des incidents, de gestion des changements, de suivi et de vérification	• SE 3.3.1 Les juridictions devraient infliger des pénalités et/ou des sanctions appropriées en cas de divulgation ou d'utilisation non autorisée des renseignements. • SE 3.3.2 Les juridictions devraient appliquer des processus appropriés pour traiter les infractions avérées ou supposées, comportant l'application effective de pénalités ou de sanctions

6. www.oecd.org/fr/fiscalite/transparence/documents/termes-de-reference-echange-automatique.pdf. Les EF 1 et 2 des examens par les pairs ont trait à l'efficacité de la collecte et de l'échange de renseignements au titre de la norme d'EAR. L'EF 1 dispose que les juridictions doivent veiller à ce que toutes les institutions financières déclarantes appliquent les procédures de diligence raisonnable conformément à la Norme commune de déclaration afin d'examiner les comptes financiers dont elles ont la gestion, et qu'elles collectent et déclarent les informations requises. L'EF 2 dispose que les juridictions doivent échanger les renseignements avec tous les partenaires appropriés intéressés, dans les meilleurs délais, en veillant à les collecter, trier, préparer, valider et transmettre conformément à la norme d'EAR.

2. Cadre juridique pour garantir la confidentialité et le bon usage des renseignements échangés (Exigence fondamentale 3.1)

EXIGENCES CONTENUES DANS LES ACCORDS INTERNATIONAUX D'ÉCHANGE

L'assistance administrative mutuelle en matière fiscale suppose que chaque juridiction ait l'assurance que l'autre juridiction traite confidentiellement les renseignements obtenus à la faveur de leur coopération.

Aussi, les accords internationaux d'échange de renseignements contiennent des dispositions sur la confidentialité et sur l'obligation qui est faite aux États contractants, à savoir les juridictions prenant part aux échanges, de tenir secrets ou confidentiels les renseignements échangés, de la même manière que les renseignements obtenus en application de leur législation interne. Les partenaires en matière d'échange de renseignements peuvent suspendre les échanges si des mesures de protection adéquates ne sont pas en place ou, en cas de violation de la confidentialité des renseignements échangés, s'ils estiment que les mesures mise en œuvre pour y remédier ne sont pas satisfaisantes.

L'encadré 1 cite des extraits de différentes dispositions types relatives à la confidentialité contenues dans des accords internationaux dont s'inspirent la plupart des accords internationaux en vigueur. Les juridictions devraient s'efforcer d'intégrer des dispositions équivalentes dans les nouveaux accords d'échange de renseignements conclus avec leurs partenaires.

Ces obligations internationales ont pour corollaire que la confidentialité des renseignements sur les contribuables, y compris des renseignements échangés, doit être protégée par un cadre juridique national et qui des mesures pratiques prises par les juridictions pour garantir la confidentialité.

Faute d'un tel cadre, les partenaires en matière d'échange de renseignements, ainsi que les contribuables, n'auront pas l'assurance que la confidentialité sera protégée et que les violations et atteintes à la confidentialité seront dûment traitées et sanctionnées, même si des mesures pratiques rigoureuses relatives à la GSI sont appliquées.

Dans ce contexte, l'EF 3.1 dispose que les juridictions doivent mettre en place un cadre juridique qui garantisse la confidentialité et le bon usage des renseignements échangés en vertu d'un accord international.

Encadré 1. **Dispositions relatives à la confidentialité contenues dans les accords internationaux types d'échange et dans la Convention concernant l'assistance administrative mutuelle en matière fiscale**

Article 26(2) du Modèle de Convention fiscale de l'OCDE concernant le revenu et la fortune[7]

« Les renseignements reçus en vertu du paragraphe 1 par un État contractant sont tenus secrets de la même manière que les renseignements obtenus en application de la législation interne de cet État et ne sont communiqués qu'aux personnes ou autorités (y compris les tribunaux et organes administratifs) concernées par l'établissement ou le recouvrement des impôts mentionnés dans au paragraphe 1, par les procédures ou poursuites concernant ces impôts, par les décisions sur les recours relatifs à ces impôts, ou par le contrôle de ce qui précède. Ces personnes ou autorités n'utilisent ces renseignements qu'à ces fins. Elles peuvent révéler ces renseignements au cours d'audiences publiques de tribunaux ou dans des jugements. Nonobstant ce qui précède, les renseignements reçus par un État contractant peuvent être utilisés à d'autres fins si la législation des deux États l'autorise et si l'autorité compétente de l'État qui fournit ces renseignements autorise cette utilisation. »

Article 8 du Modèle d'accord de l'OCDE sur l'échange de renseignements en matière fiscale[8]

« Tout renseignement reçu par une partie contractante en vertu du présent Accord est tenu confidentiel et ne peut être divulgué qu'aux personnes ou autorités (y compris les tribunaux et les organes administratifs) relevant de la compétence de la partie contractante qui sont concernées par l'établissement, la perception, le recouvrement ou l'exécution des impôts visés par le présent Accord, ou par les poursuites ou les décisions en matière de recours se rapportant à ces impôts. Ces personnes ou autorités ne peuvent utiliser ces renseignements qu'à ces fins. Elles peuvent en faire état lors d'audiences publiques de tribunaux ou dans des décisions judiciaires. Les renseignements ne peuvent être divulgués à toute autre personne, entité ou autorité ou à toute autre autorité étrangère sans l'autorisation écrite expresse de l'autorité compétente de la partie requise. »

Article 26(2) du Modèle de Convention fiscale des Nations Unies concernant le revenu et la fortune[9]

« Les renseignements reçus par un État contractant sont tenus secrets de la même manière que les renseignements obtenus en application de la législation interne de cet État, et ils ne sont communiqués qu'aux personnes ou autorités (y compris les tribunaux et organes administratifs) concernés par l'établissement ou le recouvrement des impôts visés au paragraphe 1, par les procédures ou poursuites concernant ces impôts, ou par les décisions sur les recours relatifs à ces impôts. Ces personnes ou autorités n'utilisent ces renseignements qu'à ces fins, mais peuvent faire état de ces renseignements au cours d'audiences publiques de tribunaux ou dans des jugements Nonobstant ce qui précède, les renseignements reçus par un État contractant peuvent être utilisés à d'autres fins lorsque cette possibilité résulte des lois des deux États et lorsque l'autorité compétente de l'État qui fournit les renseignements autorise cette utilisation. »

Article 22 (Secret) de la Convention concernant l'assistance administrative mutuelle en matière fiscal[10]

« 1. Les renseignements obtenus par une Partie en application de la présente Convention sont tenus secrets et protégés dans les mêmes conditions que celles prévues pour les renseignements obtenus en application de la législation de cette Partie et, en tant que de besoin pour assurer le niveau nécessaire de protection des données à caractère personnel, conformément aux garanties qui peuvent être spécifiées par la Partie fournissant les renseignements comme étant requises au titre de sa législation.

2. Ces renseignements ne sont communiqués en tout cas qu'aux personnes ou autorités (y compris les tribunaux et les organes administratifs ou de surveillance) concernées par l'établissement, la perception ou le recouvrement des impôts de cette Partie, par les procédures ou les poursuites pénales concernant ces impôts, ou par les décisions sur les recours se rapportant à ces impôts ou par le contrôle de ce qui précède. Seules lesdites personnes ou autorités peuvent utiliser ces renseignements et uniquement aux fins indiquées ci-dessus. Elles peuvent, nonobstant les dispositions du paragraphe 1, en faire état au cours d'audiences publiques de tribunaux ou dans des jugements concernant lesdits impôts.

3. [...]

4. Nonobstant les dispositions des paragraphes 1, 2 et 3, les renseignements obtenus par une Partie peuvent être utilisés à d'autres fins lorsque l'utilisation de tels renseignements à de telles fins est possible selon la législation de la Partie qui fournit les renseignements et que l'autorité compétente de cette Partie consent à une telle utilisation. Les renseignements fournis par une Partie à une autre Partie peuvent être transmis par celle-ci à une troisième Partie, sous réserve de l'autorisation préalable de l'autorité compétente de la première Partie. »

7. https://read.oecd-ilibrary.org/taxation/modele-de-convention-fiscale-concernant-le-revenu-et-la-fortune-version-abregee-2017_mtc_cond-2017-fr#page50
8. www.oecd.org/fr/fiscalite/echange-de-renseignements-fiscaux/33977677.pdf
9. www.un.org/esa/ffd/wp-content/uploads/2015/02/UN_Model2011_UpdateFr.pdf
10. https://read.oecd-ilibrary.org/taxation/la-convention-multilaterale-concernant-l-assistance-administrative-mutuelle-en-matiere-fiscale_9789264115682-fr#page26

En outre, les accords internationaux d'échange de renseignements contiennent des dispositions qui limitent la liste des personnes autorisées à consulter les renseignements échangés et les utilisations qui peuvent en être faites (encadré 1). En général, la communication des renseignements est limitée aux personnes ou autorités (y compris les tribunaux et les organes administratifs) concernées par :

- l'établissement,
- le recouvrement,
- les procédures,
- les poursuites, et
- les décisions sur les recours

concernant les impôts sur lesquels des renseignements peuvent être échangés en vertu de l'accord applicable.

Les renseignements échangés peuvent aussi être communiqués au contribuable, à son représentant ou à un témoin. Ils peuvent également être transmis aux autorités publiques ou judiciaires chargées d'autoriser la diffusion de ces renseignements au contribuable, à son représentant ou aux témoins. Les tribunaux et organes administratifs concernés par les questions fiscales mentionnées ci-dessus peuvent révéler ces renseignements lors d'audiences ou dans leurs jugements. Une fois les renseignements échangés devenus publics, ils peuvent être utilisés à d'autres fins.

En résumé, les accords qui prévoient l'échange de renseignements en matière fiscale autorisent généralement la divulgation et l'utilisation des renseignements échangés à des fins fiscales.

Néanmoins, les partenaires en matière d'échange de renseignements peuvent s'entendre pour autoriser la divulgation et l'utilisation des renseignements échangés à d'autres fins, par exemple pour faciliter les enquêtes et les poursuites dans les affaires de blanchiment de capitaux ou de financement du terrorisme. En pareils cas, ces autres finalités doivent être compatibles avec le droit national des partenaires en matière d'échange de renseignements, et la juridiction qui reçoit les renseignements doit préalablement solliciter l'autorisation de l'autorité compétente de la juridiction qui les fournit pour pouvoir les communiquer et les utiliser à des fins non fiscales. La Convention multilatérale concernant l'assistance administrative mutuelle en matière fiscale prévoit cette possibilité (voir l'encadré 1).

Dans ce contexte, une autorité compétente est la personne ou l'autorité publique désignée par une juridiction comme étant compétente pour échanger des renseignements conformément à un accord international.

SOUS-EXIGENCE 3.1.1 : UN CADRE JURIDIQUE QUI GARANTIT LA CONFIDENTIALITÉ ET LE BON USAGE DES RENSEIGNEMENTS ÉCHANGÉS

Au regard des exigences de confidentialité contenues dans les accords internationaux d'échange de renseignements, la SE 3.1.1 dispose que le cadre juridique national de chaque juridiction devrait contenir des dispositions suffisantes pour protéger la confidentialité des renseignements des contribuables, y compris des renseignements échangés, et définir les circonstances spécifiques et limitées dans lesquelles ces renseignements peuvent être divulgués et utilisés, ces circonstances devant être conformes, s'agissant des renseignements échangés, aux termes de l'accord international d'échange de renseignements applicable (bilatéral ou multilatéral) en vertu duquel l'échange a eu lieu.

Aussi, la SE 3.1.1 comporte deux principaux aspects :

- Un cadre juridique doit être mis en place pour protéger la confidentialité des informations des contribuables, y compris celle des renseignements échangés.
- Le cadre juridique doit prévoir la divulgation et l'utilisation des renseignements échangés dans des circonstances limitées uniquement, et dans le respect des termes convenus dans l'accord international en vertu duquel ils ont été échangés.

Cadre juridique protégeant la confidentialité des informations des contribuables, y compris des renseignements échangés

Le cadre juridique national d'une juridiction doit prévoir la confidentialité ou le secret des informations des contribuables, à savoir les informations qui concernent les revenus, les dépenses, les comptes, l'impôt dû, les détails personnels, les affaires commerciales ou d'autres aspects pertinents des contribuables qu'une administration fiscale peut avoir à traiter dans l'exercice de ses fonctions.

Les règles de confidentialité peuvent être contenues dans des textes de loi, des textes ou décrets d'application ou des instructions administratives. Quel que soit l'instrument législatif employé, les règles doivent être juridiquement contraignantes.

Plus précisément, le droit national devrait :

- Indiquer que les informations des contribuables traitées par l'administration fiscale sont confidentielles ou secrètes.
- Contraindre l'ensemble du personnel (agents permanents, temporaires ou sous contrat) à traiter de la façon la plus secrète et confidentielle possible les informations des contribuables dont il peut avoir connaissance au cours de son travail.
- Garantir que les obligations de confidentialité ou de secret s'appliquent au personnel pendant toute la durée de son engagement, et même après, en cas de transfert à d'autres fonctions, de départ en retraite, de fin de contrat ou d'événement similaire mettant un terme au traitement des informations des contribuables (cet aspect est examiné en détail dans la SE 3.2.2 portant sur le contrôle des ressources humaines).

Encadré 2. **Exemples d'aspects couverts par une législation sur la confidentialité**

Le cadre juridique de la juridiction A comporte diverses lois contenant des dispositions sur la confidentialité qui couvrent les renseignements fiscaux. La loi sur l'impôt sur le revenu impose une obligation générale à tous les agents de l'administration fiscale (sous-traitants compris) de garantir la confidentialité des informations des contribuables traitées dans l'exercice de leurs fonctions. En outre, la loi sur les secrets d'État interdit la divulgation d'informations secrètes par des agents publics ou des sous-traitants en exercice ou ayant cessé leurs fonctions.

La loi sur l'emploi public de la juridiction B impose une obligation de confidentialité à tous les agents publics (y compris aux agents temporaires et aux sous-traitants qui rendent des services aux autorités publiques). Le code de conduite des agents publics exige la confidentialité de toutes les informations dont ils peuvent avoir connaissance au cours de leur période d'emploi. Concernant les renseignements échangés, la loi sur la coopération fiscale internationale vise spécifiquement tous les agents et sous-traitants qui travaillent sur un aspect quelconque de l'échange de renseignements (y compris ceux qui fournissent des services informatiques) et les inclut dans le champ des dispositions générales sur la confidentialité des informations fiscales.

- Prévoir des pénalités ou des sanctions visant à dissuader et à punir les violations ou atteintes à la confidentialité (les pénalités et sanctions sont examinées en détail dans la SE 3.3.1).

Les règles de confidentialité des données fiscales peuvent figurer dans la législation fiscale, dans des législations de portée plus générale (lois régissant l'emploi public ou les obligations de service public, par exemple), les lois de protection de la vie privée ou des données et/ou d'autres lois (voir des exemples dans l'encadré 2).

Dans certaines juridictions, les dispositions générales afférentes à la confidentialité des informations fiscales peuvent être suffisamment larges pour couvrir les renseignements échangés. Tel serait le cas, par exemple, d'une disposition contenue dans une législation fiscale qui impose une obligation de confidentialité ou de secret aux agents publics ou aux personnes engagées par l'administration fiscale concernant les renseignements des contribuables dont ils peuvent avoir connaissance dans l'exercice de leurs fonctions, quelle que soit la source de ces renseignements (source nationale ou instrument d'échange de renseignements), et que le contribuable soit un ressortissant national ou un résident fiscal étranger.

Si les dispositions générales ne couvrent pas les renseignements échangés, les juridictions devront adopter des dispositions spécifiques garantissant la protection juridique de la confidentialité de ces renseignements.

Divulgation et utilisation appropriées des renseignements conformément aux accords internationaux d'échange de renseignements

Le droit national de nombreuses juridictions autorise la communication des informations des contribuables aux autorités publiques non fiscales. Par exemple, il n'est pas rare que les lois autorisent la divulgation de certaines informations sur les contribuables aux :

- Organismes chargés des enquêtes et de l'application des lois, tels que les autorités de lutte contre la corruption et contre le blanchiment de capitaux, et les autorités douanières.
- Organismes de sécurité sociale aux fins de gérer les prestations sociales.
- Membres du public le cas échéant, conformément à la législation sur la liberté de l'information.

Cadre juridique pour garantir la confidentialité et le bon usage des renseignements échangés (Exigence fondamentale 3.1)

Comme en général les accords internationaux d'échange de renseignements prévoient une divulgation et une utilisation dans des circonstances plus limitées, les juridictions doivent veiller à ce que les obligations visées par leurs accords d'échange de renseignements prennent effet et soient contraignantes au sein de leur cadre juridique national, de sorte que les renseignements échangés soient divulgués et utilisés uniquement en vertu des conditions convenues avec leurs partenaires.

Les juridictions donnent effet à leurs obligations internationales (y compris de confidentialité) par différents moyens (voir des exemples dans l'encadré 3). Une approche consiste à modifier la législation interne de façon à ce que le respect des obligations visées par les accords internationaux soit garanti dans le droit national. Dans certaines juridictions, les obligations juridiques internationales prévalent sur le droit national en cas d'incohérence, en vertu des règles sur la hiérarchie des lois ou de la constitution. Dans d'autres juridictions, les obligations découlant des accords internationaux sont mises en œuvre de telle sorte qu'en cas de conflit avec le droit national, c'est l'accord international qui prévaut. Certains pays combinent ces deux approches.

Les juridictions peuvent compléter les dispositions juridiques relatives à la divulgation et à l'utilisation des renseignements échangés par des instructions sur la procédure à suivre pour divulguer ou utiliser ces renseignements à des fins non fiscales, lorsque cela est autorisé. Ces instructions peuvent préciser qu'il est nécessaire d'obtenir l'autorisation de l'autorité compétente du partenaire en matière d'échange de renseignements qui a fourni les renseignements, et de veiller à ce que la divulgation et l'utilisation des renseignements soient compatibles avec les lois des deux parties.

Encadré 3. **Exemples de législation donnant effet aux accords internationaux d'échange de renseignements**

Dans la juridiction A, en cas d'incohérence entre le droit national et les accords internationaux, la législation qui transcrit les accords internationaux dans le droit interne précise que l'accord international prévaut.

Dans la juridiction B, une législation dispose que toute restriction applicable à l'utilisation des renseignements échangés convenue avec une juridiction étrangère ou imposée par une juridiction étrangère s'applique, même si elle est contraire au droit national.

3. Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

LA NÉCESSITÉ D'UN CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

Les protections juridiques prévues par les accords internationaux et le droit national ne trouvent leur utilité que si des pratiques et procédures sont mises en place pour qu'elles prennent effet. Par conséquent, l'EF 3.2 exige des juridictions qu'elles se dotent d'un cadre de GSI qui soit conforme aux normes et bonnes pratiques reconnues internationalement et qui assure la protection des renseignements échangés.

Ce cadre regroupe une série de dispositions en matière de gouvernance, de politiques, de procédures, de pratiques et de contrôles de sécurité. Un contrôle de sécurité est une mesure visant à atténuer ou à éliminer un risque posé à la sécurité : il peut s'agir d'une procédure, d'un composant matériel ou d'un logiciel, entre autres.

La norme d'EAR énonce les exigences à satisfaire pour mettre en place un cadre de GSI exhaustif, étant donné la nature confidentielle des renseignements échangés, leur transmission par voie électronique et les importants volumes concernés. En effet, des milliers de dossiers de comptes financiers peuvent entrer dans les systèmes des administrations fiscales et être traités par divers processus, systèmes informatiques et intervenants. Ces renseignements présentent donc intrinsèquement des risques significatifs, qu'ils résultent de leur consultation non autorisée par le personnel ou de cyberattaques ciblées, et qui peuvent entraîner des atteintes à la confidentialité faute de mesures adéquates pour les atténuer.

Les divers contrôles appliqués à ces processus, systèmes et intervenants – par le biais du cadre de GSI – tendent à réduire les risques et les menaces pesant sur les informations et à créer une « culture de protection » au sein de l'administration fiscale.

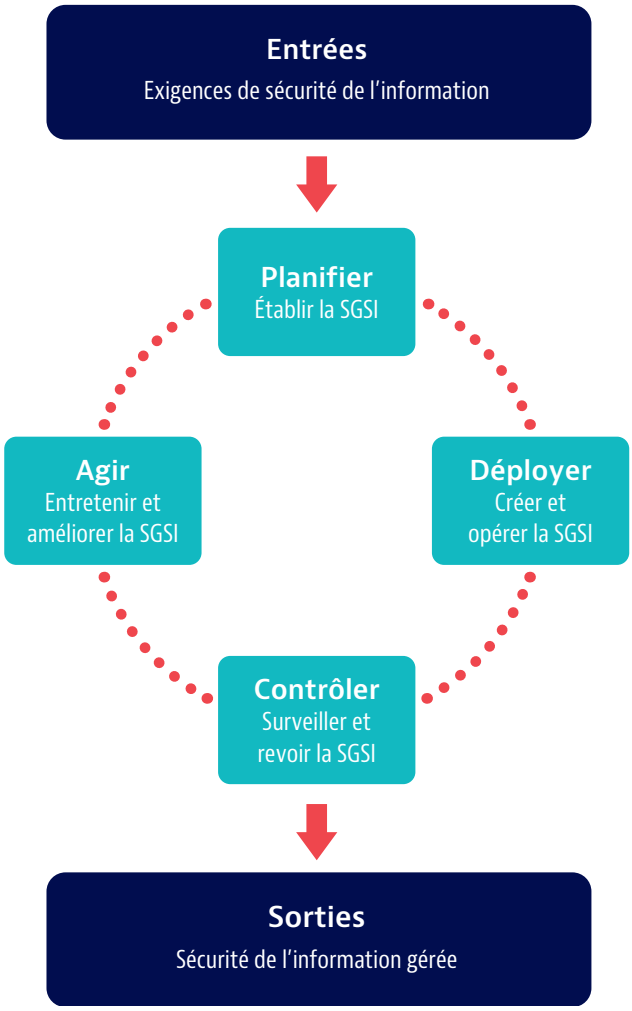
NORMES ET BONNES PRATIQUES RECONNUES INTERNATIONALEMENT

En gestion de la sécurité de l'information, ces normes et pratiques désignent notamment la « suite ISO/CEI 27000 », famille de normes publiée conjointement par l'Organisation internationale de normalisation (ISO) et par la Commission électrotechnique internationale (CEI), ou d'autres normes équivalentes. Les administrations fiscales du monde entier s'appuient sur diverses normes nationales ou internationales, mais il n'existe aucune norme universellement admise qui régisse la gestion de la sécurité de l'information, même si la suite ISO/CEI 27000 est la plus souvent citée dans les travaux du Forum mondial.

Bien que complexe en termes de contenu, cette suite de normes peut être simplifiée dans sa forme à l'aide d'un

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

FIGURE 1. **Cycle PDCA en gestion de la sécurité de l'information**



processus largement reconnu qui consiste en un cycle itératif d'amélioration continue, désigné par l'acronyme PDCA pour Planifier, Déployer, Contrôler, Agir. Celui-ci met l'accent sur le fait que, face à des menaces qui évoluent constamment, la protection des informations doit être améliorée en continu.

Le cycle PDCA consiste à élaborer et à mettre en œuvre un cadre de GSI, à planifier les contrôles requis et à les appliquer tels qu'ils ont été prévus, à s'assurer qu'ils fonctionnent correctement et à les revoir continuellement pour améliorer leurs performances tout en corrigeant leurs lacunes (voir la figure 1).

UN CADRE DE GSI POUR L'ÉCHANGE DE RENSEIGNEMENTS EN MATIÈRE FISCALE

La norme d'EAR et les évaluations de confidentialité exigent des administrations fiscales qu'elles prouvent que leurs pratiques sont conformes aux normes de la suite ISO/CEI 27000 ou qu'elles ont mis en place un cadre de sécurité de l'information équivalent[11] et que les données sur les contribuables obtenues en vertu d'un accord international d'échange de renseignements sont protégées par ce cadre.

Les normes de cette suite ont un vaste champ d'application et ne visent pas spécifiquement les administrations fiscales. Elles ont été élaborées pour permettre à tout type d'organisation de mettre en œuvre un cadre de GSI adéquat et de faire valoir sa certification de sécurité auprès d'autres organisations.

Lors de ses évaluations de confidentialité menées dans le cadre de la norme d'EAR, le groupe d'experts du Forum mondial s'est appuyé sur la suite ISO/CEI 27000 afin de dresser un tableau exhaustif, au niveau mondial, des risques auxquels sont exposées les administrations fiscales en matière de sécurité des données et de leurs bonnes pratiques concernant l'atténuation de ces risques.

Afin de faciliter le plus possible le respect des normes internationales aux fins de l'administration de l'impôt et de l'échange des renseignements, l'EF 3.2 a été subdivisé en six SE (de 3.2.1 à 3.2.6), qui correspondent globalement à la manière dont les administrations fiscales articuleraient normalement le développement de leur système de GSI en utilisant le cycle PDCA comme référence.

- La SE 3.2.1, qui énonce les grandes lignes, correspond aux parties « Planifier » et « Agir » du cycle PDCA. Il prévoit que les administrations fiscales et autres autorités responsables de l'échange de renseignements en matière fiscale (« organisations concernées ») doivent mettre en place un cadre et une politique de GSI, mais aussi un cadre pour gérer les risques et un autre pour la continuité des activités.
- Les SE 3.2.2 à 3.2.5 correspondent à la partie « Déployer » du cycle PDCA :
  - La SE 3.2.2 décrit les mesures de sécurité applicables aux ressources humaines (personnel interne et sous-traitants externes), à savoir notamment les informer de leurs obligations en matière de confidentialité et de protection des renseignements fiscaux, vérifier correctement leurs antécédents, leur délivrer des formations et des communications de

11. Reposant sur d'autres bonnes pratiques internationales telles que la Special Publication (SP) 800-53 du NIST, CSF. Les autres standards internationaux pertinents pouvant être utilisés conformément à leur champ d'application spécifique sont notamment les Objectifs de contrôle de l'information et des technologies connexes (COBIT), le référentiel COSO du Committee of Sponsoring Organisations of the Treadway Commission et le cadre de l'ITIL (Information Technology Infrastructure Library).

sensibilisation adéquates, et faire en sorte qu'elles n'aient plus accès aux informations sensibles au terme de leur période d'emploi.

- La SE 3.2.3 définit les contrôles requis pour gérer les accès aux systèmes informatiques (« accès logique ») et aux locaux (« accès physique ») afin que les renseignements soient accessibles selon le principe du « besoin d'en connaître ».

- La SE 3.2.4 précise les mesures à prendre pour sécuriser l'environnement informatique, notamment l'infrastructure, les réseaux, les applications, les postes de travail et les équipements.

- La SE 3.2.5 vise les mesures de protection des renseignements ou des données elles-mêmes, ainsi que les procédures de classification des données et de mise en place de protections adaptées à leurs niveaux de confidentialité et de sensibilité (par exemple, stockage physique sécurisé pour les documents papier et chiffrement des données numériques).

- La SE 3.2.6 coïncide avec la partie « Contrôler » du cycle PDCA. Il exige que les contrôles de sécurité fassent l'objet d'un suivi pour s'assurer qu'ils sont appliqués correctement (partie « Déployer »), par la journalisation et la consignation des accès aux données et aux systèmes physiques et numériques ainsi que de leur utilisation. En outre, pour vérifier que ces contrôles fonctionnent efficacement, des informations doivent être recueillies à partir d'autres sources, notamment via des audits et le signalement des incidents de sécurité. Enfin, les contrôles doivent être intégrés aux processus de gestion du changement, et une fonction d'audit interne et externe doit être mise en place.

Dans cette boîte à outils, ces SE servent de structure à l'EF 3.2, comme indiqué dans le tableau 2 :

Pour aider les administrations fiscales qui s'inspirent déjà de la suite ISO/CEI 27000 ou de normes équivalentes, la figure 2 présente les correspondances entre l'EF 3.2 (cadre de GSI) et la norme ISO/CEI 27001.

ÉTAPES MAJEURES DE LA MISE EN ŒUVRE D'UN CADRE DE GSI

Comme cette boîte à outils a pour but d'aider les administrations fiscales des pays en développement à élaborer un cadre de GSI conforme aux bonnes pratiques et aux normes internationales, cette section explique brièvement les grandes étapes à suivre pour mettre en œuvre ce cadre. Il est possible que ces administrations doivent répéter ce cycle à mesure que leur approche en matière de sécurité gagne en maturité.

Étape 1 : définition du champ d'application du cadre de GSI

Les juridictions ont le choix entre deux approches pour définir la portée de l'application de ce cadre à l'échange de renseignements. Celle à privilégier sera fonction de la maturité et de la complexité des opérations de leur administration fiscale, de leurs systèmes informatiques, de leurs contrôles de sécurité et de leur modalité d'échange de renseignements, à savoir automatique (réciproque ou non réciproque), sur demande ou spontané. La SE 3.2.1.1, portant sur le cycle de vie des informations, aborde ces deux approches :

- définir le cadre de GSI pour qu'il porte sur l'ensemble des opérations de l'administration fiscale et l'appliquer aux renseignements échangés ;

- le limiter dans un premier temps à un périmètre sécurisé réservé aux opérations de l'administration qui traitent les renseignements échangés.

Tableau 2. **Structure de l'EF 3.2 (cadre de GSI)**

<table>
<tr><td>Planifier, Agir</td><td colspan="2">Sous-exigence 3.2.1 Les organisations concernées devraient disposer d'un système complet approprié de gestion de la sécurité de l'information.</td></tr>
<tr><td rowspan="2">Déployer</td><td>Sous-exigence 3.2.2 Les organisations concernées devraient établir des contrôles appropriés portant sur les ressources humaines.</td><td>Sous-exigence 3.2.3 Les organisations concernées devraient établir des contrôles d'accès physique et logique appropriés.</td></tr>
<tr><td>Sous-exigence 3.2.4 Les organisations concernées devraient établir un mécanisme approprié de sécurité des systèmes d'information.</td><td>Sous-exigence 3.2.5 Les organisations concernées devraient protéger l'information de façon adéquate.</td></tr>
<tr><td>Contrôler</td><td colspan="2">Sous-exigence 3.2.6 Les organisations concernées devraient établir un cadre approprié de gestion des opérations, englobant des mécanismes de gestion des incidents, de gestion des changements, de suivi et de vérification.</td></tr>
</table>

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Étape 2 : définition d'une politique de GSI

La politique de GSI documente l'engagement de l'encadrement supérieur de l'administration fiscale à assurer une protection solide aux informations, dont les renseignements échangés. Elle définit les principes directeurs de cette sécurité ainsi que les principaux processus, procédures et contrôles mis en œuvre à cet égard. Elle précise en outre les responsabilités de haut niveau et les ressources de l'administration fiscale mobilisées pour ce faire. La politique de GSI prévoit également des revues régulières qui permettront de l'améliorer en l'adaptant au degré de maturité de l'approche en matière de sécurité de l'information de l'administration fiscale.

Étape 3 : identification des risques posés à la sécurité

La mise en œuvre d'un cadre et d'une politique de GSI solides passe avant tout par l'identification systématique des risques pesant sur les informations détenues par l'administration fiscale. Un risque est un ensemble de circonstances (scénario) dans lesquelles une menace est susceptible d'exploiter une vulnérabilité d'un actif donné. Les administrations doivent avoir une vision claire des principaux actifs concernés par l'EAR et doivent évaluer rigoureusement les menaces et vulnérabilités liées à ces actifs.

La méthodologie adoptée pour l'évaluation des risques doit permettre d'identifier tous ceux qui découlent des différentes menaces et vulnérabilités, d'en analyser l'impact et de déterminer la meilleure manière de les traiter, c'est-à-dire les contrôles à appliquer pour atténuer les risques identifiés en tenant compte de leur impact estimé. La gestion des risques liés à la sécurité des informations est examinée plus en détail dans la SE 3.2.1.4.

Étape 4 : établissement de politiques, processus et procédures spécifiques pour les domaines pertinents

Une fois les risques identifiés et les contrôles à utiliser pour les traiter établis, l'administration fiscale doit transposer et documenter les mesures qu'elle appliquera dans des politiques, processus et/ou procédures par domaine. L'encadré 4 présente une liste non exhaustive d'exemples de politiques de sécurité qui peuvent être utilisées.

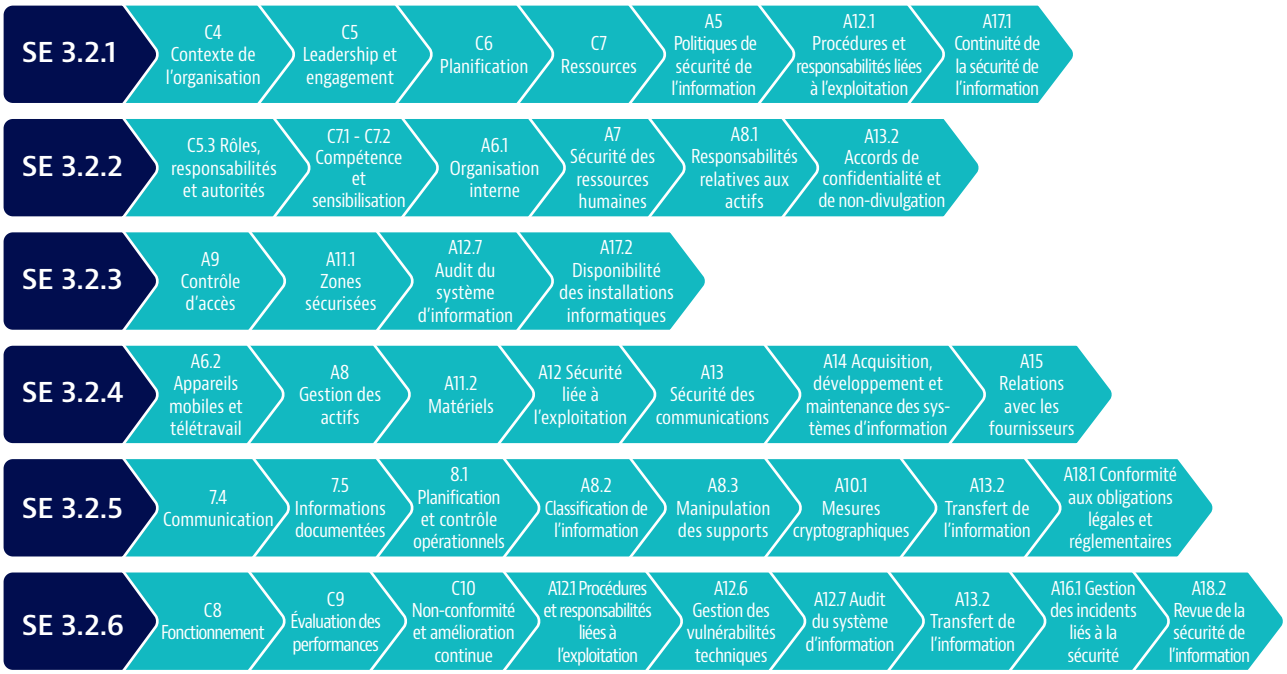
Étape 5 : formation du personnel

L'ensemble du personnel impliqué dans la GSI (et l'échange de renseignements) doit être dûment formé aux politiques, processus, procédures et contrôles mis en place pour traiter les risques posés à la sécurité des informations, afin qu'il les applique correctement.

Étape 6 : vérification de l'application efficace du système de GSI

L'administration fiscale doit vérifier régulièrement si le

FIGURE 2. **Correspondances entre l'EF 3.2 (cadre de GSI) et la norme ISO/CEI 27001**



personnel utilise le système de GSI (SGSI), c'est-à-dire l'ensemble des politiques, processus, procédures et contrôles de sécurité propres à un domaine qui constituent le cadre de GSI (voir les définitions fournies au tableau 3 et les points abordés dans la SE 3.2.1.3), mais aussi si ces contrôles fonctionnent efficacement.

Les sections suivantes de cette boîte à outils expliquent comment appliquer chacune des SE (de 3.2.1 à 3.2.6) et ainsi mettre en place un cadre de GSI conforme aux normes reconnues à l'échelle internationale.

SOUS-EXIGENCE 3.2.1 : CADRE DE GSI GLOBAL

La SE 3.2.1 requiert que les administrations fiscales définissent une stratégie et une politique de GSI globales ainsi qu'un cadre de gestion des risques. Cela inclut les structures organisationnelles de même que les objectifs et principes de sécurité généraux qui constituent le cadre de GSI. Il correspond aux volets « Planifier » et « Agir » du cycle PDCA et sert de plan directeur à la mise en œuvre du SGSI (c'est-à-dire l'ensemble des politiques, procédures et contrôles par domaine qui forment le cadre de GSI). Si le cadre de GSI est inadéquat, il est fort possible que les risques pesant sur la sécurité des informations ne soient pas contrés efficacement.

Cette SE est elle-même subdivisée en cinq SE :

- **Sous-exigence 3.2.1.1** : garantir la mise en place d'un cadre de GSI adapté à l'échange de renseignements exige avant tout des administrations fiscales qu'elles comprennent clairement le cycle de vie des renseignements échangés en leur possession, et qu'elles s'engagent à assurer la confidentialité et le bon usage de telles informations.
- **Sous-exigence 3.2.1.2** : qu'une administration fiscale élabore un cadre de GSI couvrant l'ensemble de ses opérations ou uniquement celles qui traitent les renseignements échangés, l'encadrement supérieur doit s'engager pleinement à respecter le cadre de GSI global. En principe, cet engagement est formulé par écrit dans une politique de GSI.
- **Sous-exigence 3.2.1.3** : l'administration fiscale doit également veiller à ce que le cadre de GSI soit intégré à ses processus concernés et soutenu par des systèmes de sécurité et des mécanismes opérationnels adéquats.
- **Sous-exigence 3.2.1.4** : elle doit se doter d'un SGSI solide, fondé sur les risques et les menaces auxquels elle est exposée, pour éviter d'utiliser à mauvais escient des ressources rares et précieuses.
- **Sous-exigence 3.2.1.5** : elle doit définir et gérer les scénarios de risque susceptibles d'entraver la continuité de ses activités.

Encadré 4. **Liste non exhaustive de politiques de sécurité pour différents domaines**

Une politique est un document par lequel une administration fiscale précise la mise en œuvre de processus, procédures et contrôles de sécurité dans un domaine donné. Les principaux domaines sont :

- Politique de continuité des activités (SE 3.2.1.5) ;
- Politique de sécurité relative aux ressources humaines (SE 3.2.2) ;
- Politique de gestion des accès (SE 3.2.3) ;
  - Politique de sécurité des accès physiques (SE 3.2.3.1 et 3.2.3.2) ;
  - Politique de sécurité des accès logiques (SE 3.2.3.3 et 3.2.3.4) ;
- Politique de sécurité informatique (SE 3.2.4.2) ;
  - Politique de protection contre les attaques malveillantes ;
  - Politique de journalisation et de surveillance ;
- Politique de gestion des actifs (SE 3.2.4.3) ;
- Politique de classification des informations (SE 3.2.5) ;
- Politique du bureau propre (SE 3.2.5) ;
- Politique de cryptographie (SE 3.2.5) ;
- Politique de gestion du changement (SE 3.2.6.5) ;
- Politique de gestion des incidents de sécurité (SE 3.2.6.6).

Le tableau 3 présente les définitions des principaux concepts abordés dans la SE 3.2.1.

Sous-exigence 3.2.1.1. Compréhension claire du cycle de vie des renseignements échangés et engagement à assurer leur confidentialité et leur bon usage

L'objectif des évaluations de confidentialité consiste à déterminer l'aptitude des administrations fiscales à se voir confier des types spécifiques d'informations sur les contribuables, à savoir des renseignements échangés au titre de la norme d'EAR. C'est pourquoi, en premier lieu, la SE 3.2.1 énonce ce qui est attendu des administrations fiscales concernant la gestion des différents types de données généralement transmises à d'autres administrations fiscales, en vertu d'accords internationaux d'échange de renseignements.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Tableau 3. **Définitions des principaux concepts**

Concept	Description
Actif	Tout élément de valeur qui contribue à l'exécution de processus et à la production de résultats. Il peut notamment s'agir d'informations, de personnes, de services, d'équipements ou de systèmes.
Atténuation du risque	Application active de mesures visant à réduire l'impact d'un risque ou la probabilité qu'il se concrétise.
Cadre de GSI	Cadre de gestion de la sécurité de l'information, à savoir les structures organisationnelles et principes généraux de cette sécurité, visant à orienter les administrations fiscales vers la réalisation des objectifs de GSI, selon une approche fondée sur le risque. La responsabilité de ce cadre incombe ultimement à l'encadrement supérieur de l'administration fiscale.
Conventions de dénomination	Règles régissant la manière dont sont désignées les informations afin de les discerner clairement les unes des autres.
Gestion de la continuité des activités	Processus de gestion visant à assurer la poursuite des activités dans le cas où un événement quelconque perturberait le fonctionnement normal.
Politique	Énoncé par lequel une administration fiscale documente la mise en œuvre de processus, procédures et contrôles de sécurité dans un domaine donné. Une politique répond à la question : « quelles mesures doivent être prises ? ». Les politiques doivent être hiérarchisées. Par exemple, une politique d'identification et d'authentification pour les accès aux systèmes informatiques sera subordonnée à une politique générale de gestion des accès. Une politique de GSI globale énonçant les principes de sécurité fondamentaux qui s'appliquent à toutes les politiques doit également être élaborée.
Politique de GSI	Politique qui formalise les intentions de l'administration fiscale en ce qui concerne son approche de la sécurité de l'information. Elle doit définir le champ d'application du SGSI et les objectifs généraux en matière de gestion de la sécurité de l'information auxquels chacune des autres politiques doit se conformer.
Pratiques ou contrôles	Mesures spécifiques utilisées pour gérer le risque lié à la sécurité de l'information (c'est-à-dire atténuer ou éliminer un risque). Par contrôles, on entend notamment les processus et procédures, mais également les programmes, les outils, les techniques, les technologies et les dispositifs informatiques. S'agissant de contrer un risque identifié, les contrôles sont parfois appelés mesures de protection ou contre-mesures.
Procédure	Ensemble documenté d'étapes et d'activités visant à mettre en œuvre des politiques de sécurité. Une procédure répond à la question : « comment appliquer les mesures requises et qui doit s'en charger ? ». Le terme « procédure » est souvent associé au terme « processus » (dans l'expression « processus et procédures »), car une procédure est généralement une représentation plus détaillée de chaque étape d'un processus. Bien souvent, il peut exister plus d'une procédure pour chaque étape d'un processus. Par exemple, un processus peut concerner le dépôt d'une déclaration fiscale, mais comme ce dépôt peut s'effectuer par différentes méthodes, chaque méthode peut être régie par une procédure particulière.
Processus	Séquence reproductible d'actions dont les résultats sont mesurables. Le processus est un concept essentiel pour la GSI. L'amélioration des processus et de la sécurité exige de pouvoir mesurer les résultats et d'agir en conséquence. Les processus peuvent aller de processus administratifs en matière fiscale, tels que le dépôt et l'examen des déclarations de revenu, à la mise à jour de logiciels informatiques. Toute action qui n'est pas couverte par un processus défini constitue par définition un risque pour la sécurité, puisqu'il n'y a aucune garantie de reproductibilité, ni aucune mesure ou amélioration des résultats.
Risque posé à la sécurité de l'information	Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un préjudice à l'organisation.
Sécurité de l'information	Protection de la confidentialité, de l'intégrité et de la disponibilité des informations.
Système de GSI	Système de gestion de la sécurité de l'information qui regroupe un ensemble de politiques, procédures et contrôles de sécurité propres à un domaine déployés pour mettre en œuvre le cadre de GSI. La responsabilité du SGSI incombe ultimement à l'encadrement supérieur de l'administration fiscale.
Vulnérabilité	Faille dans la conception d'un actif ou liée à sa nature, ou faiblesse résultant d'une mauvaise gestion d'un actif.

La SE 3.2.1.1 repose le cycle de vie des informations. Elle vise essentiellement à garantir que les données détenues par les administrations fiscales, y compris les renseignements échangés, sont protégées tout au long de leur cycle de vie, et ce au moyen des divers processus et systèmes de traitement, de stockage et d'utilisation des données par lesquels elles passent depuis le moment où elles entrent en possession d'une administration fiscale jusqu'à leur destruction (voir figure 3).

L'approche du cycle de vie des informations est également abordée dans la SE 3.2.5, qui porte sur les contrôles requis pour protéger les différents types d'informations traitées par l'administration fiscale. Toutefois, aux fins des évaluations de confidentialité, la SE 3.2.1.1 vise uniquement la catégorie des renseignements échangés, lesquels doivent faire l'objet de contrôles de confidentialité spécifiques imposés par les accords internationaux d'échange de renseignements.

FIGURE 3. **Cycle de vie des renseignements échangés**

Une administration fiscale doit mettre en place des contrôles de sécurité spécifiques pour chaque étape du cycle de vie des informations, en analysant correctement, dans ses différents domaines, les systèmes informatiques, les départements, les installations et le personnel pouvant intervenir dans ce cycle.

Le choix des contrôles de sécurité à déployer dépend fortement des modalités d'échange de renseignements adopté par l'administration fiscale et des risques associés à ces échanges de renseignements qu'elle a identifiés. Cette boîte à outils décrit certains contrôles, mais les administrations fiscales doivent adapter leur mise en œuvre à leur situation et à leurs particularités propres. Il est recommandé de documenter ces contrôles afin qu'ils soient appliqués de manière cohérente.

Les contrôles liés au cycle de vie des informations couvrent ce qui suit :

- les conventions de dénomination et les classifications de confidentialité utilisées pour identifier clairement, d'une part, les renseignements qui sont échangés, non seulement au titre de la norme d'EAR, mais aussi sur demande et spontanément, et, d'autre part, d'autres types d'informations échangées, telles que les déclarations pays par pays et les décisions fiscales échangées en vertu des standards relatifs à la transparence du projet BEPS;
- les modalités de stockage, c'est-à-dire les emplacements où les informations sont conservées, la manière dont elles le sont et les mesures de sécurité qui leur sont appliquées ;
- les processus garantissant l'utilisation des informations à des fins autorisées uniquement et empêchant leur consultation si elle n'est pas autorisée ;
- les mécanismes de journalisation, de consignation et de tenue de registres appropriés concernant les accès aux données ;
- les mécanismes utilisés pour l'archivage des informations et leur destruction dès lors qu'elles ne sont plus nécessaires ou au terme du délai de conservation prescrit (le cas échéant).

Le tableau 4 présente un exemple simplifié d'application de contrôles tout au long du cycle de vie des informations échangées au titre des normes d'EAR et d'échange de renseignement sur demande.

L'approche par défaut du Forum mondial en matière d'évaluation de la confidentialité est que les administrations fiscales appliquent aux informations échangées les contrôles de sécurité qu'elles utilisent pour leurs opérations en générale, en appliquant, le cas échéant, des contrôles supplémentaires renforcés aux informations échangées.

Dans le cas des pays en développement, cependant, il se peut que la mise en place d'un SGSI couvrant l'ensemble des opérations d'une administration fiscale soit en cours, et que le projet s'avère à fois long et coûteux. Ainsi, les administrations fiscales moins avancées sur le plan des technologies de l'information ou de la sécurité de l'information risquent de ne pas pouvoir s'appuyer sur l'amélioration des contrôles au niveau de toutes leurs opérations pour participer dans les meilleurs délais aux initiatives d'EAR conformément à leurs engagements internationaux et leurs accords d'échange de renseignement.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Tableau 4. **Exemple de contrôles généraux liés au cycle de vie des renseignements échangés**

Étape du cycle de vie	Renseignements échangés automatiquement (EAR)	Renseignements échangés sur demande
Gestion et journalisation des accès	Des contrôles sont mis en place et appliqués pour que seuls les utilisateurs autorisés aient accès aux données. Tous les accès à la base de données contenant les renseignements échangés automatiquement sont consignés dans des journaux et des registres.	Des contrôles sont mis en place et appliqués pour que seuls les utilisateurs autorisés aient accès aux données. Tous les accès à la base de données / armoire / salle d'archives contenant les renseignements échangés sur demande sont consignés dans des journaux et des registres.
Archivage et destruction des informations	Ces données sont détruites de façon sécurisée dès lors qu'elles ne sont plus nécessaires. Celles qui ne sont plus nécessaires avant l'expiration de leur délai de conservation restent archivées de manière sécurisée jusqu'à ce que ce délai expire et qu'elles puissent être détruites.	Ces données sont détruites de façon sécurisée dès lors qu'elles ne sont plus nécessaires. Celles qui ne sont plus nécessaires avant que leur délai de conservation n'ait pris fin restent archivées de manière sécurisée jusqu'à ce que ce délai expire et qu'elles puissent être détruites.
Classification et étiquetage	Ces données sont classifiées comme étant confidentielles et étiquetées en tant que telles.	Ces données sont classifiées comme étant confidentielles et étiquetées en tant que telles.
Traitement et utilisation	Ces données sont utilisées uniquement pour l'administration en matière fiscale et conformément aux accords d'échange de renseignements.	Ces données sont utilisées uniquement pour l'administration en matière fiscale et conformément aux accords d'échange de renseignements.
Modalités de stockage	Ces données sont conservées séparément des bases de données contenant d'autres informations.	Ces données, lorsqu'elles sont au format numérique, sont conservées séparément des bases de données contenant d'autres informations. Lorsqu'il s'agit de documents papier, ils sont conservés dans des armoires verrouillées ou dans des salles de dossiers accessibles au personnel autorisé uniquement.

Les administrations fiscales des pays en développement peuvent par conséquent envisager de s'attacher en priorité à instaurer de solides contrôles liés au cycle de vie pour les renseignements échangés, dans le contexte de l'élaboration d'un cadre de GSI centré sur un « périmètre sécurisé » au sein duquel seront exécutées les opérations liées à l'échange de renseignements, telles que la mise en correspondance des données, l'analyse des risques, la sélection des dossiers et le contrôle fiscal (voir encadré 5).

Le Forum mondial peut, sur demande, offrir aux juridictions des orientations détaillées sur la mise en œuvre de l'approche fondée sur le périmètre sécurisé.

Sous-exigence 3.2.1.2. Politique en matière de GSI, leadership, engagement, et cadre organisationnel

La SE 3.2.1.2 prévoit que les administrations fiscales doivent gérer la sécurité de l'information au moyen d'une politique de GSI écrite qui fait partie intégrante d'un cadre de GSI global définissant clairement les rôles et les responsabilités en matière de sécurité. Cette politique relève de la responsabilité de l'encadrement supérieur et doit être tenue à jour.

Cette SE met en évidence l'importance fondamentale d'un leadership stratégique pour assurer l'efficacité du SGSI. À cet égard, l'engagement de l'encadrement supérieur de l'administration fiscale en matière de sécurité de l'information et son appui sans équivoque à l'affectation de ressources et de fonds à la planification et à la mise en œuvre du SGSI sont essentiels.

Si l'encadrement supérieur fait de la sécurité de l'information une priorité et démontre sa détermination à garantir la réalisation des objectifs du SGSI, le personnel de l'administration fiscale, à tous les échelons, suivra cette direction.

En revanche, s'il laisse entendre que l'on peut sacrifier les objectifs de sécurité, alors la sécurité sera compromise. Bien que l'élaboration d'une approche pour le SGSI constitue un effort collectif orchestré et dirigé par des spécialistes des affaires fiscales, il est important que l'encadrement supérieur en définisse les orientations générales.

Le leadership et l'engagement en matière de GSI dans les administrations fiscales reposent sur ces éléments essentiels :

- Objectifs de GSI
- Politique de GSI
- Définition des rôles, des responsabilités et des autorités relatifs au SGSI

Encadré 5. Périmètre sécurisé pour les renseignements échangés

Qu'est-ce qu'un périmètre sécurisé ?

Il s'agit d'un environnement physique et/ou virtuel hautement sécurisé (et donc adéquatement protégé conformément aux normes applicables) mis en place au sein d'une administration fiscale, et qui permet aux juridictions de recevoir, de conserver en lieu sûr et de traiter les renseignements échangés automatiquement, spontanément ou sur demande, tandis que se poursuivent les efforts à plus long terme pour mettre en œuvre les normes internationales de GSI à l'échelle de toute l'administration fiscale. C'est également une approche tactique qui réduit les coûts et le délai de mise en œuvre par rapport au déploiement des contrôles de sécurité nécessaires pour couvrir l'ensemble des opérations.

Un périmètre sécurisé suppose que l'administration fiscale gère et exerce le contrôle sur le cycle de vie des renseignements échangés, en maintenant un degré élevé de séparation entre ceux-ci et les autres processus, technologies, personnels et ensembles de données déjà utilisés pour les opérations fiscales au niveau national. Il requiert généralement la présence d'une unité organisationnelle sécurisée au sein de l'administration, où des contrôles de sécurité plus rigoureux peuvent être mis en place pour répondre aux exigences strictes des accords d'échange de renseignements, des partenaires en matière d'échange de renseignements et des normes du Forum mondial (il peut s'agir, par exemple, d'un bureau dans un immeuble du siège central ou d'un bâtiment distinct).

En pratique, cela signifie que l'administration fiscale ne va traiter et utiliser les données reçues des partenaires en matière d'échange de renseignements qu'au sein du périmètre sécurisé. Des ressources technologiques, physiques et humaines doivent être affectées au traitement des renseignements échangés au sein de ce périmètre, ainsi qu'au croisement des données, à l'évaluation des risques de non-conformité, aux revues, aux contrôles fiscaux ou aux autres activités liées à la conformité réalisées à l'intérieur du périmètre.

Comment mettre en place un périmètre sécurisé ?

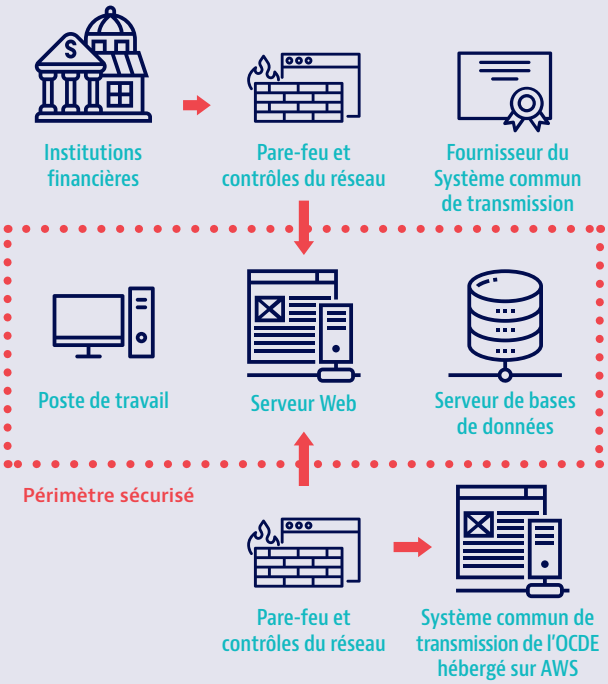
Pour mettre en place un périmètre sécurisé, une administration fiscale doit d'abord réfléchir soigneusement à la manière d'intégrer au mieux ce périmètre dans ses structures opérationnelles. Ainsi, si une unité interne chargée de la gestion des opérations particulièrement sensibles (par exemple, un service qui gère les grandes fortunes ou un bâtiment situé dans la capitale) est déjà dotée d'une sécurité plus robuste, il est envisageable de lui confier les fonctions de traitement et d'utilisation des renseignements échangés.

Une autre solution consiste à analyser comment marier le traitement des renseignements échangés aux actuelles opérations de l'administration. Par exemple, si une même unité gère les gros contribuables et les grosses fortunes, étant donné que, le plus souvent, les informations reçues des partenaires en matière d'échange de renseignements concernent ces catégories de contribuables, il serait sans doute logique d'intégrer le périmètre sécurisé dans cette unité.

Les principales étapes de la mise en place d'un périmètre sécurisé sont généralement les suivantes :

- l'installation d'un ou de plusieurs ordinateurs qui seront spécifiquement réservés aux informations reçues dans le cadre de l'échange de renseignements ;
- le déploiement de mesures de contrôle spécifiques pour sécuriser et contrôler l'accès physique aux locaux, tels que des tourniquets avec passage d'une carte, un système de vidéosurveillance de la zone, l'accès limité à une seule personne à la fois ou encore des alarmes ;
- la formation et la sensibilisation appropriées du personnel, par exemple des fonctionnaires chargés de la discipline fiscale, qui travailleront dans le périmètre sécurisé en utilisant les renseignements échangés ;
- l'établissement d'une structure de gouvernance globale de la GSI, assortie d'une politique et des processus applicables au périmètre sécurisé, que l'encadrement supérieur de l'administration fiscale se chargera de promouvoir ;
- l'acquisition, la production et le déploiement des contrôles informatiques minimaux requis pour le ou les systèmes dédiés au traitement et à l'utilisation des renseignements échangés, à savoir notamment : le document de conception du système et le plan des contrôles, les contrôles au niveau des passerelles, la segmentation des réseaux internes, l'octroi d'accès par liste blanche, la gestion des accès et l'authentification, les restrictions d'accès pour le personnel et les ordinateurs, la tenue de journaux d'audit centralisés, la gestion des changements, le chiffrement des communications, la gestion des risques et l'analyse des vulnérabilités.

Voici un exemple d'architecture réseau de périmètre sécurisé, fourni à titre d'illustration uniquement.



Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Objectifs de GSI

Les administrations fiscales doivent définir des objectifs précis pour le SGSI et les résultats à atteindre. En fonction de leur maturité ou de leur taille, elles peuvent procéder à la planification et la fixation des objectifs à différents niveaux. Les objectifs de GSI peuvent être définis dans le cadre de la planification stratégique de l'administration fiscale, de la stratégie informatique ou, idéalement, d'une stratégie qui vise spécifiquement la sécurité de l'information.

Quelle que soit la manière dont ces objectifs sont établis, des ressources et des fonds doivent être alloué à leur réalisation, et les responsabilités associées à chaque objectif et activité doivent être clairement définies.

Toute administration fiscale devrait avoir pour principaux objectifs de GSI de :

- protéger les informations sensibles qu'elle détient au sujet des contribuables et les autres actifs informationnels concernés conformément aux lois nationales sur la confidentialité et sur la protection des données et aux engagements de confidentialité pris dans le cadre de traités internationaux ;
- atténuer les risques posés à la sécurité des informations par des contrôles et mesures de gestion des accès qui sont en adéquation avec ces risques, tout en permettant aux utilisateurs (c'est-à-dire son personnel) d'accéder aux données dont ils ont besoin pour effectuer leur travail efficacement ;
- établir un système de signalement des incidents liés à la sécurité par son personnel et de favoriser un environnement de travail ouvert et positif dans lequel son personnel reconnaît ses erreurs et œuvre collectivement à l'amélioration continue de la sécurité de l'information (PDCA) ;
- mettre en place des dispositifs de rapport et des outils de mesure et d'examen efficaces (avec des données précises et sécurisées) pour vérifier si les objectifs sont atteints et si leurs contrôles sous-jacents fonctionnent dans la pratique.

Politique de GSI

Pour une administration fiscale, communiquer efficacement les objectifs de GSI à son personnel passe avant tout par une politique de GSI globale.

Les administrations fiscales disposent généralement de diverses politiques spécifiques, chacune portant sur un domaine précis, dont la gestion des ressources humaines, l'accès physique aux locaux, l'accès logique aux systèmes informatiques, l'utilisation des équipements informatiques ou encore la gestion des vulnérabilités. Ces politiques spécifiques sont généralement gérées par des unités opérationnelles différentes, ce qui peut les rendre incohérentes.

Il est donc recommandé d'établir une politique de GSI globale qui exprime les intentions de l'administration fiscale quant à sa démarche en matière de sécurité de l'information. Cette politique doit définir le champ d'application du SGSI et les objectifs généraux de gestion de la sécurité de l'information (comme indiqué au point précédent) auxquels toutes les autres politiques individuelles doivent se conformer.

La politique de GSI doit également formuler l'engagement de l'encadrement supérieur à allouer les

Encadré 6. **Exemple de la structure générale d'une politique de GSI**

Une politique de GSI peut être plus ou moins détaillée, mais sera généralement structurée comme suit :

- Déclaration d'objectif : raison(s) de l'existence de la politique.
- Description du public visé : qui doit lire la politique et à qui elle s'applique. Il peut s'agir de parties tant internes qu'externes ; par exemple, le personnel de l'administration fiscale et les prestataires de services informatiques.
- Approche adoptée concernant les objectifs et principes de GSI ; par exemple, la protection de la confidentialité et de l'intégrité des informations tout en garantissant leur disponibilité pour que le personnel puisse remplir ses fonctions.
- Vue d'ensemble des principaux domaines et principes de sécurité, avec des références générales à des politiques spécifiques. Bien que la politique de GSI définisse le cadre général de la sécurité de l'information, elle doit au moins aborder l'approche adoptée dans les domaines suivants :
  - Sécurité informatique
  - Sécurité physique
  - Sécurité des ressources humaines
  - Gestion de la continuité des activités.
- Principaux rôles et responsabilités, et mécanismes de signalement, de remontée et de mesure.
- Revues et autorité responsable : qui est chargé d'approuver et de revoir la politique, et à quelle fréquence.

ressources nécessaires à la poursuite de ses objectifs de sécurité. L'encadré 6 présente un exemple de la structure générale d'une politique de GSI.

L'encadrement supérieur de l'administration fiscale doivent veiller à ce que le personnel (y compris les sous-traitants) soit informé de la politique de GSI et de son contenu ; un programme complet de communication et de formation est donc recommandé. La formation et la sensibilisation à la sécurité sont examinées plus en détail dans la SE 3.2.2, qui traite des contrôles applicables aux ressources humaines.

Principales fonctions et responsabilités en matière de GSI

La direction des administrations fiscales doit, par le biais de la politique de GSI et en respectant son champ d'application, attribuer des responsabilités de gestion de la sécurité de l'information clairement définies à l'ensemble de son personnel, et au moins aux personnes ou groupes suivants :

- Principal responsable de la sécurité de l'information
- Cadres supérieurs dans les domaines couverts par la politique de GSI
- Chef du service informatique
- Personnel du service informatique
- Équipe d'audit interne

C'est généralement le responsable de la sécurité des systèmes d'information (RSSI) qui est aux commandes de la sécurité de l'information, mais cette fonction peut être assurée par un autre poste, selon la structure organisationnelle et la culture de l'administration fiscale.

Il est généralement conseillé que le RSSI rende compte directement à la direction de l'administration fiscale et qu'il ne fasse pas partie du service informatique. En effet, le RSSI doit être responsable des contrôles et politiques liés à un certain nombre de domaines de sécurité, couvrant des processus qui ne relèvent pas uniquement des technologies de l'information (sécurité physique, ressources humaines, audit interne, etc.). L'encadré 7 présente un aperçu des qualités attendues d'un RSSI et des fonctions qu'il est censé exercer.

Il est recommandé de distinguer clairement les fonctions et responsabilités respectives du personnel informatique et du personnel chargé de la sécurité de l'information. Les voies que ces équipes utiliseront pour communiquer entre elles doivent également être définies avec précision et mises en place. Le personnel informatique doit se concentrer en priorité sur la mise en œuvre et le fonctionnement efficaces des systèmes informatiques, et sur l'intégration des aspects liés à la sécurité dans leur développement, tel que défini dans les politiques. Les administrations fiscales doivent clairement documenter dans un organigramme les lignes et rapports hiérarchiques entre le personnel informatique et le personnel chargé de la sécurité de l'information.

Encadré 7. **Qualités et fonctions du RSSI**

Quelles compétences et quelle expérience doit-il posséder ?

Le RSSI doit disposer à la fois de compétences techniques et organisationnelles, avoir une très bonne connaissance de la sécurité de l'information et posséder une expérience dans un certain nombre de domaines de la sécurité. Il doit être à l'aise pour discuter de questions techniques et maîtriser les exigences professionnelles, réglementaires et légales en matière de sécurité.

Les aptitudes spécifiques attendues d'un RSSI varieront en fonction de l'ampleur des opérations de l'administration fiscale, mais le plus important est qu'il soit convaincu de l'importance d'une sécurité bien conçue et adaptée, et qu'il communique cette vision au reste du personnel.

Dans les petites administrations fiscales, un RSSI peut être un membre du personnel doté de solides compétences en sécurité et en informatique. Dans les plus grandes, des équipes composées de plusieurs spécialistes couvrant chaque domaine des opérations peuvent être nécessaires, auquel cas le RSSI devra probablement posséder un éventail de compétences qui, bien souvent, fait défaut en interne.

Où le RSSI doit-il se trouver dans la structure organisationnelle ? Comment sa fonction doit-elle être supervisée ?

En tant que responsable principal de la sécurité, le RSSI doit être en contact direct avec la direction de l'administration fiscale. Ses fonctions peuvent être décrites dans un mandat ou une description de poste qui est approuvée par la direction de l'administration fiscale et qui précise, entre autres, les principaux objectifs à réaliser en matière de sécurité et le type de comptes rendus qu'il devra fournir ainsi que leur fréquence.

En fonction de la taille de l'administration fiscale, le RSSI peut avoir à ses côtés une équipe qui l'aide à exercer les responsabilités et les activités prévues dans ses attributions.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Sous-exigence 3.2.1.3. SGSI

La SE 3.2.1.3 prévoit que les administrations fiscales doivent traiter la question de la sécurité de l'information en prenant les dispositions opérationnelles appropriées et en l'intégrant à la gestion des processus organisationnels concernés. En substance, il requiert la mise en place d'un SGSI qui soit intégré aux opérations de l'administration.

Comme indiqué au tableau 3, le cadre de GSI désigne les structures organisationnelles et les principes généraux de sécurité de l'information visant à guider les administrations fiscales dans la réalisation des objectifs de GSI, tandis que le SGSI comprend les politiques, procédures et contrôles spécifiques d'un domaine donné qui sont nécessaires pour mettre en œuvre ce cadre.

La taille de l'administration fiscale, la complexité de ses opérations et la maturité de ses systèmes informatiques sont autant d'éléments qui influencent le niveau de détail du SGSI (voir figure 4).

FIGURE 4. **Composantes du cadre de GSI et du SGSI**

Les composantes du SGSI doivent être mises au point d'après les évaluations des risques effectuées par l'administration fiscale. La gestion des risques est abordée en détail dans la SE 3.2.1.4.

Un SGSI peut être formalisé dans un document général (tel qu'un manuel) qui regroupe les différents ensembles de politiques, procédures et contrôles afférents à un domaine de sécurité particulier. Les administrations fiscales peuvent envisager de donner la structure suivante au document relatif à leur SGSI :

- Introduction
- Champ d'application du SGSI
- Organigramme, fonctions et responsabilités, et structure hiérarchique entre les parties prenantes
- Politique de GSI
- Principaux processus de GSI
- Approche de la gestion des risques et risques identifiés

Encadré 8. **Exemple d'une politique pour un domaine de sécurité donné dans le contexte d'un cadre de GSI et d'un SGSI**

Cadre de GSI. Objectif : protéger les informations sensibles concernant les contribuables et les autres actifs informationnels concernés.

SGSI et politique de GSI. Stratégie de protection des renseignements échangés automatiquement détenus par l'administration fiscale, conformément à l'évaluation des risques effectuée sur cet actif informationnel. Tout accès aux systèmes et bases de données contenant les renseignements échangés automatiquement est strictement contrôlé par l'utilisation de mots de passe complexes.

Mise en œuvre d'une politique en matière de mots de passe, en tant que contrôle de sécurité. Dans l'Active Directory, la stratégie de groupe du système qui stocke les renseignements échangés automatiquement est paramétrée comme suit : Les mots de passe doivent comporter au moins 15 caractères et être modifiés tous les 180 jours. Un utilisateur ne peut pas réutiliser ses dix derniers mots de passe et il lui est interdit de communiquer ses mots de passe à quiconque, sous quelque forme que ce soit. Le personnel reçoit des instructions sur l'utilisation des mots de passe.

Mise en œuvre d'une politique en matière de mots de passe, en tant que procédure. Le RSSI est tenu de veiller à ce que la politique en matière de mots de passe soit appliquée et respectée à l'échelle des systèmes et bases de données contenant les renseignements échangés automatiquement. Il doit être consulté lors de la mise en place des systèmes pour garantir que cette politique est correctement appliquée. Il doit également, en coordination avec les spécialistes en informatique (généralement les administrateurs système), s'assurer que la politique est mise en œuvre et fonctionne efficacement. Dans le cas contraire, des mesures correctives doivent être prises (par exemple, par l'amélioration des orientations fournies au personnel). Le RSSI doit également effectuer régulièrement des contrôles ponctuels, afin de vérifier que le personnel comprend la politique et l'applique correctement. Enfin, il doit collaborer activement avec le personnel chargé des opérations de sécurité pour déterminer si les contrôles opérationnels tels que la journalisation, la surveillance et la gestion des incidents permettent d'identifier les problèmes de mise en œuvre de cette politique.

- Diverses politiques pour traiter les risques identifiés dans un domaine de sécurité particulier (qui font référence à des procédures ou contrôles spécifiques). Parmi les divers domaines généraux auxquels s'étend la sécurité de l'information, les administrations fiscales devraient intégrer les suivants dans leur SGSI aux fins des évaluations de confidentialité :
  - Ressources humaines (RH) (SE 3.2.2) ;
  - gestion des accès (SE 3.2.3) ;
  - sécurité informatique (SE 3.2.4) ;
  - protection des informations (SE 3.2.5) ;
  - gestion des opérations (SE 3.2.6).
- Approche en matière de contrôle des politiques documentées du SGSI
- Approche en matière de l'audit interne du SGSI
- Périodicité du réexamen du SGSI

L'encadré 8 présente un exemple simplifié de ce que pourrait être la structure d'une politique liée à un domaine de sécurité spécifique dans le contexte d'un cadre de GSI et d'un SGSI.

Sous-exigence 3.2.1.4. Gestion des risques posés à la sécurité des informations

Comme les administrations fiscales disposent généralement de ressources humaines et financières limitées, il leur est recommandé, afin que ces ressources soient allouées efficacement, de concevoir un SGSI fondé sur une évaluation des risques de sécurité auxquels elles sont exposées.

La SE 3.2.1.4 prévoit par conséquent que les administrations fiscales gèrent systématiquement leurs risques spécifiques en matière de sécurité de l'information, en tenant compte des menaces, des vulnérabilités et des impacts.

En vertu des normes internationales relatives à la gestion des risques, telles qu'ISO 31000 et ISO 27005[12], un risque en sécurité de l'information peut être défini comme étant « la possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise donc à l'organisation ».

12. www.iso.org/fr/iso-31000-risk-management.html et www.iso.org/fr/standard/75281.html

Les administrations fiscales sont censées disposer d'un processus de gestion des risques solide et complet, assorti d'une méthodologie qui doit décrire les étapes de ce processus, les responsabilités propres à chacune de ces étapes et les critères utilisés pour l'évaluation des risques.

Elles peuvent utiliser une méthodologie de gestion des risques spécifique uniquement pour le SGSI, ou lui appliquer une méthodologie adoptée pour d'autres domaines de leurs opérations. Dans le second cas de figure, il est important d'adapter les critères de cette autre méthodologie à la sécurité de l'information.

En général, la méthodologie de gestion des risques s'appliquant à la sécurité de l'information comprend les étapes décrites dans le tableau 5. Toutefois, ces détails ne sont donnés qu'à titre de référence et les administrations fiscales sont encouragées à opter pour les méthodologies les plus adaptées à leurs spécificités.

La gestion des risques est un processus continu, et les risques doivent être réexaminés et évalués à intervalles réguliers. Ainsi, il est important de surveiller périodiquement l'efficacité des mesures d'atténuation des risques. Face à un scénario de risque, les administrations fiscales doivent lancer la procédure de gestion des incidents, décrite en détail dans la SE 3.2.6.6.

Il est essentiel que les membres du personnel soient conscients des principaux risques pesant sur la sécurité des informations, et que ce thème soit abordé dans les programmes de sensibilisation ou les activités de formation menés par l'administration fiscale.

Les administrations fiscales peuvent documenter les résultats de l'évaluation des risques dans un registre des risques ou tout autre outil qu'elles utilisent pour les aider dans ces évaluations. Le tableau 6 présente, à titre d'exemple, un registre des risques comportant des références pour les groupes d'actifs « Ressources humaines » et « Actifs informationnels » et fondé sur la méthodologie décrite au tableau 5.

Ce registre est fourni pour illustration uniquement. Les administrations fiscales peuvent envisager d'utiliser des registres de risques distincts pour les différents groupes d'actifs, pour les domaines informatiques et non informatiques, ou recourir à un registre centralisé. Elles sont encouragées à adopter l'approche la mieux adaptée à leurs spécificités.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Tableau 5. **Exemple de méthodologie de gestion des risques basée sur les lignes directrices de la suite ISO 27000**

Étape	Description	Résultat
1. Identification des actifs	Dresser un inventaire des principaux actifs de l'organisation, en identifiant le propriétaire de chaque actif. Le propriétaire d'un actif est la personne responsable de la gestion et de l'utilisation de cet actif. Les actifs peuvent varier en fonction de la portée de l'évaluation. Par exemple, pour une évaluation globale des risques dans le cadre de EAR, il est probable que seuls les processus et systèmes opérationnels liés à cet échange soient identifiés comme des actifs. Dans le cas où l'évaluation porterait uniquement sur les systèmes informatiques, leurs composants spécifiques (matériels et logiciels) seraient identifiés comme des actifs.	**Exemples de catégories d'actifs :** • Processus organisationnels • Ressources humaines • Actifs informationnels • Image et réputation • Actifs logiciels • Actifs matériels • Autres actifs physiques • Services externalisés • Services de soutien internes
2. Valorisation des actifs	Effectuer une valorisation des actifs en termes d'importance pour l'administration fiscale et de réalisation de ses objectifs en matière de sécurité de l'information.	**Valeurs possibles d'un actif :** **1.** Très peu d'importance **2.** Peu d'importance **3.** Importance moyenne **4.** Grande importance **5.** Très grande d'importance
3. Identification des scénarios de risque	Cette étape peut être répartie comme suit : • Identification des vulnérabilités des actifs ou des menaces qui pèsent sur ceux-ci, ou des scénarios de risque. • Évaluation de la probabilité que le scénario de risque se réalise.	**Probabilité qu'un scénario de risque se produise :** **1.** Rare **2.** Très faible **3.** Modérée **4.** Élevée **5.** Très élevée
4. Évaluation de l'impact	Évaluer l'impact qu'aurait la réalisation du scénario de risque sur la confidentialité, l'intégrité et la disponibilité des informations et/ou sur les objectifs de sécurité.	**Valeurs d'impact proposées :** **0.** Aucun impact **1.** Faible impact **2.** Impact moyen **3.** Fort impact
5. Appréciation du risque	Réaliser une appréciation du risque. On peut utiliser une formule simple qui prend en considération la valeur de l'actif, la probabilité que le scénario de risque se produise et la valeur de l'impact.	**Formule pour l'appréciation du risque :** Valeur de l'actif * probabilité de réalisation du scénario de risque * valeur de l'impact
6. Définition du niveau de risque acceptable	Définir le niveau de risque jugé acceptable, en fonction de la valeur (importance) des actifs, des réglementations de la juridiction ou des obligations découlant des traités conclus. Un risque acceptable peut être défini comme étant un risque pour lequel la direction de l'administration fiscale est prête à accepter les conséquences de sa survenance. Habituellement, la mise en œuvre des mesures nécessaires pour atténuer de tels risques coûte plus qu'elle n'apporte. Cependant, même un risque défini comme étant « acceptable » doit toujours faire l'objet d'une surveillance, car il peut évoluer et s'intensifier. En cas de changement des exigences opérationnelles ou de la disponibilité des ressources, il est possible de revoir les décisions concernant les risques acceptables.	Ces décisions doivent être documentées et réexaminées à intervalles réguliers.
7. Traitement des risques	Identifier les contrôles appropriés pour le traitement des risques.	**Options de traitement d'un risque :** • Acceptation du risque : aucune mesure spécifique n'est prise ; par exemple, aucun chiffrement n'est appliqué à certaines données lorsqu'elles sont « au repos » (inactives). Le risque fait malgré tout l'objet d'une surveillance. • Atténuation du risque : application de mesures visant à réduire la probabilité que le risque se produise ; par exemple, utilisation de pare-feu et d'un chiffrement pour protéger une base de données. • Évitement du risque : le service ou l'application concernés seront complètement désactivés, de façon à ce que la probabilité de survenance du risque soit nulle ; par exemple, le système ne sera pas connecté à Internet pour prévenir les attaques de pirates. • Transfert du risque : le risque identifié sera géré par une autre entité (cyber-assurance pour faire face aux atteintes à la sécurité des données). Cette option est recommandée uniquement pour réduire les conséquences financières d'un risque et ne doit être utilisée que dans des circonstances très limitées.
8. Surveillance et réévaluation des risques	En se fondant sur le suivi régulier de la mise en œuvre des contrôles de sécurité, l'audit interne et d'autres processus d'examen, actualiser le processus de gestion des risques et ses résultats.	Il recommandé de revoir le processus tous les ans ou à chaque changement majeur de l'environnement.

Tableau 6. **Exemple de structure de registre des risques**

Groupe d'actifs	Actif	Valeur de l'actif (1-5)	Menace	Vulnérabilité	Probabilité de survenance du risque (1-5)	Valeur d'impact (0-3)	Appréciation du risque (valeur de l'actif * probabilité de survenance * impact)	Contrôles sélectionnés si le traitement du risque est nécessaire
Ressources humaines	Direction de l'administration fiscale	4	Indisponibilité de la direction pour la prise de décisions essentielles	Changement constant des responsabilités	4	3	48	Atténuation : délégation de pouvoir
	Personnel de premier plan du service informatique	5	Indisponibilité de l'administrateur système pour l'application des correctifs d'urgence	Un seul administrateur système dans le service informatique	3	3	45	Atténuation : constitution d'une équipe composée de trois administrateurs système
Actifs informationnels	Données sur les contribuables nationaux et renseignements échangés automatiquement (au format numérique)	5	Atteinte à la sécurité des données et divulgation d'informations confidentielles	Vulnérabilités des systèmes	3	5	75	Atténuation : tests d'intrusion, chiffrement des données en transit, contrôles de pare-feu, sauvegarde des données, journalisation et consignation dans un registre de tous les accès à la base de données, accès accordés selon le principe du « besoin d'en connaître »
	Renseignements échangés détenus, au format papier	5	Accès à la salle des dossiers par une personne non autorisée, qui divulgue des informations confidentielles	Salle des dossiers insuffisamment sécurisée	3	5	75	Atténuation : mise en place d'un code d'accès à la salle des dossiers pour que seul le personnel autorisé puisse y entrer ; journalisation et consignation dans un registre de tous les accès à cette salle

Sous-exigence 3.2.1.5. Gestion de la continuité des activités

La SE 3.2.1.5 prévoit que les administrations fiscales doivent mettre en place des mécanismes appropriés pour gérer et assurer la continuité de leurs activités. On entend par là la manière dont elles s'assurent de pouvoir poursuivre l'exécution de leurs principales opérations, y compris le recouvrement de l'impôt et l'EAR, dans le cas où un événement perturberait leur fonctionnement normal. Pareil événement peut être une catastrophe naturelle, une pandémie, une attaque par un logiciel de demande de rançon ou un incident technique qui paralyse les systèmes informatiques.

La continuité de l'activité et la planification associée (plan de continuité de l'activité, ou PCA) sont étroitement liées au processus de gestion des risques. Comme le montre la figure 5, la continuité de l'activité est un processus de gestion qui comprend l'identification des scénarios de risque, l'évaluation de leur impact, l'établissement d'un PCA pour assurer la continuité des opérations si un tel scénario devait se produire, la mise à l'épreuve et le réexamen du PCA, ainsi que la formation du personnel au PCA. Les étapes courantes de ce processus sont présentées ci-dessous.

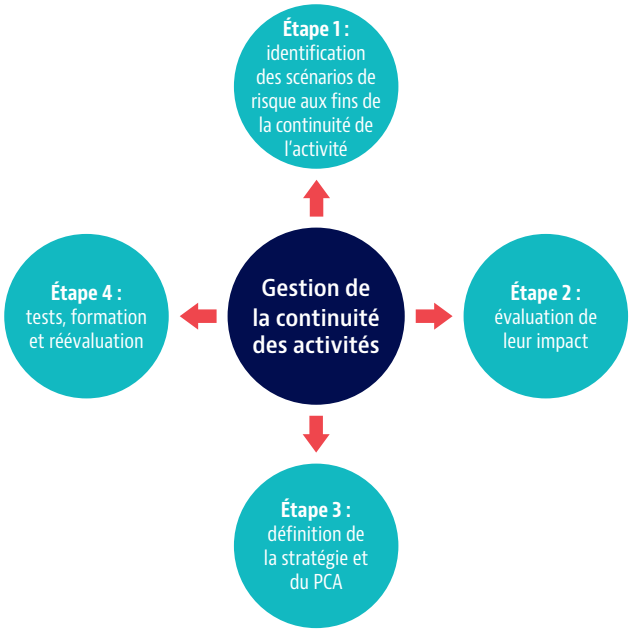
Étape 1 : identification des scénarios de risque aux fins de la continuité de l'activité

Les cadres supérieurs et les principaux représentants des domaines concernés (service informatique, département chargé de la sécurité physique, service des ressources humaines, etc.) identifient ensemble les scénarios de risque probables et susceptibles de perturber le fonctionnement normal de l'administration fiscale. Il peut s'agir d'une catastrophe naturelle, d'une pandémie ou d'un incident technique majeur pouvant entraîner plusieurs des problèmes suivants :

- l'indisponibilité du personnel ;

- l'indisponibilité des installations ou du matériels ;
- l'indisponibilité des systèmes d'information ou de communication.

FIGURE 5. **Processus de gestion de la continuité de l'activité**



Étape 2 : évaluation de l'impact des scénarios de risque sur les activités

Les administrations fiscales doivent évaluer et documenter l'impact potentiel de chaque scénario de risque sur la continuité de leurs activités, par exemple sur l'EAR ou sur le recouvrement de l'impôt. Cet impact peut être exprimé en termes qualitatifs (incapacité de l'administration fiscale à échanger les renseignements en temps voulu, par exemple) ou quantitatifs (le montant des impôts non perçu dans les délais par exemple).

Étape 3 : définition de la stratégie et du PCA

Les administrations fiscales doivent définir une stratégie leur permettant de faire face et de remédier aux effets qu'aurait la concrétisation d'un scénario de risque sur leur activité. Chaque PCA doit décrire trois étapes principales (pour un exemple de sa structure, voir l'encadré 9) :

- Assurer une réponse immédiate, en donnant la priorité à la sécurité du personnel, le cas échéant.
- Permettre la restauration des fonctionnalités essentielles. Le PCA doit à cet égard préciser :
  - les principaux systèmes et la priorité qui leur est donnée lors de la procédure de restauration ;
  - les membres du personnel ou les fournisseurs critiques et leurs coordonnées personnelles (adresses courriel et numéros de téléphone privé) ;
  - les informations, documents papier et/ou sauvegardes ou disques externes critiques qui doivent impérativement être transférés vers un emplacement de secours ;
  - la personne qui prend la décision du retour à la normale.

Encadré 9. **Exemple de structure d'un PCA**

1. Priorités en matière de reprise. Les opérations essentielles, qui sont prioritaires pour la reprise et qui doivent être transférées dans un autre lieu.
2. Stratégie de relocalisation et lieu du transfert. Le site de substitution doit être utilisé en cas de sinistre ou de perturbation empêchant la poursuite de l'activité sur le site habituel de l'administration fiscale. Cette stratégie pourrait inclure des sites de relocalisation à court et à long terme, en fonction de la gravité de la perturbation des activités.
3. Données critiques : sauvegarde des informations numériques et copie des documents papier.
4. Étapes de la reprise :
   a. Survenue du sinistre
   b. Activation du PCA
   c. Relocalisation vers le site de substitution
   d. Reprise, c'est-à-dire activités ou tâches spécifiques destinées au rétablissement des opérations normales et critiques
   e. Retour à la normale
5. Plan de rétablissement des activités : les équipes informatiques et de reprise d'activité gèrent, contrôlent et vérifient périodiquement tous les documents qui sont essentiels à la poursuite des activités et qui seraient affectés par des perturbations des installations ou des catastrophes ; elles sauvegardent et stockent périodiquement les fichiers les plus importants hors site.
6. Équipe de rétablissement des activités, avec les fonctions et responsabilités de ses membres, ainsi que leurs coordonnées.

Encadré 10. **Exemple de PCA d'une administration fiscale**

Le PCA de l'administration fiscale de la juridiction A comprend des mesures détaillées visant à garantir que cette administration est en mesure de se remettre d'une perturbation majeure de ses activités. Il a été élaboré en tenant compte des principaux scénarios de risque, bien qu'il soit suffisamment générique pour pouvoir s'appliquer à la plupart des menaces.

Il recense toutes les parties prenantes qui doivent être impliquées si une situation d'urgence devait perturber les opérations, et leurs coordonnées sont mises à jour immédiatement en cas de changement afin qu'elles puissent être contactées rapidement.

Le PCA répertorie également tous les systèmes informatiques cruciaux et indique dans quel ordre de priorité effectuer leur reprise. Il prévoit que tous doivent être remis en état de marche dans les 24 à 48 heures qui suivent l'incident, et que le délai pour le retour à la normale ne doit pas dépasser une semaine. L'administration fiscale dispose d'un site de substitution vers lequel elle peut transférer ses opérations au besoin.

Le personnel est formé chaque année au PCA, et ce dernier est publié sur l'intranet de l'administration fiscale.

Pour roder son personnel à ce plan, l'administration fiscale procède à des simulations sur ordinateur deux fois par an et à des séances de mise en pratique au moins une fois par an. Les simulations visent à évaluer l'état de préparation et les connaissances du personnel concernant le PCA, à avoir la certitude que chacun connaît le rôle qu'il devra assumer en cas d'urgence et à identifier les éventuelles lacunes du plan. Leurs résultats permettent également d'améliorer le PCA.

- Exécution de la procédure pour le retour à la normale, avec description des étapes correspondantes.

Les PCA doivent être révisés régulièrement pour tenir compte de l'évolution des scénarios de risque, des changements apportés quant au personnel critique et de la mise à jour de leurs coordonnées, des modifications concernant les types d'informations détenues ou les systèmes informatiques, etc.

Étape 4 : tests, formation et réexamen du PCA

Les PCA doivent être soumis à des tests au moins une fois par an, en faisant l'objet de simulations ou de séances de mise en pratique complètes. L'objectif principal d'un test est de vérifier que le personnel connaît la procédure à suivre en cas d'urgence, telle que définie dans le PCA. Les résultats des tests doivent être communiqués et utilisés pour améliorer le PCA.

Il est extrêmement important que le personnel reçoive une formation sur le PCA. Des séances régulières de sensibilisation de tout le personnel concerné doivent être organisées. Un exemple de tests et de formation associés à un PCA est fourni dans l'encadré 10.

La gestion des scénarios d'indisponibilité des systèmes informatiques et de communication relève généralement de la responsabilité du département informatique. Ce point est analysé plus en détail dans la SE 3.2.4.5, qui traite de la continuité des services informatiques sur la base d'accords de niveau de service.

SOUS-EXIGENCE 3.2.2 : CONTRÔLES APPLICABLES AUX RESSOURCES HUMAINES

Ces contrôles désignent les politiques et procédures de nature juridique et administrative mises en place pour gérer les ressources humaines de l'administration fiscale (en général, le personnel et les sous-traitants) en veillant à ce qu'elles respectent et protègent la confidentialité des renseignements fiscaux.

Les membres du personnel ont accès à des informations sensibles sur les affaires des contribuables, ainsi que sur la politique de l'administration fiscale et la conduite de ses activités, par exemple dans le cadre de contrôles fiscaux, de l'analyse des risques et des procédures d'enquête. En outre, ils sont étroitement associés à chaque étape du cycle de vie des renseignements échangés.

Aussi les administrations fiscales devraient-elles mettre en place des contrôles tout au long du cycle de l'emploi, afin d'assurer que leur personnel interne, mais aussi les tiers ou les sous-traitants, respectent le principe de confidentialité. La confiance entre un employeur et son personnel repose sur une première sélection lors du recrutement (souvent suivie d'une période d'essai initiale) et sur des années de relation employeur-employé.

Cette section est scindée en quatre parties : une description succincte du cycle de vie de l'emploi, suivie d'une analyse des activités et processus de chacune des étapes de ce cycle, à savoir le recrutement, la période d'emploi et la cessation de l'emploi.

Elle décrit en détail ces trois étapes du cycle, ainsi que les contrôles spécifiques qui peuvent leur être appliqués. Le tableau 7 présente les définitions des principaux concepts abordés dans la SE 3.2.2.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Tableau 7. **Définitions des principaux concepts**

Concept	Description
Accord de non-divulgation	Entente formelle ou contrat définissant les règles de non-divulgation des informations confidentielles à des tiers.
Formation	Accompagnement du personnel de l'administration fiscale (salariés et sous-traitants) pour qu'il acquière et développe les connaissances, les aptitudes et les compétences de base nécessaires pour intégrer la confidentialité et la sécurité dans les processus fiscaux.
Hameçonnage	(Phishing en anglais) Type d'escroquerie en ligne au cours de laquelle des criminels envoient des courriels frauduleux conçus pour sembler provenir d'une source légitime et tromper le destinataire de façon à lui extorquer des informations confidentielles, telles que des identifiants d'accès aux systèmes.
Ingénierie sociale	Pratique de manipulation qui exploite la nature confiante du personnel dans un but malveillant, afin d'obtenir des informations qui peuvent être utilisées à des fins personnelles. Également appelée "piratage psychologique".
Sensibilisation	Pratique consistant à exposer régulièrement le personnel à des messages les mettant en garde contre les menaces/risques informatiques ou de sécurité, ces messages étant généralement communiqués simultanément à tous les membres du personnel d'un domaine particulier ou de l'ensemble de l'administration fiscale, et même aux tiers externes, etc.

Cycle de vie du personnel

La SE 3.2.2, qui reflète les normes internationales, prescrit que les administrations fiscales doivent mettre en place diverses politiques et procédures (c'est-à-dire les contrôles) au cours des trois étapes du cycle de vie de l'emploi : les contrôles relatifs au recrutement (SE 3.2.2.1 et 3.2.2.2), à la période d'emploi (SE 3.2.2.3 et 3.2.2.4) et à la cessation de l'emploi (SE 3.2.2.5). Les principaux contrôles sont présentés dans la figure 6.

Catégories de personnel d'une administration fiscale

Les contrôles appliqués tout au long du cycle de vie de l'emploi devraient l'être à l'ensemble du personnel (ce qui, au sens large, inclut les agents permanents et temporaires, ainsi que les sous-traitants et les prestataires de services externes). Une administration fiscale n'emploie pas une seule catégorie de personnel, et il n'est pas rare d'y trouver les catégories mentionnées dans le tableau 8 :

Il peut y avoir d'autres catégories à prendre en considération, selon le contexte particulier de la juridiction concernée et de son droit du travail.

Les administrations fiscales doivent tenir compte de leurs différentes catégories de personnel lorsqu'elles évaluent les divers types de processus qui s'appliquent à elles tout au long de leur cycle de vie de l'emploi. Ainsi, elles devraient mettre en place des contrôles appropriés pour les tiers externes engagés pour exercer des fonctions sensibles (comme administrer les systèmes qui hébergent des renseignements échangés) et veiller à ce que tout le personnel qui gère ou traite des informations sensibles sur les contribuables, quelle que soit les modalités de leur contrat, bénéficie d'une formation adaptée à leur rôle.

Les contrôles de sécurité spécifiques directement appliqués aux sous-traitants sont examinés plus en détail dans la SE 3.2.4.4, portant sur la gestion des prestations de services des fournisseurs.

Les contrôles appliqués peuvent également dépendre de

FIGURE 6. **Cycle de vie de l'emploi et contrôles visant à garantir la confidentialité**

Tableau 8. **Catégories de personnel d'une administration fiscale**

Catégorie	Description
Agents	Personnes qui sont généralement embauchées en vertu d'un contrat de travail à durée indéterminée, ou bien d'un contrat à durée déterminée mais renouvelable.
Agents temporaires	Personnes qui sont généralement embauchées en vertu d'un contrat à durée déterminée dans un but précis (pour des services de conseil par exemple).
Fonctionnaires	Personnes nommées à un poste dans l'administration publique, généralement à vie.
Sous-traitants (contractants externes)	Les sous-traitants peuvent être de deux types, en fonction de la relation contractuelle : ● Des prestataires externes engagés pour fournir d'un service spécifique, comme un système logiciel informatique, ou pour nettoyer les locaux. ● Des sous-traitants engagés pour assumer une fonction particulière, telle qu'une mission à court terme, ou pour exercer une fonction pour laquelle il n'existe pas de personnel suffisamment qualifié en interne. Il peut s'agir d'un expert externe mandaté pour dispenser une formation sur site de deux semaines sur l'utilisation d'un système spécialisé.

la manière dont est organisée la fonction des ressources humaines de l'administration fiscale. Les ressources humaines ne sont pas une fonction propre à l'administration fiscale mais plutôt une fonction générique sur laquelle celle-ci s'appuie et qui n'est donc pas toujours gérée en son sein. Ainsi, dans certaines juridictions, un seul département peut assurer la direction des ressources humaines du ministère des Finances ou de l'ensemble du secteur public, ou administrer de manière centralisée certaines catégories de personnel (comme la fonction publique), tandis que la gestion du personnel sans statut de fonctionnaire est confiée à l'administration fiscale.

Quelle que soit la structure organisationnelle en place, les juridictions devraient pouvoir identifier correctement la place de la fonction de gestion des ressources humaines dans leur système global de gouvernement et son lien avec l'administration fiscale. Elle pourra ainsi évaluer les mesures que devraient prendre les différents organismes publics ou services concernés pour veiller à ce que les différentes politiques et procédures prévoient des contrôles adaptés à la sensibilité de la fonction de l'administration fiscale.

Les sections suivantes présentent des orientations concernant les contrôles à appliquer aux trois étapes du cycle de l'emploi.

Sous-exigences 3.2.2.1 et 3.2.2.2. Étape 1 : contrôles lors du recrutement

Cette section concerne les contrôles de sécurité qui s'appliquent lors de la procédure de recrutement. Il s'agit des vérifications effectuées et des dispositions prises pour s'assurer de pouvoir confier le traitement d'informations confidentielles aux personnes susceptibles d'être embauchées. Ces contrôles doivent être conformes aux lois et règlements applicables dans la juridiction (le code des impôts et le code de la fonction publique, par exemple) et en adéquation avec les impératifs propres à l'administration, la classification des informations à consulter et leur degré de sensibilité, ainsi que les risques identifiés.

La SE 3.2.2.1 exige des administrations fiscales qu'elles veillent à ce que les rôles et responsabilités en matière de

FIGURE 7. **Procédure de recrutement**

sécurité du personnel et des sous-traitants soient définis et documentés, et que l'engagement qu'ils supposent soit clairement expliqué. Elles doivent en outre les soumettre à des examens réguliers conformément à la politique de sécurité (et des accords de confidentialité et de non-divulgation devraient également être signés). Ces points sont abordés plus en détail plus loin.

Quant à la SE 3.2.2.2, il prévoit de vérifier pour tous les candidats (agents et sous-traitants) leurs antécédents ainsi que leur aptitude à exercer la fonction concernée, conformément aux bonnes pratiques reconnues et aux risques identifiés. Ces contrôles s'appliquent à la procédure de recrutement, qui peut être segmentée en trois phases, chacune s'accompagnant de son propre ensemble de contrôles de confidentialité (voir figure 7).

Phase 1 : entretien d'embauche

La procédure liée à cet entretien doit souligner auprès des candidats potentiels l'importance que revêtent la confidentialité et la sécurité de l'information. Ainsi, le formulaire de recrutement peut comporter un marquage approprié pour la classification de sécurité et indiquer le niveau de confidentialité que la fonction impliquera. En outre, les candidats présélectionnés pour l'entretien peuvent se voir expliquer leurs obligations de confidentialité ainsi que les conséquences qu'entraînerait le non-respect de celles-ci (sanctions administratives ou pénales) si le poste leur était attribué.

Tableau 9. **Types de vérifications des antécédents effectuées lors de la procédure de recrutement**

Vérification des antécédents	Description
Contrôle de la véracité des informations fournies dans la candidature	Ce contrôle consiste à vérifier l'expérience professionnelle, les diplômes et titres, les formations et compétences techniques, les références et autres renseignements indiqués par le candidat. En soumettant de fausses informations, un candidat manque au principe de probité à respecter pour exercer un emploi dans une administration fiscale. Toutefois, il n'est pas toujours nécessaire de vérifier tous les diplômes, titres, compétences et références présentés. Des contrôles par sondage sur certains critères convenus fondés sur les risques, ou des contrôles complets pour tous les candidats mais dans certains domaines uniquement, peuvent suffire à garantir que les candidatures sont acceptables.
Vérification du casier judiciaire	Parallèlement au contrôle des informations de la candidature, une vérification du casier judiciaire est généralement nécessaire. Dans certaines juridictions, le fait d'avoir un casier judiciaire est considéré comme totalement incompatible avec un emploi dans l'administration fiscale. Les administrations fiscales pour lesquelles la présence d'un casier judiciaire ne constitue pas un barrage au recrutement devraient toutefois envisager d'appliquer certains critères limitatifs, tels que la gravité de l'infraction, le temps écoulé depuis qu'elle a été commise, etc. En outre, elles peuvent prendre des mesures compensatoires en cas d'embauche d'un candidat ayant un casier judiciaire, comme instaurer des périodes d'essai ou d'initiation (avec un critère déclenchant la rupture de contrat) pendant lesquelles la personne serait soumise à une surveillance renforcée. En ce qui concerne les infractions commises au cours de la période d'emploi, les juridictions devraient indiquer clairement aux potentielles recrues que toute poursuite pénale doit être signalée et peut avoir des conséquences (dont le licenciement).
Vérification des antécédents financiers	La divulgation des données financières du candidat à des fins de vérification peut également être demandée, en particulier si celui-ci brigue un poste de haut niveau. Bien que ce contrôle puisse être utile au travail de l'administration fiscale, son application dépendra généralement du contexte particulier de la juridiction (elle est de mise notamment lorsque le sentiment de corruption est élevé). Dans certaines juridictions, cette vérification peut s'inscrire dans le cadre d'une inspection financière plus approfondie effectuée pour les personnes qui cherchent à obtenir l'autorisation de traiter des informations extrêmement sensibles (voir le point « Validation de l'aptitude au poste » ci-dessous).
Validation de l'aptitude au poste	Certaines juridictions disposent de services d'habilitation ou de validation propres à un ministère ou interministériels (souvent intégrés aux services de sécurité nationale), qui effectuent différents types de contrôles d'aptitude visant à appréhender correctement les antécédents et le caractère de la personne concernée. Ces vérifications doivent généralement être réalisées avant d'assigner un poste impliquant l'accès à des informations confidentielles et peuvent varier selon le niveau de classification (informations protégées, secrètes ou ultrasecrètes, par exemple). Il est fréquent que certains agents d'une administration fiscale traitent des données ayant un niveau de classification de confidentialité très élevé, telles que des dossiers financiers et commerciaux de gros contribuables ou de responsables politiques. Ce filtrage à plusieurs niveaux aide les organismes publics et leur personnel à traiter les informations en fonction du degré de sécurité qu'elles requièrent. Ces contrôles d'habilitation peuvent porter sur les éléments suivants : preuve d'identité, condamnations pénales et délits, dépistage de drogue positif, solvabilité, faillite, revenus des cinq dernières années, dépendance aux jeux, etc. Des vérifications plus poussées peuvent également être réalisées, notamment par des entretiens avec la personne, ainsi qu'avec quelques membres de la famille, des amis et des associés.

Phase 2 : vérification des antécédents et validation

Tous les candidats à l'emploi, pour des postes permanents et temporaires, les sous-traitants et autres, doivent faire l'objet de vérifications de leurs antécédents et de leur aptitude à exercer la fonction concernée, ainsi que d'autres modalités de contrôle appropriées. Les vérifications des antécédents peuvent être plus ou moins approfondies et leur rigueur variera généralement selon le type de fonction et les obligations de confidentialité associées (voir tableau 9).

Même si ces contrôles et vérifications sont présentés comme étant applicables avant l'entrée en fonction, il est également important de les renouveler périodiquement, et il se peut que certains doivent être réitérés pendant la période d'emploi dans certaines circonstances. C'est le cas par exemple en cas de changement important dans la fonction exercée par l'agent ou si celui-ci se voit confier un rôle plus stratégique, lui donnant accès à des informations plus sensibles ou d'une classification de confidentialité plus élevée. Les contrôles et vérifications, en particulier s'ils sont supérieurs au niveau de base, devraient normalement être valides pour une durée déterminée, avec un processus de révision du niveau des contrôles et vérifications et une actualisation des habilitations.

Dans le cas des sous-traitants, les administrations fiscales doivent également procéder à des contrôles et vérifications des antécédents. Elles peuvent toutefois décider de confier cette tâche au sous-traitant lui-même, qui s'engage alors à appliquer les contrôles requis par l'administration fiscale à son propre personnel et à s'assurer qu'il respecte les politiques de sécurité de l'administration fiscale. Dans pareil cas, l'administration fiscale doit s'assurer que ce tiers effectue correctement les vérifications des antécédents et respecte les clauses du contrat qui les lie. Les contrôles applicables aux sous-traitants sont également abordés dans la SE 3.2.4.4, qui traite de la gestion des prestations de services des fournisseurs. Pour les contrats de sous-traitance de longue durée, l'administration fiscale peut demander à ce que la vérification des antécédents du sous-traitant ou de son personnel soit renouvelée de temps en temps (selon les intervalles minimums prévus par la législation en vigueur ou par la politique générale du personnel, par exemple). L'encadré 11 présente quelques exemples de contrôles à effectuer lors du recrutement.

Encadré 11. **Exemples de contrôles applicables lors du recrutement**

L'administration fiscale de la juridiction A procède à des vérifications des antécédents pour toutes les catégories de personnel. Lors de la procédure de recrutement, elle demande au ministère de l'Intérieur un certificat attestant que la personne concernée ne s'est vue infliger aucune sanction pénale et ne fait pas l'objet de poursuites pénales. Des preuves des diplômes et titres mentionnés par le candidat sont également demandées. Ses anciens employeurs sont contactés.

Si le poste visé implique l'accès à des informations confidentielles (renseignements échangés, par exemple), un processus de validation et d'habilitation de sécurité est également lancé et prévoit des enquêtes sur les affaires financières de la personne, sa nationalité, sa santé mentale et d'autres informations personnelles pertinentes. Si le candidat avait déjà été employé par l'administration fiscale, des facteurs tels que le respect des règles en matière de traitement des informations et des documents ainsi que la conduite en général pendant la période d'emploi sont pris en compte.

Si l'administration fiscale doit engager des sous-traitants pour gérer des renseignements échangés, ou pour obtenir des logiciels, du matériel ou des services, les membres de leur personnel font également l'objet de vérifications des antécédents, de contrôles et de validation comme pour le personnel régulier, en fonction des risques identifiés et du type de service à fournir. La société elle-même serait également examinée pour vérifier l'existence d'éventuels problèmes de réputation.

Phase 3 : communication sur les rôles et obligations en matière de confidentialité lors du recrutement

Comme expliqué dans la SE 3.2.2.1, les candidats à un emploi dans l'administration fiscale doivent être correctement informés sur leurs obligations lors de la procédure de recrutement, mais cette règle s'applique aussi lors de la prise de fonction de nouveau personnel et pendant toute la période d'emploi. Les rôles et responsabilités en matière de confidentialité et de sécurité de l'information devraient être clairement documentés et communiqués à l'ensemble des recrues et du personnel, notamment par les moyens suivants :

- dispositions relatives au secret fiscal dans la législation applicable, par exemple le code des impôts ou le code de la fonction publique ;
- politique de sécurité ou autres documents relatifs à la gestion de la sécurité de l'information ;
- contrats, conditions d'emploi ou autres instruments officiels de nomination signés par le personnel ;
- accords de confidentialité et de non-divulgation ou ententes similaires, telles qu'une clause de confidentialité insérée dans les contrats du personnel travaillant dans l'unité chargée de l'échange de renseignements.

Il convient également que les administrations fiscales s'assurent que le personnel nouvellement embauché a bien compris ses obligations et qu'il s'engage à travailler dans le respect des politiques de confidentialité et de sécurité. À

Encadré 12. **Exemple de communication sur les obligations de confidentialité lors du recrutement**

Au moment d'être embauchée par l'administration fiscale de la juridiction B, chaque personne signe un accord de confidentialité et de non-divulgation dans le cadre de ses conditions d'emploi. Dans cet accord, elle est explicitement informée de ce qui suit :

- L'accès aux systèmes d'information est strictement réservé aux activités professionnelles appropriées.
- L'usage qu'elle fait des systèmes d'information peut faire et fera l'objet d'une surveillance.
- Tout usage inapproprié peut entraîner une enquête administrative et, le cas échéant, pénale.

En outre, les nouvelles recrues reçoivent un exemplaire de la partie du code des impôts qui énonce les obligations en matière de secret fiscal.

Elles assistent à une brève séance de formation donnée par un représentant du service de gestion des ressources humaines et le responsable du service du recrutement, qui expliquent comment interpréter la législation et l'appliquer dans la pratique, ainsi que les obligations en matière de confidentialité et de non-divulgation. Ensuite, elles doivent compléter un court questionnaire.

Au terme de ce programme d'initiation, elles participent à une cérémonie officielle au cours de laquelle elles prêtent un serment de confidentialité, qu'elles s'engagent à respecter même lorsque la relation d'emploi sera terminée.

cette fin, des processus et des procédures devraient être mis en place pour déterminer l'efficacité de la communication, quel que soit l'instrument ou le moyen de communication utilisé. Par exemple, les administrations fiscales peuvent expliquer les politiques de confidentialité et évaluer dans quelle mesure elles sont comprises par le personnel grâce à des programmes d'initiation obligatoires assortis de tests et d'un retour d'information des participants pendant la première semaine d'emploi. L'encadré 12 présente un exemple de ce type de communication lors du recrutement.

Sous-traitants

Une administration fiscale peut avoir recours à des prestataires externes pour obtenir certains services, comme des services informatiques, des services de nettoyage, ou l'entretien des imprimantes, ou faire appel à des contractants recrutés pour leurs compétences spécifiques, telles que l'analyse de données, entre autres. Ces sous-traitants et leur personnel doivent comprendre les politiques de confidentialité de l'administration fiscale et s'engager à les respecter et à les faire respecter.

Les relations avec les sous-traitants seront normalement régies par des contrats et/ou des accords de niveau de service, qui sont analysés plus en détail dans la SE 3.2.4.4 portant sur la gestion des prestations de services des fournisseurs :

- Un **contrat** est une convention contraignante qui stipule les obligations et responsabilités des parties.
- Un **accord de niveau de service** est une entente conclue avec un sous-traitant par laquelle une administration fiscale définit le niveau de service minimum attendu de celui-ci. Les accords de niveau de service portent essentiellement sur des mesures de performance et des indicateurs qui visent à s'assurer que la prestation de service par le sous-traitant est conforme aux critères de qualité convenus.

Que la relation soit régie par un contrat ou un accord de niveau de service, le document doit formuler explicitement les obligations en matière de protection de la confidentialité et de sécurité de l'information, à savoir au minimum les points ci-dessous :

- **Accès**. L'accès aux systèmes de l'administration fiscale doit être accordé sur la base du « besoin d'en connaître » et être en rapport avec le champ d'application des services que le contractant est appelé à fournir (voir la SE 3.2.3 pour de plus amples détails sur la gestion des accès).
- **Signalement des incidents**. Les sous-traitants doivent signaler tous les incidents liés à la sécurité de l'information au RSSI dès que possible après qu'ils se sont produits ou ont été constatés. En cas d'atteinte à la confidentialité, l'incident doit faire l'objet d'une remontée (voir la SE 3.2.6.6 pour de plus amples détails sur la gestion des incidents de sécurité).

Sous-exigences 3.2.2.3 et 3.2.2.4. Étape 2 : contrôles applicables tout au long de la relation employeur-employé

Cette section vise à garantir que, durant sa période d'emploi, le personnel est régulièrement tenu informé de ses obligations de confidentialité et qu'il applique correctement les politiques et procédures de sécurité au quotidien. Pour ce faire, il convient d'envisager un programme associant formation et sensibilisation, ainsi que la mise en place de mécanismes visant à encourager et à contrôler la conformité.

La SE 3.2.2.3 prescrit que les administrations fiscales doivent veiller à ce que leurs agents et sous-traitants reçoivent régulièrement des formations et des messages de sensibilisation à la sécurité, dont le contenu sera parfaitement à jour, et que les personnes occupant des

postes sensibles bénéficient d'orientations supplémentaires concernant le traitement des informations plus confidentielles. La SE 3.2.2.4 indique quant à lui qu'elles sont tenues de s'assurer que leur personnel applique correctement les politiques et procédures de sécurité.

Formation et sensibilisation à la sécurité

Bien que la formation et la sensibilisation aient des objectifs similaires et connexes, il s'agit néanmoins de concepts distincts (voir figure 8).

En matière de formation et de sensibilisation, les besoins ainsi que les contenus et la périodicité doivent être identifiés et définis à la fois aux échelons supérieurs de l'administration fiscale (RSSI, hauts responsables des divisions de l'administration fiscale, services de gestion des ressources humaines et informatique, par exemple) et dans le cadre de la relation qui unit le responsable hiérarchique à son équipe.

Formation

Les formations sur la confidentialité et la sécurité devraient faire partie intégrante des exigences institutionnelles et des politiques de développement professionnel du personnel. La formation est un processus qui débute avant la tenue des activités de formation, au moment d'identifier les besoins en formation, et qui se poursuit jusqu'à ce que le personnel applique effectivement les connaissances ainsi acquises dans son travail quotidien. Les formations doivent être dispensées de manière régulière, pour que le personnel soit au fait des dernières évolutions.

Selon le modèle adopté pour sa fonction de formation et de développement professionnel, une administration fiscale peut désigner des responsables différents pour diriger les formations sur la confidentialité et la sécurité. Dans tous les cas, il est recommandé de faire en sorte que les services chargés des ressources humaines, de l'informatique et de la sécurité participent à l'élaboration du contenu des formations et à leur conduite.

Différentes formations à la sécurité peuvent être assurées, dont les suivantes :

- **Formations aux concepts de base de la sécurité**. Celles-ci s'adressent à tout le personnel et les informent sur la politique de sécurité et d'autres politiques importantes de l'administration relatives aux processus de confidentialité et de sécurité, telles que le code des impôts, les mesures de sécurité physique, etc. Elles peuvent être intégrées à la formation d'initiation évoquée précédemment, dans le contexte des contrôles à effectuer lors du recrutement.
- **Formations associées à la fonction**. Elles sont adaptées aux besoins de chaque fonction. Par exemple, le personnel de l'unité chargée de l'échange de renseignements est censé recevoir une formation spéciale sur les processus de traitement des informations échangées, comme indiqué dans le manuel sur l'échange de renseignements ou dans une procédure similaire, et il doit être particulièrement sensibilisé aux obligations découlant des traités conclus, concernant le traitement et l'utilisation des informations reçues des autorités compétentes étrangères. En outre, les membres du personnel occupant des postes de haut niveau ou ayant des responsabilités importantes (dont le RSSI) pourraient bénéficier d'une formation ad hoc liée aux impératifs particuliers de leur fonction, telle qu'une formation certifiée en matière d'opérations de sécurité, de cyber sécurité, de gestion des accès, etc.
- **Formations sans lien avec une fonction spécifique**, mais ayant trait à l'environnement de travail du personnel. Ces formations peuvent par exemple expliquer comment prendre soin des installations et du matériel (ordinateurs de bureau et portables, par exemple) ou les risques associés aux technologies Internet.
- **Formations basées sur les changements de fonction**, qui sont données par exemple lors de la promotion à un nouveau poste.

Sensibilisation

Les campagnes de sensibilisation peuvent servir à transmettre :

- **des messages relatifs aux menaces et risques informatiques**, par exemple pour avertir le personnel

FIGURE 8. **Définitions des concepts de formation et de sensibilisation**

Formation	Accompagnement du personnel pour qu'il acquière et développe les connaissances, les aptitudes et les compétences de base nécessaires pour intégrer la confidentialité et la sécurité dans les processus fiscaux.
Sensibilisation	Pratique consistant à exposer régulièrement le personnel à des messages les mettant en garde contre les menaces et risques de sécurité, liés à l'informatique ou non. Ces communications sont généralement transmises simultanément à l'ensemble du personnel, ou du moins au personnel faisant partie de groupes ou de domaines bien définis (y compris le personnel externe, le cas échéant).

des dangers que représente le fait de cliquer sur un lien contenu dans un courriel provenant d'une source inconnue, ou à le mettre en garde contre les *attaques d'hameçonnage ou de harponnage*[13], qui peuvent tenter de recueillir des informations et dont l'utilisation pourrait mettre en péril les données de l'administration fiscale en déclenchant des téléchargements de programmes malveillants, tels que des logiciels de demande de rançon et des logiciels espions ;

- **des messages relatifs aux menaces et risques pour la sécurité physique**, par exemple en rappelant au personnel l'importance de toujours signaler la perte d'un badge d'identification avec photo.

Les campagnes de sensibilisation devraient non seulement aider le personnel à éviter d'être victime d'attaques informatiques ou autres, mais aussi lui apprendre ses responsabilités en tant qu'agent du fisc (par exemple, toujours signaler les attaques d'hameçonnage au service responsable et/ou au RSSI, afin que des mesures préventives ou correctives appropriées puissent être prises).

Comme pour les formations, il est recommandé de faire participer les services chargés des ressources humaines, de l'informatique et de la sécurité à l'élaboration de ces campagnes et à leur déploiement. L'encadré 13 présente un exemple de formation et de sensibilisation à la sécurité au sein d'une administration fiscale.

Vérifier que le personnel applique correctement les politiques et procédures de sécurité

Les membres du personnel doivent appliquer les politiques de sécurité dans leur travail quotidien et lorsqu'ils utilisent des systèmes ou processus qui impliquent le traitement d'informations confidentielles. L'encadrement supérieur de l'administration fiscale a besoin de méthodes pour évaluer le niveau d'observance des obligations de sécurité par le personnel. Ces méthodes peuvent consister par exemple à :

- intégrer la sécurité de l'information parmi les objectifs ou indicateurs de performance du personnel, et dans la liste des points abordés lors des réunions sur la performance entre l'encadrement et leurs subordonnés ;
- définir clairement les objectifs des formations et des campagnes de sensibilisation à la sécurité, en fonction des impératifs de confidentialité auxquels elles répondent, et assurer le suivi de leurs résultats au moyen d'enquêtes ou de questionnaires, de réunions d'équipe et d'un retour d'information du personnel à l'encadrement supérieur.

Le rôle des encadrants est crucial, car ce sont eux qui auront la plus grande force de persuasion pour amener leur équipe

13. Les e-mails d'hameçonnage sont envoyés à de nombreux destinataires. Les e-mails d'harponnage ciblent un seul destinataire.

Encadré 13. **Exemple de formation et de sensibilisation à la sécurité**

Tout le personnel de l'administration fiscale de la juridiction C reçoit une formation obligatoire sur la sécurité de l'information au moins tous les deux ans, conformément à la politique de GSI. La formation est dispensée par l'Institut d'études fiscales, qui fait partie de l'administration fiscale. Son contenu est élaboré par le RSSI en collaboration avec le chef du service informatique et l'Institut, et il est régulièrement mis à jour en fonction de l'évolution de l'environnement de sécurité et des commentaires des participants et des cadres supérieurs. La formation traite de la confidentialité en relation avec les processus fiscaux, ainsi que de questions plus générales, telles que les risques découlant de l'utilisation des nouvelles technologies et des médias sociaux, ainsi que les risques liés à la sécurité physique.

L'administration fiscale propose également des modules de formation en ligne sur les thèmes suivants :

- législation relative au secret fiscal, politique de GSI et code de déontologie ;
- protection contre les menaces informatiques et d'Internet, l'ingénierie sociale et l'hameçonnage ;
- classification, stockage et gestion des informations ;
- signalement des incidents de sécurité et gestion des violations de données.

Ces modules de formation en ligne comportent, à la fin de chaque section, des questionnaires permettant de vérifier que le participant a assimilé les acquis obligatoires pour qu'il puisse poursuivre la formation. Il doit fournir au minimum 90 % de réponses correctes à chaque questionnaire. Le RSSI et les responsables hiérarchiques vérifient que chaque membre du personnel a réussi la formation et reçoivent un retour d'information par le biais des réunions d'équipe.

Le personnel reçoit quotidiennement des courriels du service informatique concernant la protection des informations et des systèmes informatiques contre les menaces internes et externes. Ces messages contiennent des exemples en rapport avec divers sujets : courriels malveillants, gestion des mots de passe, politique du bureau et de l'écran propres, ingénierie sociale et canulars sur Internet. Ils sont également disponibles sur l'intranet de l'administration fiscale.

L'administration fiscale impose à ses sous-traitants d'assurer à leur personnel des formations sur la sécurité de l'information, conformément aux accords de niveau de service conclus. Son équipe d'audit interne vérifie chaque année que les sous-traitants respectent cette obligation.

Encadré 14. **Exemple de mise en œuvre et d'évaluation du respect des politiques de confidentialité**

Le personnel de l'administration fiscale de la juridiction A se voit régulièrement rappeler son obligation de préserver la confidentialité des informations fiscales, par le biais de bannières contextuelles, d'annonces sur l'intranet et de formations. Les procédures disciplinaires sont publiées sur l'intranet. L'accès non autorisé et la divulgation d'informations sont considérés comme des fautes graves.

Tout le personnel exerçant des fonctions liées à la gestion des informations sur les contribuables est tenu d'inclure dans ses objectifs annuels au moins un objectif ayant trait à la sécurité de l'information.

L'équipe d'audit interne effectue de manière suivie certains contrôles, tels que l'examen des journaux d'audit des accès aux systèmes, pour vérifier si des membres du personnel ont consulté des informations alors qu'ils n'y étaient pas autorisés. Les résultats de ces contrôles sont communiqués aux responsables hiérarchiques et au RSSI.

Lorsqu'une action administrative ou judiciaire est engagée contre un membre du personnel pour violation des obligations de confidentialité, les faits sont portés à la connaissance du reste du personnel via les réunions de service et l'intranet, à titre de dissuasion.

à entreprendre les formations nécessaires, et ils pourront vérifier que celle-ci a bien compris les concepts abordés et les applique correctement dans ses tâches quotidiennes.

S'assurer que le personnel applique les politiques de confidentialité et de sécurité passe également par des procédures disciplinaires et des sanctions en cas de non-respect. Ces procédures doivent être portées à la connaissance du personnel et lui être rappelées à chaque étape du cycle de vie de l'emploi.

Les sanctions peuvent être de nature administrative, civile ou pénale, en fonction de la gravité de l'infraction. Le cadre juridique national devrait permettre l'imposition de sanctions (cet aspect est analysé en détail dans l'EF 3.3, qui traite des dispositions contraignantes et des processus applicables en cas de non-respect des obligations de confidentialité).

Les administrations fiscales doivent clairement démontrer leur volonté d'appliquer des sanctions pour tout comportement qui ne répond pas aux normes établies, et lorsque la protection des informations est en jeu. Par ailleurs, il est essentiel que le personnel sache qu'en matière de sécurité de l'information, les bonnes conduites et les bons résultats seront récompensés, tandis que les mauvaises pratiques seront combattues et sanctionnées comme il se doit. L'encadré 14 présente un exemple de mise en œuvre et d'évaluation du respect des politiques de confidentialité.

Sous-exigence 3.2.2.5. Étape 3 : contrôles applicables lors de la cessation d'emploi

La SE 3.2.2.5 prévoit que les administrations fiscales doivent disposer de politiques et de processus de gestion des ressources humaines visant à protéger les informations confidentielles au terme de la relation de travail. En d'autres termes, elles doivent se doter de procédures bien définies à appliquer lorsqu'une personne prend sa retraite ou démissionne ou lorsque son contrat de travail prend fin, et ce pour toutes les catégories de personnel, y compris les sous-traitants. Certaines administrations fiscales peuvent considérer qu'un changement de poste constitue une cessation d'emploi dans la fonction précédente, et les contrôles décrits dans cette section peuvent être utilisés dans pareil cas de figure, le cas échéant.

Ces contrôles doivent garantir que la confidentialité des informations est préservée au terme de la période d'emploi, et ils couvrent essentiellement les aspects décrits ci-après (voir un exemple dans l'encadré 15).

Récupération des actifs ou biens mis à disposition par l'administration

Un processus devrait être prévu pour vérifier que tout personnel sortant a bien restitué tous les biens qui lui avaient été fournis par l'administration, à savoir, entre autres, les badges d'identification, les ordinateurs portables, les téléphones mobiles et les clés USB (ce processus est lié à la SE 3.2.4.3, qui traite de la gestion des actifs).

Les supérieurs hiérarchiques et/ou les services chargés de la gestion des actifs ou des ressources humaines devraient être responsables de ce processus. Ce dernier peut être exécuté, par exemple, au moyen d'une liste de contrôle qui sera signée par le membre du personnel concerné, parfois dans le cadre d'une « réunion de départ ».

Retrait des droits d'accès

Le retrait des droits d'accès consiste à révoquer rapidement, lorsque la situation l'exige, toutes les autorisations d'accès d'une personne, tant pour l'accès physique (aux bâtiments ou aux bureaux) que logique (aux systèmes). La SE 3.2.3, qui porte sur la gestion des accès, décrit en détail comment déterminer les besoins en matière d'accès physique et comment octroyer et retirer des droits d'accès logique.

Normalement, les agents sont autorisés à accéder à des zones de travail privées de l'administration fiscale, et certains peuvent avoir des droits spéciaux leur donnant accès à des zones soumises à un contrôle plus strict (les

centres de données ou les salles d'archives, par exemple). L'accès à ces zones peut être autorisé au moyen d'un badge d'identification avec photo, d'un laissez-passer électronique, d'un dispositif d'identification biométrique, de codes de sécurité ou d'autres méthodes, en fonction des mesures de sécurité physique requises par les différents locaux.

S'agissant du personnel sortant, toutes ces autorisations d'accès devraient lui être retirées en exigeant de lui de restituer le badge d'identification avec photo, de désactiver l'identification biométrique et les codes de sécurité, etc. Interviennent généralement dans ce processus les responsables hiérarchiques, la direction de la sécurité physique et/ou le service des ressources humaines.

Un processus permettant de retirer les droits d'accès logique aux systèmes dans les plus brefs délais devrait également être mis en place, vu son caractère primordial pour la sécurité de l'information, car le piratage des droits d'accès non utilisés est une cause majeure de violations de données.

L'utilisation des droits d'accès logique doit donc faire l'objet d'un contrôle rigoureux. Leur retrait doit être organisé avant le dernier jour où ces droits sont nécessaires, et les droits doivent être retirés à la fin de ce dernier jour. Par ailleurs, ce retrait devrait être du ressort des cadres responsables de l'application ou du processus fiscal concerné (avec le soutien technique du département informatique), car ce sont eux qui sont chargés de déterminer les critères d'accès et d'approuver les droits d'accès au système.

Si un membre du personnel quitte l'administration fiscale ou est licencié pour faute, le processus doit permettre de lui retirer immédiatement tous ses droits d'accès (physiques et logiques) si une demande appropriée est introduite (par un cadre supérieur ou le supérieur hiérarchique, ou le service d'enquête, par exemple).

Clarification des obligations futures concernant la confidentialité

Le personnel d'une administration fiscale en apprend beaucoup sur les informations sensibles concernant les contribuables et leurs affaires fiscales. Il doit en assurer la confidentialité, et ce même après la fin de la relation d'emploi. Cette obligation doit être clairement portée à l'attention du personnel dont le contrat de travail est sur le point de prendre fin. Elle doit être également énoncée dans un document officiel signé par la personne et par un cadre habilité (par exemple, le document couvrant également la restitution des actifs).

SOUS-EXIGENCE 3.2.3 : CONTRÔLES DES ACCÈS PHYSIQUES ET LOGIQUES

La SE 3.2.3 vise à protéger la confidentialité en garantissant que seuls les utilisateurs qui ont un motif professionnel légitime de consulter certaines informations puissent y accéder.

Les normes internationales en matière de GSI exigent des administrations fiscales qu'elles disposent de politiques globales de gestion des accès couvrant tous les types d'accès (voir la SE 3.2.3.1 pour l'accès physique et la

Encadré 15. **Exemple de contrôles applicables lors de la cessation d'emploi**

Dans l'administration fiscale de la juridiction B, les droits d'accès aux systèmes du personnel sortant lui sont automatiquement retirés par le service informatique en fonction de la date de fin de contrat communiquée par le service des ressources humaines. Si la situation l'exige, par exemple en cas de mauvaise conduite, le retrait de ces droits intervient avant cette date.

Un entretien de sortie a lieu le dernier jour de travail. Le supérieur hiérarchique de la personne concernée, un représentant du service des ressources humaines et un représentant de la direction du service de la sécurité physique sont présents. La personne est tenue de signer un document attestant que tous les biens et actifs mis à disposition par l'administration ont été restitués et qu'elle est astreinte à vie au secret en ce qui concerne toutes les informations confidentielles dont elle a eu connaissance durant la période où elle était employée par l'administration fiscale. Le document indique également que le non-respect des dispositions en matière de confidentialité sera sanctionné civilement ou pénalement, et recommande d'éviter toute situation ou tout poste qui pourrait donner lieu à des conflits d'intérêts eu égard aux obligations de confidentialité applicables.

L'entretien de sortie prévoit également de vérifier que tous les biens de l'administration ont été récupérés et que tous les droits d'accès ont été retirés, et ce au moyen d'une liste de contrôle portant sur ce qui suit :

- Récupérer le laissez-passer, les jetons de sécurité, codes et clés qui avaient été délivrés à la personne pour qu'elle puisse accéder aux informations confidentielles sur les systèmes et dans les locaux
- Récupérer l'ordinateur portable et le téléphone mobile fournis par l'administration
- Reprendre tous les actifs informationnels et les documents confidentiels qui lui avaient été remis pour accomplir son travail
- Vérifier qu'elle n'a plus accès aux applications informatiques et aux locaux/zones à accès restreint
- Vérifier que son compte de messagerie a été désactivé
- Signaler son départ aux parties concernées (collègues, etc.).

Tableau 10. **Définitions des principaux concepts**

Concept	Description
Accès logique	Accès aux systèmes par les processus d'identification, d'authentification et d'autorisation.
Accès physique	Accès à des zones spécifiques sur site.
Authentification	Lorsqu'un utilisateur accède aux systèmes informatiques, le processus d'authentification garantit et confirme l'identité de l'utilisateur en se basant sur le principe de non-répudiation.
Autorisation	Processus qui permet à un utilisateur authentifié sur un système d'accéder à des ressources selon les principes du « besoin d'en connaître » et du « moindre privilège ».
Besoin d'en connaître	Principe de la gestion des accès selon lequel les informations sur les contribuables ne doivent être accessibles qu'au personnel ayant un motif professionnel légitime de les consulter.
Contrôles d'accès	Contrôles de sécurité garantissant que l'accès aux informations, aux locaux et aux systèmes est accordé selon les principes du « besoin d'en connaître » et du « moindre privilège ».
Fourniture d'accès	Le fait d'accorder l'accès aux informations par la création de comptes utilisateur, la gestion des mots de passe et l'attribution de droits d'accès et d'autorisations spécifiques aux utilisateurs.
Gestion des accès	Politiques, processus et procédures, relevant de la haute direction du management supérieur, et non pas uniquement de la fonction informatique de l'administration fiscale, qui régissent les accès physiques et logiques, et ainsi que les processus effectifs relatifs à l'octroi et l'audit au contrôle de l'accès logique et à l'identification et l'authentification des utilisateurs.
Identification	Processus utilisé par les systèmes informatiques pour identifier un utilisateur doté d'un droit d'accès en l'individualisant.
Moindre privilège	(Droits strictement nécessaires) Principe de la gestion des accès selon lequel l'accès légitime doit être limité aux fonctions spécifiques minimales dont l'utilisateur a besoin pour effectuer son travail.
Utilisateur légitime	Utilisateur qui obtient un droit d'accès spécifique en vertu des principes du « besoin d'en connaître » et du « moindre privilège ».

SE 3.2.3.3 pour l'accès logique aux systèmes informatiques).

Les administrations fiscales devraient par conséquent prendre des dispositions pour, d'une part, mettre en œuvre et administrer ces politiques comme il se doit, c'est-à-dire protéger de façon adéquate leurs locaux et avoir défini des périmètres internes et externes (SE 3.2.3.2) et, d'autre part, autoriser les accès logiques comme indiqué par les responsables opérationnels, et pas uniquement par le service informatique (SE 3.2.3.4).

La présente section a pour objet de fournir des orientations concernant la définition de ces politiques et leur mise en application. Le tableau 10 présente les définitions des principaux concepts abordés dans la SE 3.2.3.

Cette SE comporte trois volets :

- Principes généraux de la gestion des accès
- Orientations sur la sécurité physique dans les locaux des administrations fiscales (SE 3.2.3.1 et 3.2.3.2)
- Orientations pour la mise en place d'une politique et de contrôles en matière d'accès logique (SE 3.2.3.3 et 3.2.3.4).

Cette section n'a pas vocation à traiter en profondeur le sujet de la gestion de l'accès. Elle met en lumière des aspects génériques susceptibles de s'appliquer à toutes les administrations fiscales et considérés comme essentiels pour la gestion des accès dans le contexte d'une telle administration.

Grands principes de la gestion des accès

Les normes internationales relatives à la gestion des accès sont régies par deux principes, qui doivent être appliqués sans exception (voir figure 9) :

- **Les accès doivent être contrôlés selon le principe du « besoin d'en connaître »**, ce qui signifie que les informations sur les contribuables ne doivent être accessibles qu'au personnel ayant un motif professionnel légitime de les consulter. Ce principe en sous-tend un autre, appelé principe du « moindre privilège », selon lequel l'accès légitime doit être limité aux fonctions spécifiques dont les utilisateurs ont besoin pour accomplir leur travail. Grâce à l'application de ces principes, les contribuables sont assurés de la protection de leur droit à la vie privée et donc de pouvoir communiquer ouvertement avec les autorités fiscales.

- **Les accès (physiques et logiques) doivent être consignés** dans des journaux ou des registres, qui mentionnent l'identité des personnes qui ont accédé aux locaux ou aux informations, les dates et heures de ces accès et leur durée, et détaillent les actions effectuées. L'application de ce principe permet de remonter plus facilement aux personnes concernées et de décourager fortement les actions inappropriées et illicites.

FIGURE 9. **Principes de la gestion des accès**

Le tableau 11 présente les catégories d'utilisateurs qui peuvent légitimement accéder aux informations au sein d'une administration fiscale.

Sous-exigences 3.2.3.1 et 3.2.3.2. Sécurité des accès physiques

Cette section traite de la manière d'aborder les politiques de sécurité pour les accès physiques à chacune des zones d'une administration fiscale, ainsi que les procédures et contrôles requis pour garantir leur efficacité.

Transposer la sécurité physique en politique(s)

L'accès physique aux bâtiments d'une administration fiscale doit être encadré par une ou plusieurs politiques de sécurité physique approuvées par l'encadrement supérieur. La SE 3.2.3.1 exige par conséquent des administrations fiscales qu'elles se dotent d'une politique de contrôle des accès physiques, qui sera sous la responsabilité de l'encadrement supérieur. En vertu de la SE 3.2.3.2, elles sont tenues de dûment protéger leurs sites physiques et d'avoir établi des périmètres sécurisés, intérieurs comme extérieurs.

Les politiques doivent être en adéquation avec la taille et la complexité de l'administration fiscale, et elles doivent fournir des orientations aux responsables de la gestion de la sécurité physique dans chacun des sites d'implantation de l'administration.

Les politiques de sécurité physique peuvent être définies en termes de conception de la sécurité des locaux physiques, de besoins des utilisateurs et de contrôles spécifiques mis en place pour gérer l'accès.

Conception de la sécurité des sites physiques

Les politiques doivent définir les différents sites, à savoir bâtiments, locaux et bureaux, de l'administration fiscale et déterminer les mesures de sécurité physique requises

Tableau 11. **Catégories d'utilisateurs légitimes**

Utilisateurs	Description
Agents de l'administration fiscale	Membres du personnel qui, en raison de leur fonction, sont directement impliqués dans le traitement des informations sur les contribuables. Il peut s'agir du personnel de l'unité chargée de l'échange de renseignements et de certaines divisions responsables d'activités d'analyse des risques et de contrôle qui utilisent les renseignements échangés (exemples de divisions : grandes entreprises et activités internationales, contrôle fiscal international, grandes fortunes).
Sous-traitants informatiques	Personnels des sous-traitants informatiques qui gèrent des services pour le compte de l'administration fiscale, tels que ceux qui administrent les systèmes et les bases de données hébergeant les informations sur les contribuables, y compris les renseignements échangés, et qui ont fait l'objet d'une vérification des antécédents et d'un contrôle d'habilitation appropriés.
Autorités de contrôle	Tribunaux, organes administratifs et de supervision impliqués dans l'établissement, le prélèvement, le recouvrement, les poursuites et les décisions sur les recours relatifs à l'impôt, y compris en ce qui concerne les renseignements échangés en vertu d'un accord international. Certains pays ont mis en place des systèmes juridiques permettant de partager des données avec des autorités de contrôle spécifiques et autorisées.
Contribuables et mandataires	Les informations peuvent également être communiquées aux contribuables concernés et à leurs représentants autorisés (par exemple, les mandataires). La technologie moderne permet aux juridictions de mettre en place des systèmes de libre-service grâce auxquels les contribuables peuvent non seulement déposer eux-mêmes leur déclaration fiscale, mais également gérer les paiements et d'autres aspects de leurs affaires fiscales.

en fonction des catégories d'utilisateurs qui devront accéder à ces diverses zones.

Lors de l'élaboration des politiques de sécurité physique, il faut tout d'abord chercher à protéger les informations contre tout accès illégitime. À cette fin, les bonnes pratiques internationales à prendre en considération sont les suivantes :

- Aménagement des locaux de manière à pouvoir séparer des autres les utilisateurs « de confiance » (agents et sous-traitants), qui ont le droit d'accéder aux zones réservées, réglementées ou internes
- Organisation de l'espace des bâtiments et des locaux conformément aux principes du « besoin d'en connaître » et du « moindre privilège », et séparation physique pour les zones de travail plus sensibles ou celles où se déroulent des activités critiques (par exemple, les centres de données ou les lieux de traitement des données fiscales particulièrement sensibles, qui sont uniquement accessibles avec des niveaux d'habilitation de sécurité élevés, accordés aux personnes de haute confiance comme les membres de l'unité chargée de l'échange de renseignements).

Catégories d'utilisateurs et leurs besoins en matière d'accès et de sécurité

Pour les différentes catégories d'utilisateurs, dont les niveaux de droits d'accès varient, il faut établir leurs besoins professionnels spécifiques ainsi que des ensembles de contrôles pour garantir qu'ils n'accèdent qu'aux locaux pour lesquels cet accès est justifié par un motif légitime.

Établir les besoins implique d'évaluer quels utilisateurs doivent disposer de l'accès, à quoi ils doivent accéder et pourquoi. Les principales catégories d'utilisateurs sont les suivantes :

- Agents de l'administration fiscale qui ont le droit d'accéder aux zones privées des bâtiments ;
- Agents autorisés à accéder à des bâtiments tels que le centre de données, dont l'accès fait l'objet d'un contrôle plus strict ;
- Personnel d'autres départements gouvernementaux ;
- Personnel des prestataires de services informatiques et non informatiques (société de nettoyage, par exemple) ;
- Contribuables et représentants fiscaux en visite pour discuter de questions fiscales, ou membres du public.

Si l'administration fiscale est implantée dans des locaux dont elle n'est pas propriétaire, le bâtiment peut héberger d'autres catégories d'utilisateurs particuliers ayant leurs propres besoins en matière de sécurité.

Contrôles visant à gérer les accès physiques

Les politiques doivent inclure un ensemble structuré de contrôles de sécurité physique appliqués au sein de l'administration fiscale. Pour que ces contrôles soient conformes aux bonnes pratiques, ils doivent être fondés sur les risques et tenir compte des considérations relatives à la conception physique et aux besoins des utilisateurs.

Tableau 12. **Exemple de tableau de la sécurité physique**

Locaux	Catégories d'utilisateurs	Contrôles
Entrée principale	Agents de l'administration fiscale, sous-traitants informatiques	Vidéosurveillance en temps réel, agents de sécurité, contrôle des effets personnels
	Autres autorités publiques	
	Contribuables	
Bureaux internes	Agents de l'administration fiscale, sous-traitants informatiques	Laissez-passer électroniques avec identifiant et photo, tourniquets, vidéosurveillance
	Autres autorités publiques	Laissez-passer provisoires avec identifiant, tourniquets, vidéosurveillance ; doivent être constamment escortées par des agents de l'administration fiscale
Unité chargée de l'échange de renseignements et salles d'archives	Personnel de l'unité chargée de l'échange de renseignements	Laissez-passer électroniques avec identifiant et photo, tourniquets, vidéosurveillance, système d'alarme et de détection des intrusions, serrures d'entrée à touches, authentification multifacteur aux dispositifs informatiques
Centre de données	Administrateurs informatiques	Laissez-passer électroniques avec identifiant et photo, tourniquets, vidéosurveillance, système d'alarme et de détection des intrusions, serrures d'entrée à touches, authentification multifacteur aux dispositifs informatiques, système de climatisation, protection contre les incendies

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Encadré 16. Bonnes pratiques internationales en matière d'élaboration des contrôles de sécurité physique

Les contrôles de sécurité physique doivent être structurés de manière logique. Ainsi, il conviendrait de procéder de « l'extérieur vers l'intérieur », en commençant par le contrôle le plus éloigné, situé à l'endroit où une personne s'approche d'un bâtiment, et en se dirigeant progressivement vers le poste de travail de l'utilisateur. Cette approche logique devrait répondre aux questions suivantes :

- Que trouve-t-on en bordure de périmètre ? Est-ce le terrain entourant chaque bâtiment, y compris les aires de stationnement ? L'accès à la zone de stationnement est-il contrôlé, et si oui, comment ? Si le terrain est clôturé par des barrières, celles-ci sont-elles surveillées ? Des systèmes de contrôle secondaires tels que la vidéosurveillance sont-ils installés, et la surveillance est-elle en temps réel ?
- Existe-t-il un relevé précis des différents accès (portes, portes coupe-feu, etc.) que les utilisateurs peuvent emprunter pour entrer dans le bâtiment ou en sortir ? Et pour chaque type de porte, a-t-on clairement renseigné la manière de l'utiliser et qui doit s'en servir (par exemple, accès du personnel, accès des contribuables ou les deux, sortie de secours, entrée dédiée aux livraisons) ?
- La plupart des bâtiments ont une entrée et, bien souvent, il s'agit d'une zone où le personnel et d'autres personnes se côtoient. Comment les différents utilisateurs du bâtiment sont-ils autorisés à y accéder ? Ont-ils besoin d'un laissez-passer électronique ? Comment les laissez-passer (électroniques ou autres) sont-ils délivrés et contrôlés ? Sont-ils dotés d'une photo ? S'il n'y a pas de photo, existe-t-il d'autres moyens de vérifier que le détenteur du laissez-passer est l'utilisateur légitime ?
- Quels sont les contrôles effectués dans d'autres zones publiques à l'intérieur des bâtiments, comme les guichets de demande d'informations ?
- Comment peut-on accéder aux zones privées d'un bâtiment, par exemple en utilisant un laissez-passer électronique ? Les utilisateurs doivent-ils passer par un tourniquet qui limite l'accès à une personne à la fois ? Si ce n'est pas le cas, existe-t-il des contrôles secondaires, tels que des agents de sécurité ? Ou un système de vidéosurveillance ? Si un tel système est installé, la vidéosurveillance se fait-elle en temps réel ?
- Dans les zones d'accès restreint d'un bâtiment, comment le personnel sait-il si d'autres personnes ont le droit d'y être présente ?
- Quelles sont les règles concernant la gestion de la sécurité physique dans les zones de travail individuelles à l'intérieur des bâtiments ?
- Quels contrôles sont utilisés dans les zones dédiées aux opérations plus sensibles (unité chargée de l'échange de renseignements, salle d'archives) ?
- Quels types de contrôles sont généralement mis en place à l'intérieur d'un bâtiment ? Par exemple, la vidéosurveillance est-elle utilisée et, si oui, à quelles fins ? Et comment est-elle contrôlée ? Il est important de noter que les caméras de vidéosurveillance ne doivent pas être placées en orientant l'objectif vers les bureaux, les écrans de PC, les armoires de dossiers, etc.
- Y a-t-il des espaces publics autour du bâtiment (immeubles voisins, maisons à proximité) qui pourraient être utilisés pour porter atteinte à la confidentialité, et quels sont les contrôles appliqués à cet égard ?

Une approche alternative ?

On peut également envisager de scinder la liste de contrôle comme suit :

- Contrôles de référence qui constituent l'ensemble de contrôles minimaux.
- Tous les contrôles supplémentaires ou renforcés qui sont appliqués en réponse à un risque ou à un problème spécifique.

Une liste complète des contrôles peut être établie, par exemple, sous la forme d'une matrice répertoriant les différentes zones des bâtiments ou la totalité des types d'accès, les catégories d'utilisateurs, les droits d'accès dont ils disposent et les contrôles requis. Le tableau 12 ci-dessous présente un exemple simplifié de matrice de la sécurité physique, tandis que les encadrés 17 et 18 fournissent des orientations détaillées et des exemples d'approches à prendre en considération lors de l'élaboration de contrôles de sécurité physique.

Tester les contrôles de sécurité physique

Un système devrait être mis en place pour vérifier si les contrôles de sécurité prévus dans la politique sont correctement mis en œuvre et fonctionnent efficacement. Les résultats de tests antérieurs réalisés conformément aux plans d'essai devraient être pris en compte pour améliorer les contrôles. Par la suite, ces plans d'essai devraient être revus selon les besoins, en se basant sur les résultats du plan existant.

En général, lors de l'évaluation ou des tests des contrôles de sécurité physique, les aspects suivants doivent être pris en compte :

- Les évaluations de la sécurité physique doivent être réalisées de façon périodique et actualisées en fonction des résultats et des enseignements tirés des évaluations et/ou incidents précédents, avec une combinaison de tests aléatoires et fondés sur les risques.

Encadré 17. **Exemple d'évaluation de contrôles de la sécurité physique**

La division chargée de la gestion de la sécurité physique de l'administration fiscale de la juridiction A vérifie au moins une fois par mois que les contrôles physiques fonctionnent. Elle procède notamment à des inspections techniques des serrures d'entrée, des alarmes et des caméras de surveillance. Un audit de la sécurité physique est réalisé tous les trois ans par un prestataire de services externe.

Toute défaillance du système de contrôle des accès physiques est signalée à la division chargée de la gestion de la sécurité physique. Si des éléments probants indiquent un accès inapproprié aux locaux, une enquête est déclenchée pour déterminer si des dégâts matériels ont été occasionnés (vol ou détérioration de biens, par exemple) ou s'il y a pu y avoir violation de données (numériques ou documents papier). Les résultats et conclusions de l'enquête sont documentés et exploités pour remédier à la défaillance du ou des contrôles à l'origine de l'incident.

Les centres de données sont surveillés et dotés d'un système de contrôle d'accès électronique nécessitant une identification biométrique. Les rapports contenant les journaux d'accès aux centres de données sont examinés toutes les deux semaines. Ces centres sont équipés de systèmes de vidéosurveillance distincts.

- Les incidents et les événements liés à la sécurité physique doivent être signalés rapidement aux responsables des bâtiments, consignés et documentés (les contrôles de gestion des incidents sont décrits plus en détail dans la SE 3.2.6.6). Si les incidents ne sont pas correctement signalés et consignés, on pourrait croire à tort que le système fonctionne. De nombreux types d'incidents peuvent se produire, et leurs niveaux de gravité de même que leur impact peuvent varier. Citons par exemple la perte par un employé de son laissez-passer, les tentatives d'accès inapproprié aux bâtiments, les déplacements d'une zone à l'autre sans utiliser le laissez-passer ou encore le vol de matériel officiel. Le personnel doit être conscient de l'importance de signaler les incidents, dont les détails doivent être en outre documentés dans un format approprié afin que les mesures adéquates puissent être prises.
- Les évaluations des contrôles des sites critiques (dont les centres de données, l'unité d'échange de renseignements et la salle d'archives) devraient, si nécessaire, recourir à des mesures supplémentaires adaptées à la classification des informations traitées dans ces locaux (voir la SE 3.2.5.1 sur la protection des informations) et aux évaluations des risques institutionnels (voir la SE 3.2.1.4 sur la gestion des risques).

Sous-exigences 3.2.3.3 et 3.2.3.4. Accès logique

Cette section expose l'approche globale permettant de concevoir et de tester des contrôles d'accès logiques (i.e. informatiques) appropriés aux informations détenues sous forme électronique dans différents systèmes informatiques.

La SE 3.2.3.3 demande aux administrations fiscales de disposer d'une politique de contrôle d'accès logique, définie par l'encadrement supérieur et basée sur les principes du besoin d'en connaître et du moindre privilège. La SE 3.2.3.4 leur impose de disposer de politiques, de processus et de procédures définie par l'encadrement supérieur et pas uniquement par le service informatique de l'organisation, qui régissent l'accès logique, et de procédures efficaces pour mettre à disposition et réaliser le contrôle de l'accès logique, ainsi que pour identifier et authentifier les utilisateurs.

Les phases de la gestion de l'accès logique

Les exigences se reflètent généralement dans les trois phases de la gestion de l'accès logique, telles que présentées dans la figure 10 :

FIGURE 10. **Les phases de la gestion de l'accès logique**

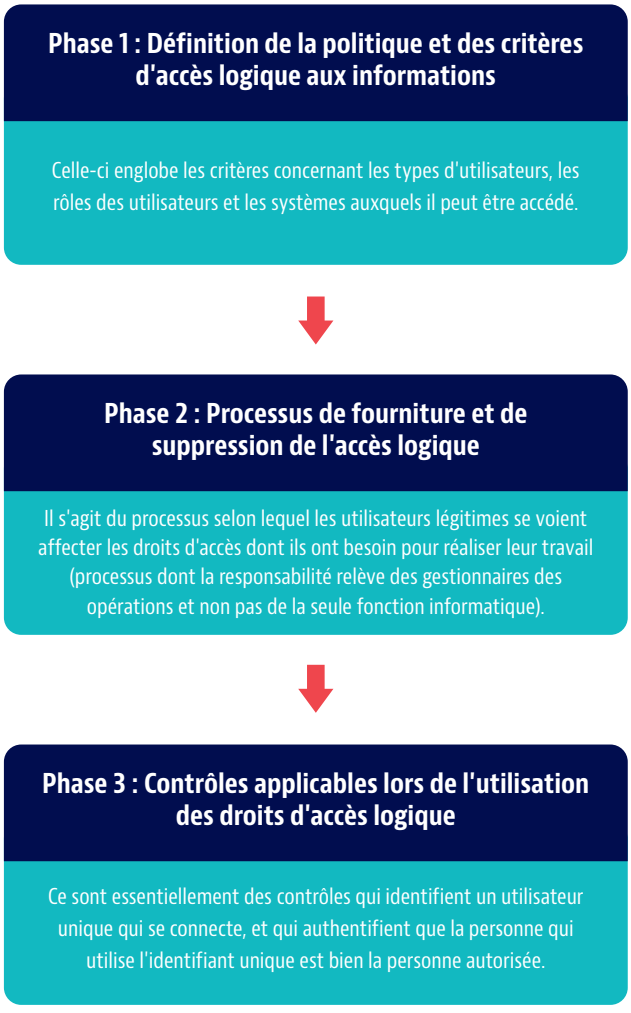


Tableau 13. **Définition de la politique et des critères d'accès logique aux informations**

Considérations permettant de documenter la définition des critères d'accès logique aux informations	Personne(s) définissant les critères de l'accès au système d'information
• La politique d'accès logique doit refléter les principes du besoin d'en connaître et du moindre privilège, à savoir établir que les utilisateurs disposent uniquement des droits d'accès dont ils ont besoin pour réaliser leur travail ou pour remplir leur rôle, et que cet accès légitime doit être restreint aux fonctions spécifiques dont ont besoin les utilisateurs. • Quand des types de rôle utilisateur diffèrent pour différents processus fiscaux, des contrôles adéquats doivent être en place pour garantir la cohérence des critères sur l'ensemble des systèmes. • Les droits d'accès peuvent dépendre du site de stockage des données : centres de données au sein des bâtiments de l'administration fiscale, centres de données délocalisés, ou dans le cloud (nuage). [14] [15] • Il peut exister des droits et politiques d'accès associés à l'utilisation d'applications informatiques, comme la messagerie électronique ou les navigateurs Internet à des fins non professionnelles. • Il peut exister des droits d'accès associés au travail en-dehors du cadre du bureau, en particulier un accès sécurisé à des données confidentielles en cas de travail en-dehors des réseaux locaux au sein des bureaux de l'administration fiscale.	Les critères d'accès logique aux informations seront déterminés par les personnes responsables du processus métier qui utilise l'application fiscale concernée, et approuvés par les dirigeants de l'administration fiscale. Ce sont les dirigeants qui sont responsables du fonctionnement des systèmes de l'administration fiscale, c'est pourquoi ils doivent aussi être les arbitres en dernier ressort concernant le mode de conception des contrôles d'accès. Par exemple, il incombe au principal agent fiscal en charge de la gestion du système d'échange automatique de renseignements (EAR) de déterminer les critères d'accès à ce système. Si les contrôles de gestion d'accès sont trop laxistes, la confidentialité peut être compromise, et si les contrôles sont trop stricts, l'efficacité du travail peut être mise à mal. Comme avec de nombreux points de sécurité, il doit exister un juste équilibre entre confidentialité et disponibilité. Les conséquences d'un mauvais équilibre sont des conséquences opérationnelles, et non des conséquences informatiques. La bonne pratique recommande cependant de mettre au point ces critères en collaboration avec le service informatique. Le service informatique maîtrise les éléments techniques associés aux avantages et aux inconvénients de la fourniture d'accès, et sait quels sont les secteurs spécifiques qui exigeront probablement des restrictions, par exemple ceux associés à des privilèges d'accès élevés, comme les rôles d'administrateur. Les administrateurs sont généralement des utilisateurs responsables de l'administration de l'infrastructure informatique au sein du réseau de l'administration fiscale, et ne doivent normalement pas disposer d'un accès Internet, messagerie électronique comprise, dans le cadre de leur rôle d'administrateur.

Phase 1 : définition de la politique et des critères d'accès logique aux informations.

Le tableau 13 résume la définition des critères d'accès logique aux informations.

Phase 2 : processus de fourniture et de suppression de l'accès logique

Fourniture d'un accès logique

Lorsque les critères d'accès logique aux informations ont été déterminés, la phase suivante consiste à fournir un accès aux informations, à savoir accorder aux utilisateurs les droits d'accès prédéterminés pour leur type de rôle (voir l'encadré 18). La fourniture d'un accès logique est pertinente dans certaines circonstances, à savoir :

- En cas de recrutement de nouveau personnel, qui a besoin d'un accès.
- Quand le personnel change de travail ou de rôle (par exemple un agent fiscal qui passe d'une division en charge de la législation à une division de contrôle fiscal, et a par conséquent besoin d'un accès aux informations du contribuable).
- Quand le personnel a de nouvelles fonctions ou responsabilités qui s'ajoutent à son rôle (par exemple un cadre est chargé de la gestion des contribuables tant professionnels que particuliers).
- En cas de demandes d'accès ponctuel pour des rôles particuliers.

Cette liste n'a pas vocation à être exhaustive et d'autres circonstances peuvent probablement être envisagées. Dans tous les cas, dans le cadre de la fourniture d'un accès logique, les administrations fiscales doivent déterminer toutes les circonstances individuelles dans lesquelles il peut être nécessaire de fournir un accès logique à des applications, systèmes ou services informatiques.

14. Les détails portant sur les contrôles appliqués en cas de recours à des services de prestataires externes sont décrits dans la SE 3.2.4.4.

15. Les services publics envisagent de plus en plus l'utilisation de services dits dans le cloud (nuage) au lieu des centres de données contrôlés par le service lui-même.

Encadré 18. **Pourquoi la fourniture d'un accès logique est-elle si importante ?**

La fourniture d'un accès permet aux agents de l'administration fiscale de disposer en temps opportun des droits d'accès légitimes dont ils ont besoin pour réaliser leur travail. Mais s'il n'existe pas de moyen clair pour délivrer ces droits, ces agents peuvent éventuellement créer des processus d'accès ad hoc qui leur permettront de poursuivre leur travail. Il est peu probable que de tels processus improvisés soient alors conformes aux politiques de sécurité et de confidentialité.

Supposons par exemple que l'administration fiscale de la juridiction B ne dispose pas de procédures formelles établies, contrôlées par l'encadrement supérieur, pour fournir un accès basé sur le rôle. Il existe par contre des pratiques manuelles et ad hoc entre les divisions opérationnelles et le service informatique pour accorder des droits d'accès spécifiques. Dans certains cas, si le personnel a besoin d'un certain accès, il envoie un courriel à un collègue du service informatique, qui lui accorde l'accès sans implication de l'encadrement supérieur. Dans d'autres cas, la demande d'accès est d'abord approuvée par un responsable du personnel avant d'être soumise au service informatique, mais elle inclut des droits qui ne sont pas nécessaires pour que le personnel en question réalise les tâches associées à son travail. Dans ces cas-là, aucun historique du processus d'autorisation d'accès n'est conservé. Au cours d'une évaluation des normes de confidentialité, il doit être recommandé à cette juridiction de mettre en place et d'appliquer un processus formel de gestion d'accès, accompagné de procédures formelles de fourniture et de suppression des droits d'accès logique.

Suppression d'un accès logique

Une autre exigence critique est la possibilité de retirer, ou de supprimer des droits d'accès (voir l'exemple dans l'encadré 19). Le piratage des droits d'accès est reconnu comme motif significatif d'atteinte à la sécurité des données. Les administrations fiscales doivent par conséquent prendre les précautions appropriées pour garantir que les seuls accès au système disponibles à un moment donné sont ceux requis par les utilisateurs légitimes. Les situations qui doivent être couvertes par la suppression de la mise à disposition des droits d'accès devraient inclure :

- **Personnel qui quitte son poste**. Les droits d'accès doivent être supprimés au plus tard le dernier jour de travail. Si une personne quitte son poste dans des circonstances spécifiques, par exemple pour mauvaise conduite, les droits d'accès doivent pouvoir être retirés immédiatement.
- **Changement de poste ou de rôle**. Les droits d'accès doivent être supprimés dès la fin de l'ancien poste et de nouveaux droits d'accès doivent être accordés simultanément ou avant.
- **Suppression temporaire**. Si par exemple un membre du personnel est absent pendant de longues périodes, pour ses loisirs ou pour maladie, ou en cas d'enquête pour mauvaise conduite.
- **Accès non utilisé**. Des droits d'accès non utilisés doivent être supprimés.
- **Accès à durée limitée**. Il doit d'une façon générale être possible de mettre à disposition un accès pour une durée limitée, de sorte que le processus supprime automatiquement l'accès après expiration d'une certaine durée (et il doit pouvoir exister un processus associé pour restaurer rapidement l'accès si nécessaire).

Contrôles procéduraux une fois l'accès logique fourni

Lorsque l'accès aux systèmes est fourni, des procédures de vérifications adéquates doivent être entreprises pour garantir que seuls les utilisateurs légitimes disposent des droits d'accès (voir l'exemple dans l'encadré 20). Les procédures de vérifications peuvent comporter les éléments suivants :

- Revues périodiques par du personnel dédié, les superviseurs ou les cadres supérieurs qui ont approuvé la requête d'accès, pour vérifier que :
  - Les personnes présentées comme disposant de droits d'accès sont bien des utilisateurs légitimes.
  - Les personnes auxquelles un accès a été accordé sont bien des utilisateurs actuels (par exemple ils ont toujours ce rôle ou ne sont pas à la retraite).
- Revues périodiques par le service d'audit interne.

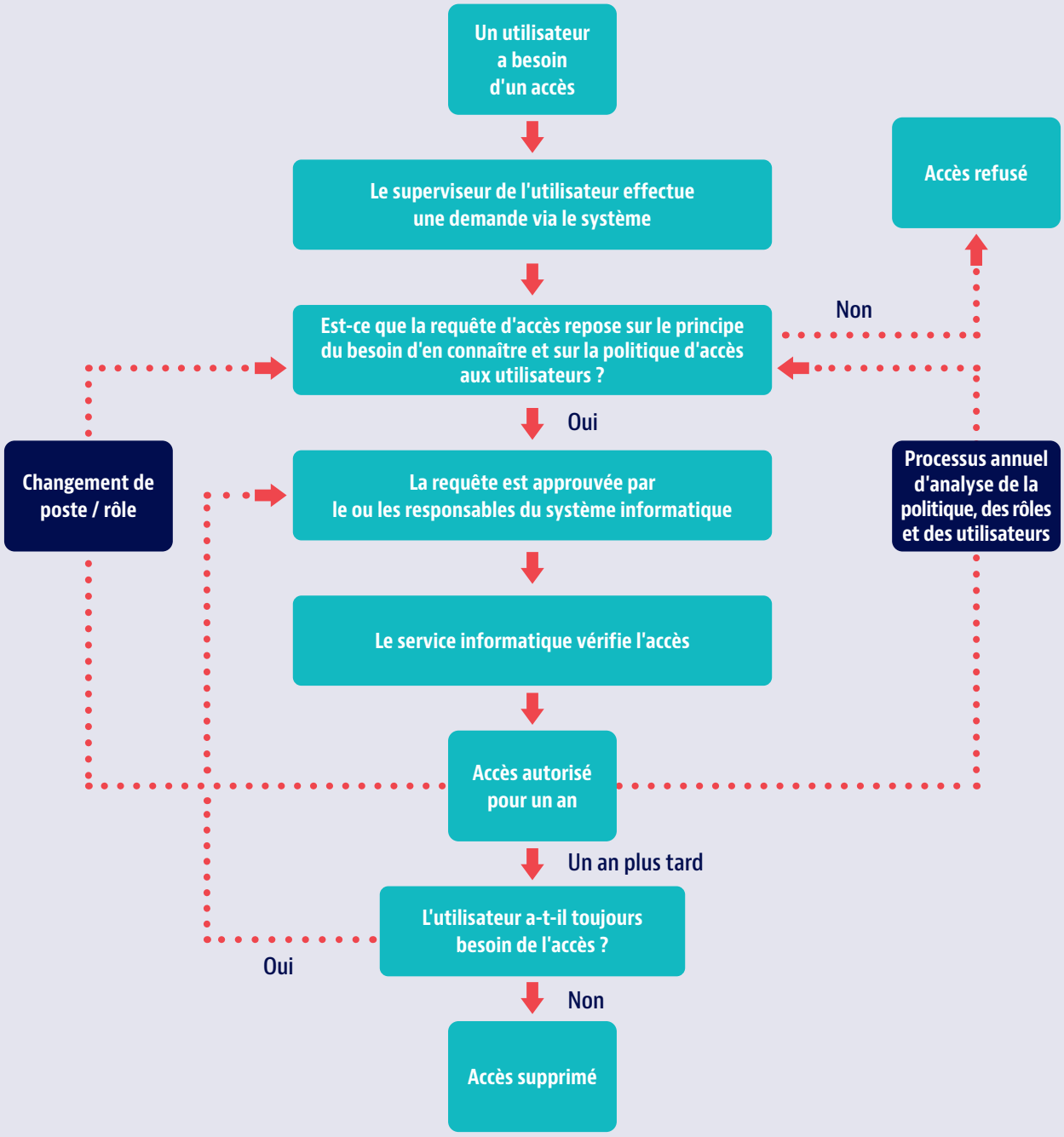
Phase 3 : contrôles applicables lors de l'utilisation des droits d'accès logique

Lorsque les utilisateurs disposent de droits d'accès aux systèmes d'information, ils doivent accéder à ces systèmes ou « se connecter ». Les administrations fiscales doivent garantir que les utilisateurs sont identifiables de façon unique et authentifiés à chaque fois qu'ils accèdent à un système.

Encadré 19. **Exemple de fourniture et de suppression d'un accès logique**

Dans l'administration fiscale de la juridiction C, l'accès des utilisateurs à des systèmes informatiques est prédéfini en fonction de leur rôle (i.e. travail), et repose sur la « Politique de fourniture et de suppression de l'accès utilisateur au sein des systèmes de l'administration fiscale C ». L'autorisation des accès utilisateur exige l'approbation de leur superviseur (au minimum le responsable de l'unité). Les accès doivent ensuite être approuvés par les responsables du système informatique, et seuls des cadres supérieurs peuvent être nommés responsables des systèmes. Une fois l'approbation donnée par les responsables, l'accès est contrôlé puis accordé par le service informatique, dans le cadre d'une vérification technique finale.

La figure suivante montre un exemple de processus de fourniture et de suppression d'accès logique :



Encadré 20. **Exemple de procédures de vérification des accès logiques**

L'administration fiscale de la juridiction A a nommé une équipe de coordinateurs des droits d'accès chargée d'examiner les droits accordés à tous les utilisateurs, employés et sous-traitants. Une fois les droits accordés, les coordinateurs émettent des courriels de confirmation aux superviseurs et cadres supérieurs pour vérifier qu'ils ont bien approuvé les requêtes d'accès. Cette équipe de coordination vérifie également périodiquement que tous les droits d'accès sont valides, et que tous les comptes et accès obsolètes ont été supprimés. Ces vérifications font l'objet d'un rapport, d'une analyse et d'une approbation par le responsable du système d'information, et par le service des ressources humaines. La fréquence des vérifications varie en fonction des classifications du système, mais est d'au moins une fois tous les six mois.

Identification

Tous les utilisateurs de systèmes informatiques doivent disposer d'un ou de plusieurs identifiant(s) unique(s) afin de respecter le principe selon lequel toutes les actions peuvent être associées à des individus identifiables.

Il se peut qu'un utilisateur possède plusieurs identités, par exemple s'il a accès à des fonctions associées à différents niveaux de privilèges, mais ces identités doivent rester uniques pour l'utilisateur concerné. S'il était très exceptionnellement impossible d'utiliser des identifiants uniques, des contrôles compensatoires devraient alors avoir lieu, par exemple la combinaison d'une connexion contrôlée et d'une autorisation de la direction.

Authentification

L'identification doit être renforcée par des exigences d'authentification. La forme standard de l'authentification est un mot de passe, ou une série de caractères connus seulement de la personne qui porte l'identifiant unique. L'encadré 21 souligne quelques bonnes pratiques internationales associées à la gestion du mot de passe et du compte utilisateur.

Il est aussi possible de recourir à d'autres formes d'authentification en plus des mots de passe. Un exemple est l'utilisation des identifiants de poste de travail. Des postes de travail (PC, ordinateurs portables, etc.) délivrés par une administration fiscale avec des identifiants uniques peuvent être utilisés pour obtenir une garantie supplémentaire dans le cadre du processus d'authentification. Il est par exemple possible que l'accès ne soit autorisé que par la saisie de l'identifiant unique de l'ordinateur personnel ou de l'ordinateur portable suite à la saisie du mot de passe de l'utilisateur. Si la réalisation de ce type d'association peut être un moyen de faire davantage confiance au processus d'authentification, elle peut aussi s'avérer restrictive sur le plan opérationnel en liant les utilisateurs à leur propre machine. Ce facteur doit être envisagé avant d'opter pour l'utilisation d'identifiants de poste de travail ou d'autres options d'authentification supplémentaires.

Authentification à facteurs multiples

Il peut exister des situations spéciales dans lesquelles des contrôles par authentification supplémentaire ou authentification à « facteurs multiples » sont nécessaires. Il existe trois types d'authentifiants : quelque chose que vous connaissez, par exemple un mot de passe, quelque chose que vous possédez, par exemple un jeton, et quelque chose que vous êtes, par exemple une empreinte digitale. L'administration fiscale doit utiliser au moins deux des trois authentifiants pour mettre en œuvre une authentification à facteurs multiples.

Les situations qui peuvent exiger une authentification à facteurs multiples peuvent inclure :

- **Données sensibles**. Dans le cas de données sensibles, par exemple des informations échangées, des

Encadré 21. **Bonnes pratiques internationales associées à la gestion du mot de passe et du compte utilisateur**

Gestion du mot de passe. Les pratiques peuvent comporter des contraintes ou normes minimum sur le type et le nombre de mots de passe pouvant être utilisés, des restrictions sur le nombre d'échecs de mot de passe répété, et l'exigence d'un changement régulier des mots de passe. Par exemple, la longueur minimum d'un mot de passe peut être d'au moins 10 caractères alphanumériques, le verrouillage du compte intervenant après 5 échecs de tentative de connexion et le changement du mot de passe devant être réalisé au moins tous les 90 jours.

Gestion de la session. Les pratiques peuvent comporter le verrouillage du poste de travail si ce dernier n'est pas utilisé, et des procédures de sécurité permettant de protéger les informations si les utilisateurs ne verrouillent pas les machines. Par exemple, le poste de travail peut être configuré par défaut pour se déconnecter et demander une réauthentification de l'utilisateur après 10 minutes d'inactivité.

Comptes inactifs. Les pratiques peuvent comporter la surveillance de l'utilisation du compte et la désactivation des comptes s'ils ne sont pas utilisés. Par exemple, les comptes ayant fait l'objet d'aucune connexion pendant au moins 30 jours consécutifs sont désactivés.

contrôles d'authentification plus stricts peuvent être nécessaires. Il peut s'agir d'une authentification standard à deux facteurs (par exemple un mot de passe à niveau de sécurité très élevé, couplé à un jeton de sécurité ou à une mesure biométrique), mais qui pourrait aussi être renforcée par des contrôles d'authentification supplémentaires, par exemple l'association de l'utilisateur à un poste de travail particulier (PC, ordinateur portable, etc.) situé dans une pièce très sécurisée. Quels que soient les contrôles supplémentaires utilisés pour les données sensibles, le niveau de contrôle doit toujours reposer sur une évaluation rigoureuse du risque, et doit équilibrer le besoin de confidentialité avec le besoin de disponibilité.

- **Administrateurs**. Pour les utilisateurs qui travaillent au service informatique et disposent d'un accès d'administrateur privilégié à l'infrastructure et aux systèmes informatiques, souvent appelés « administrateurs » ou « super-utilisateurs », des contrôles d'authentification supplémentaires sont généralement imposés. La bonne pratique internationale pour ce type d'utilisateur consiste à disposer d'une authentification à deux facteurs au moins à laquelle s'ajoute des contrôles supplémentaires, qui peuvent comporter :
  - l'octroi d'un accès privilégié pendant une durée limitée, si bien que le droit d'accès est régulièrement vérifié et que les activités sont analysées avant que l'accès soit à nouveau établi pour une période supplémentaire.
  - l'affectation d'un travail en binôme à des utilisateurs privilégiés, chacun pouvant alors vérifier les actions de l'autre.
  - l'utilisation de programmes commerciaux génériques qui se focalisent spécifiquement sur la gestion de l'accès privilégié.
- **Accès à distance par les utilisateurs**. L'accès aux informations sur le contribuable est étroitement contrôlé, et en-dehors du bureau, l'accès est limité à certaines fonctions et à certains types d'accès au système. En cas d'octroi d'un accès externe à des données sensibles, les risques doivent être efficacement mesurés et atténués. Les principales difficultés ne sont pas techniques, car il existe des moyens très efficaces pour crypter les informations, mais concerne la possibilité de contrôler efficacement l'accès d'un utilisateur à son périphérique (par exemple ordinateur portable ou tablette).

SOUS-EXIGENCE 3.2.4 : LA SÉCURITÉ DU SYSTÈME INFORMATIQUE

La SE 3.2.4 concerne la protection des informations en protégeant l'infrastructure (matérielle et logicielle) dans laquelle les informations sont stockées, et par laquelle elles sont employées et utilisées. La protection des informations elles-mêmes est abordée dans la section suivante, SE 3.2.5.

Dans la SE 3.2.4, on s'attend à ce que les administrations fiscales :

- fassent de la sécurité une partie intégrante de la fourniture de services informatiques afin de soutenir les fonctions opérationnelles, de disposer d'un plan de sécurité pour les applications métiers et d'harmoniser leurs systèmes avec la sécurité (SE 3.2.4.1).
- déploient une gamme appropriée de contrôles de la sécurité informatique (SE 3.2.4.2).
- gèrent efficacement leurs actifs informatiques (SE 3.2.4.3).
- assurent de façon appropriée la fourniture de services par les fournisseurs (SE 3.2.4.4).
- assurent la continuité des services informatiques et leur résilience aux pannes (SE 3.2.4.5).

Le tableau 14 présente les définitions des principaux concepts abordés dans la SE 3.2.4.

Sous-exigence 3.2.4.1. Faire de la sécurité un élément à part entière de la fourniture des services informatiques

Les systèmes informatiques n'existent pas pour rien : ils soutiennent la gestion efficace et l'automatisation des opérations et processus métiers des administrations fiscales. En conséquence, toutes les fonctions informatiques, notamment celles ayant trait à la gestion de la sécurité des informations, doivent être en parfaite harmonie avec les besoins des opérations et processus métiers qu'elles soutiennent. Les administrations fiscales doivent alors décider de la façon dont elles mettent en œuvre la sécurité informatique.

Harmoniser les technologies de l'information et la sécurité avec les fonctions métiers

Les processus de conception des technologies de l'information doivent pour ce faire s'assortir d'un bon niveau d'implication entre le service informatique et les responsables métiers et les utilisateurs. L'administration fiscale doit donc identifier les personnes responsables de la bonne communication entre ces parties prenantes. Sans un tel engagement, les systèmes informatiques peuvent ne pas réaliser ce que les processus métiers exigent d'eux, ce qui pourrait alors générer des problèmes pouvant compromettre la confidentialité et l'intégrité des informations.

L'intégration de la sécurité dans les systèmes d'information et leur harmonisation avec l'activité exigent un service

Tableau 14. **Définitions des principaux concepts**

Concept	Description
Accord de niveau de service	Accord qui définit le niveau de service minimum qu'une entité proposant un service doit respecter.
Contrôle de sécurité informatique	Mesure administrative, technique ou physique mise en œuvre pour atténuer un risque informatique.
Contrôles de base	Ensemble de contrôles de sécurité minimum qu'une administration fiscale applique à certains risques, quelle que soit leur gravité.
Externalisation	Recours à un prestataire externe pour la fourniture de biens et services.
Gestion des actifs	Processus qui garantit que les actifs de l'administration fiscale sont identifiés et suivis depuis leur création ou leur achat jusqu'à leur destruction/cession, de leur mise au rebut ou de leur cession.
Gestion des fournisseurs	Processus basé sur le risque et qui garantit qu'un prestataire externe qui accède aux données ou aux bâtiments de l'administration fiscale ne fait pas peser de risque sur la confidentialité et la sécurité.
Logiciel malveillant	Logiciel à caractère malveillant. Programme créé pour exploiter une vulnérabilité dans un système ciblé afin de l'endommager ou de voler des informations.
Pare-feu	Équipement placé au niveau de points stratégiques d'un réseau (généralement ceux faisant face à un accès externe ou Internet et à des zones internes séparées) et qui autorise ou bloque le trafic en fonction de règles.
Récupération	Fait référence à la restauration des services et des opérations d'exploitation en cas de dysfonctionnement majeur.
Résilience	Fait référence à l'atténuation du risque d'interruption de service et à la garantie d'une tolérance aux pannes dans les services en proposant jusqu'à un certain point une continuité du service.
Test d'intrusion	Le test d'intrusion simule les actions d'un pirate informatique contre l'organisation.

informatique bien organisé. Un service informatique doit :

- Identifier et définir ses fonctions, en établissant clairement des périmètres fonctionnels (e.g. qualité, développement et soutien).
- Identifier les interlocuteurs clés au sein des services métiers.
- Rencontrer régulièrement les parties prenantes des services métiers.

Un organigramme (voir l'exemple de la figure 11) montrant les flux de communication entre le service informatique et d'autres services (notamment la gouvernance, la sécurité et les unités métiers) aidera à identifier les personnes censées établir et communiquer les exigences de sécurité concernant les processus métiers, et les solutions informatiques qui les soutiennent.

De nombreuses variables influencent la façon dont les administrations fiscales structurent leur service informatique, la façon dont celui-ci soutient leurs services métiers et la façon dont les contrôles de sécurité informatique sont mis en œuvre (voir le tableau 15).

Quelle que soit l'organisation informatique retenue, il est impératif de considérer son effet sur la gestion du risque de la sécurité informatique et du risque de sécurité des informations. Cette considération doit mener à la mise en œuvre de structures de gouvernance et de processus appropriés qui garantissent l'intégration entre sécurité informatique et opérations de l'administration fiscale au quotidien. Les administrations fiscales doivent aussi établir des procédures claires qui garantissent la hiérarchisation des priorités concernant les aspects de la sécurité lors de la mise en place de projets informatiques, notamment le corps spécifique ou les personnes responsables.

Mise en œuvre de la sécurité informatique

Après avoir opté pour une structure adaptée qui intègre la sécurité informatique, une administration fiscale doit aussi prendre des décisions sur la mise en œuvre de systèmes informatiques et de la sécurité. Parmi les questions à envisager :

- Est-ce que les services informatiques seront développés en interne, externalisés, ou les deux (en termes d'applications et de systèmes informatiques) (voir l'encadré 22) ?
- Qui décidera, et qui sera responsable des différents services informatiques ?
- Comment sera-t-il garanti que les évaluations de sécurité associées au développement ou à l'acquisition des services et applications informatiques seront correctement réalisées ?
- Comment dans la pratique la sécurité sera-elle intégrée aux technologies de l'information (à savoir dans la conception des environnements informatiques, le développement de nouveaux systèmes, des modifications de systèmes existants, ainsi que dans l'infrastructure sous-jacente) ?

Un processus essentiel pour parvenir à une intégration entre les systèmes informatiques, la sécurité et les systèmes métiers est la gestion du changement, couverte plus en détail dans la SE 3.2.6.5. Les changements de système peuvent générer des risques supplémentaires ou avoir un impact négatif sur l'efficacité des contrôles de sécurité déjà mis en place. La gestion du changement garantit par conséquent que la conception et les changements des systèmes informatiques sont des processus contrôlés, en considérant les exigences de sécurité et en incorporant une évaluation adéquate des impacts.

Sous-exigence 3.2.4.2. Déployer une gamme appropriée de contrôles de la sécurité informatique

Les administrations fiscales doivent déployer des contrôles de la sécurité informatique en se basant sur les différentes données qui permettent de déterminer quels sont les contrôles appliqués et la manière dont ils le sont. Ces données incluent

FIGURE 11. **Exemple d'organigramme présentant les flux de communication entre le service informatique et les autres services**

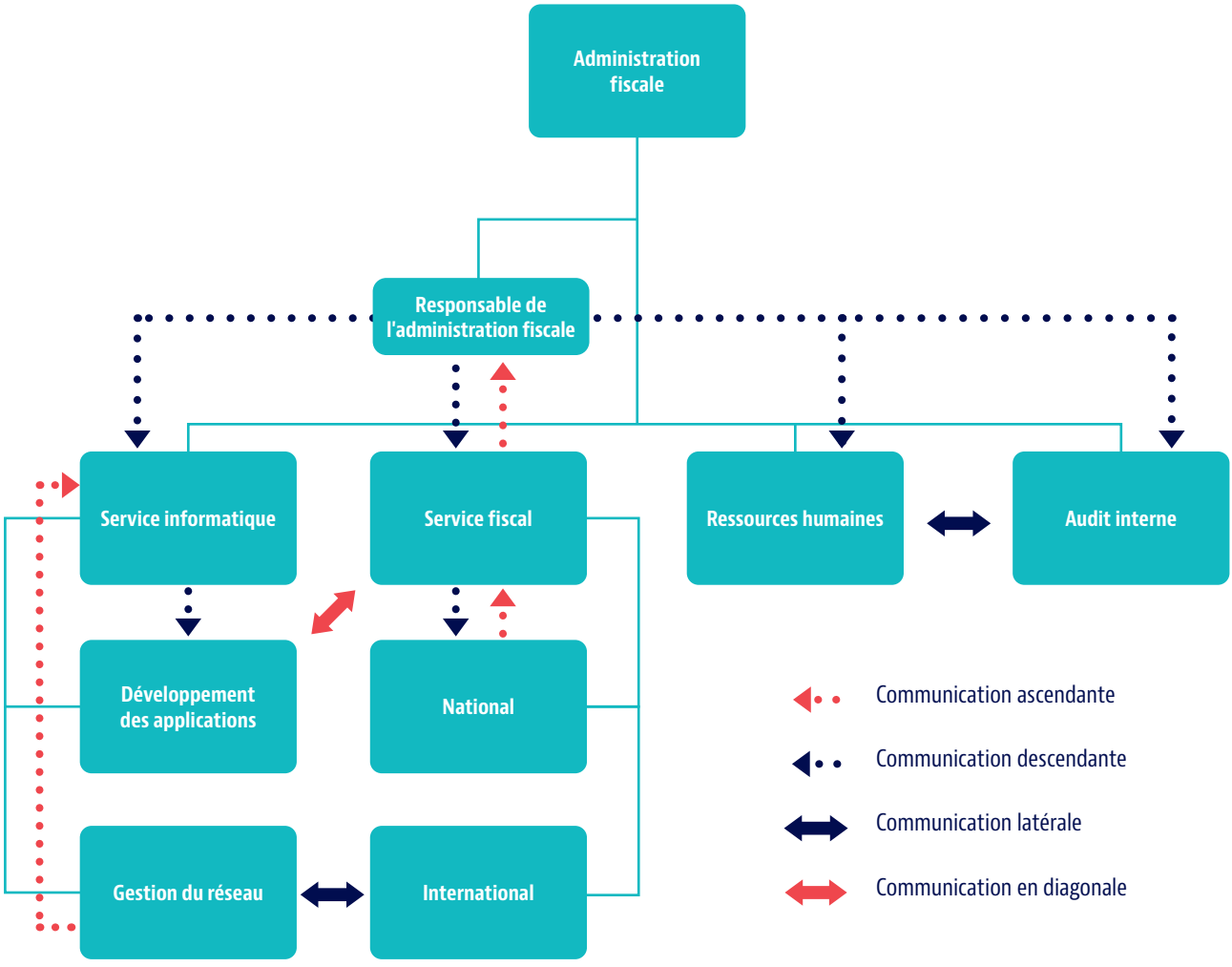


Tableau 15. **Exemples de variables qui influencent la façon dont un service informatique est structuré**

Taille de l'administration fiscale	Externalisation des fonctions informatiques	Approche du cycle de vie	Harmonisation du système informatique
Dans de grandes administrations ou des administrations plus complexes, le service informatique peut inclure de nombreuses activités différentes, notamment l'architecture informatique, la conception, le développement, la gestion de projet, la gestion des versions, les opérations, la gestion du service et la gestion de la sécurité informatique. Ces activités peuvent être structurées en tant que sous-services. Dans de plus petites administrations cependant, un service unique prendra en charge toutes les activités. Quelques activités ou toutes les activités, ainsi que les décisions techniques associées, peuvent être externalisées, par exemple par l'acquisition de solutions informatiques dans le commerce.	Le service informatique lui-même peut être exploité hors de l'administration fiscale. Par exemple, un service informatique séparée au sein du Ministère des finances et qui propose des services informatiques pour tous les services de ce ministère. Dans d'autres cas, certaines ou toutes les fonctions du service informatique peuvent être externalisées vers des entreprises privées, dont la fourniture de services de bureautique.	Les activités qui soutiennent la fourniture de services informatiques peuvent être structurées en termes de cycle de vie informatique, avec des équipes dédiées pour chaque partie du cycle de vie (par exemple conception, développement, publication et opérations). La structure peut établir la façon dont les différentes équipes du service informatique collaborent entre elles, ainsi qu'avec les services métiers et les utilisateurs du système d'information.	L'intégration de la sécurité des informations dans la fourniture des services informatiques peut être simplifiée si les systèmes informatiques sont harmonisés de sorte que seulement quelques solutions, mais les mêmes sur toute l'infrastructure, sont utilisées. Les administrations fiscales qui disposent d'un degré d'harmonisation élevé peuvent constater que cela permet de réduire les coûts et de gérer les problèmes de sécurité. L'harmonisation peut aussi s'appliquer à des appareils et des équipements mobiles connectés à l'administration fiscale depuis l'extérieur (par exemple télétravail et équipement mobile du personnel accédant au réseau de l'administration fiscale).

les informations obtenues via la gestion des incidents et des problèmes (SE 3.2.6.6), la gestion des vulnérabilités (SE 3.2.6.4), et, le plus important, la gestion du risque (SE 3.2.1.4).

En fonction de la structuration de la fonction informatique, l'approche de déploiement des contrôles peut être plus ou moins formalisée ou documentée. Quelle que soit l'approche retenue, la façon dont les différentes données contribuent aux décisions d'application des contrôles informatiques doit être évidente au sein du service informatique et au sein de l'administration fiscale. Cela offre une traçabilité pour les membres de l'équipe informatique en charge de la gestion des contrôles. Ces personnes doivent aussi clairement comprendre les impacts de tous les changements du système pour pouvoir agir en conséquence et garantir que les contrôles existants continuent à fonctionner convenablement.

Comme le montre la figure 12, les contrôles de la sécurité informatique (et les contrôles de sécurité d'une façon générale) incluent des :

- **Contrôles de base** : contrôles minimum appliqués suite à l'identification initiale par l'administration fiscale de risques spécifiques, quelle que soit leur gravité.

Encadré 22. **Avantages et inconvénients éventuels : le développement de services informatiques internes ou externalisés**

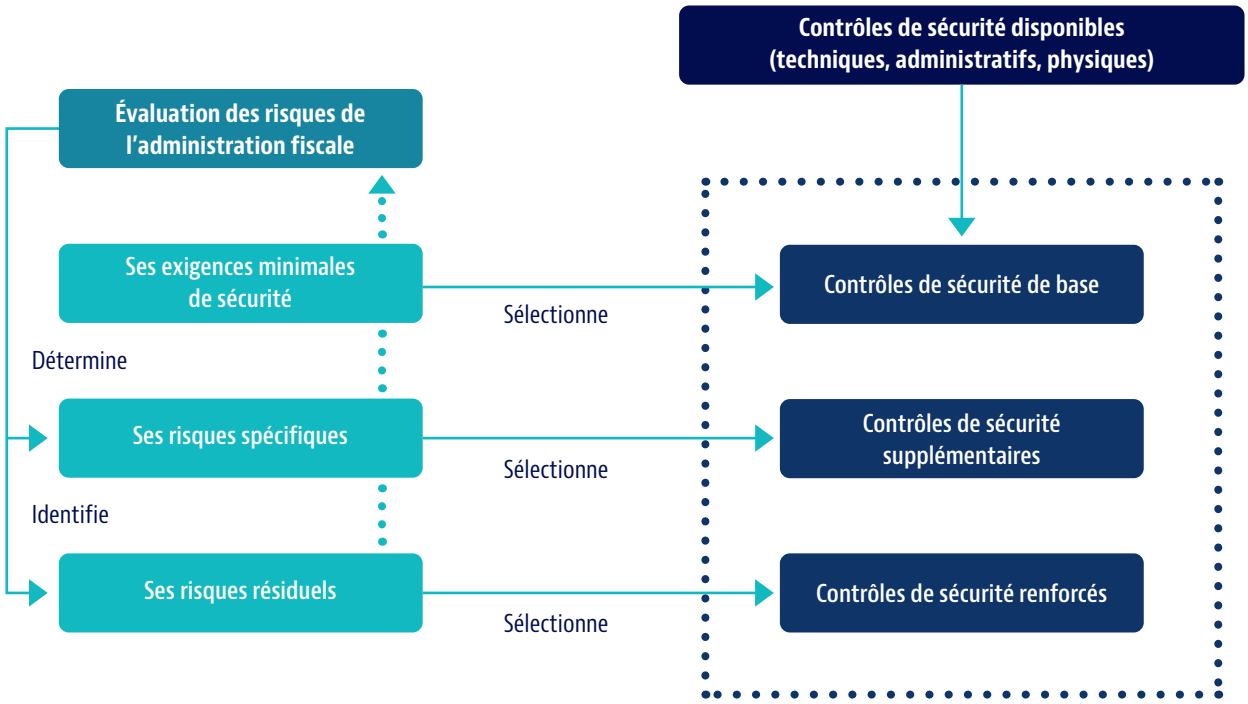
Développement interne

On peut citer parmi les avantages un meilleur contrôle interne des services informatiques, de meilleures relations de confiance et la confidentialité. Les inconvénients peuvent comporter le développement d'un savoir-faire interne, des programmes de formation intensifs ou des dépenses plus élevées.

Développement externalisé

Les avantages peuvent inclure une meilleure aptitude des services informatiques à se concentrer sur les principales activités de l'administration fiscale, l'accès aux nouvelles technologies, une réduction des dépenses courantes et une plus grande flexibilité. Les inconvénients peuvent être la nécessité de contrôler les prestataires tiers et leurs employés, un éventuel désaccord culturel, par exemple entre le prestataire et le personnel en interne, ou des problèmes de confidentialité.

FIGURE 12. **Types de contrôles de sécurité**



- **Contrôles supplémentaires** : mesures supplémentaires déployées pour atténuer les risques identifiés, en fonction du niveau de gravité des risques évalués. Comme cela a été traité dans la SE 3.2.1.4, en identifiant les risques, les administrations fiscales devront décider, pour chaque risque, de la façon dont elles souhaitent les gérer, et notamment quels contrôles appliquer. Les contrôles sont par conséquent appliqués en fonction de l'appétit de l'administration fiscale pour le risque.

- **Contrôles renforcés** : contrôles qui aident à gérer les menaces avancées, par exemple des technologies permettant de détecter et de prévenir une exfiltration de données.

Les administrations fiscales sont censées évaluer l'efficacité des contrôles de sécurité appliqués, de préférence à l'aide de mesures, et disposent d'un processus formel pour ces évaluations.

Chaque type de contrôle peut être par nature administratif (par exemple une politique ou un processus), physique (par exemple des caméras de surveillance) ou technique (par exemple un pare-feu ou un logiciel). Une combinaison de ces différents contrôles peut être nécessaire pour atténuer un risque unique (voir les exemples dans le tableau 16). Les différents types de contrôles sont abordés tour à tour.

Contrôles de base

Des contrôles de base proportionnels seront choisis en fonction du degré de sensibilité des informations hébergées sur un système et du niveau de confidentialité requis. L'encadré 23 comporte des exemples de contrôles de base courants basés sur les risques de sécurité informatique.

Tableau 16. **Exemples de contrôles de base, supplémentaires et renforcés**

Contrôles de base	Antivirus, journalisation & surveillance	Télévision en circuit fermé, système d'éclairage	Politique du mot de passe
Contrôles supplémentaires	Authentification à facteurs multiples	Barrières, sas de sécurité	Politique de sensibilisation
Contrôles renforcés	Systèmes de prévention contre la perte des données, Centre d'opérations de sécurité interne permanent	Data center de niveau Tier 1, Site chaud avec réplication active/active	Politique « Apportez Votre Équipement personnel de Communication » (AVEC), politique de chiffrement renforcé pour informations hautement sensibles

Encadré 23. Exemples de contrôles de base

Antivirus et pare-feu

Les antivirus et les pare-feu sont des protections obligatoires. Si la nécessité de ces deux contrôles est considérée comme allant de soi pour la plupart des organisations, de nombreuses cyber-attaques tirent parti de la mauvaise configuration et de la gestion incorrecte de ces équipements et logiciels.

Quand l'antivirus protège les postes de travail et les serveurs contre des menaces connues, les pare-feu aident à isoler différentes parties du réseau et à donner l'alerte en cas de détection d'un trafic inadéquat. Le maintien à jour d'un antivirus et la bonne configuration des règles du pare-feu sont des exigences indispensables.

Gestion des correctifs et des mises à jour

La correction des applications et systèmes d'exploitation est un aspect critique de la protection d'une infrastructure informatique. Il est fréquent que les cyber-menaces, comme le piratage informatique, impliquent l'utilisation d'un code d'exploitation publié qui cible une vulnérabilité pour laquelle un correctif existe déjà depuis longtemps. Les pirates informatiques savent pertinemment que si les systèmes orientés vers l'extérieur sont régulièrement corrigés, les systèmes internes, pour des raisons organisationnelles, peuvent de pas être corrigés aussi rigoureusement.

Les correctifs devraient être installés par défaut. Même s'ils sont rares, des problèmes peuvent survenir lors de l'installation de correctifs. En cas de problème, il est toujours possible de revenir à une configuration antérieure du système grâce aux points de restauration et ce, jusqu'à ce que le problème soit résolu par une nouvelle version du correctif.

Les administrations fiscales sont encouragées à élaborer et mettre en place une politique de gestion des correctifs en tant que contrôle qui garantit que les correctifs et les mises à jour de tous les systèmes d'exploitation et progiciels sont déployés sur un intervalle temporel défini (généralement en quelques jours). Un processus critique de déploiement de correctif doit aussi être en place pour assurer que les correctifs critiques sont bien déployés dans les délais définis (généralement quelques heures). Les administrations fiscales doivent aussi définir ce qu'est un correctif classé comme critique.

Renforcement de la sécurité des systèmes

La configuration des systèmes pour les rendre sécurisés par défaut est une protection obligatoire contre les cyber-menaces. Les administrations fiscales doivent être capables d'empêcher les pirates informatiques d'exécuter des codes malveillants dans leur environnement informatique, et il est important de savoir ce qui se passe au sein de cet environnement pour s'assurer que les opérations sont appropriées.

Pour cela, les administrations fiscales doivent configurer des systèmes d'exploitation standard tel que recommandé par les vendeurs. Concernant l'utilisation des applications, la mise en place d'un outil de liste blanche peut être mis en place afin de restreindre l'exécution des seuls exécutables et scripts autorisés. Les macros doivent en outre être restreintes en ce qu'une approbation est nécessaire pour leur exécution, ou qu'elles ne peuvent s'exécuter que si elles sont signées. Enfin, il est important de désactiver les applications potentiellement dangereuses, comme les extensions de navigateur, les publicités sur Internet et les applets.

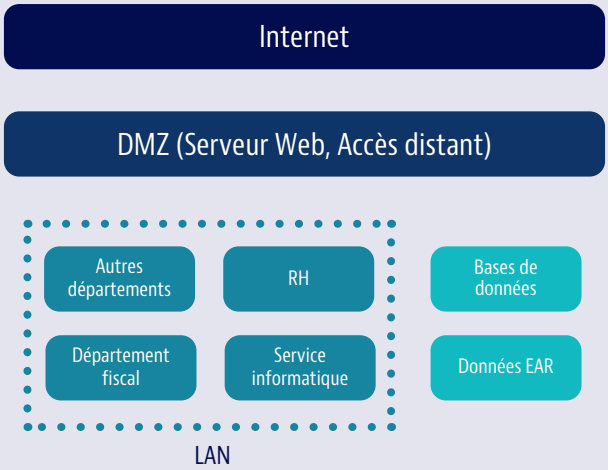
Segmentation du réseau

La mise en œuvre de la segmentation du réseau consiste à placer des murs entre les systèmes critiques et les réseaux internes et externes. Un « segment plat », sans mur ou avec des murs limités, peut créer un environnement qui n'exige qu'une seule intrusion sur le réseau pour qu'un pirate informatique obtienne un large accès. Un réseau plat permet au pirate informatique de pivoter entre hôtes et services avec une obstruction minime et un faible risque de détection. Un poste de travail mis en péril ne devrait pas pouvoir se connecter à des bases de données importantes.

Un moyen courant pour concevoir le réseau consiste à diviser le réseau en réseaux plus petits, tel qu'illustré sur la figure suivant, en ayant normalement des zones dédiées :

- une zone dédiée pour les systèmes orientés vers l'extérieur, généralement appelés DMZ (zone démilitarisée) ;
- une zone administrateur dédiée ;
- une zone pour les bases de données sensibles et les applications critiques, telles que les bases de données et les applications d'EAR ;
- une zone pour le réseau interne, généralement appelé LAN (Local Area Network).

Les réseaux internes peuvent être sous-segmentés par activité, par exemple ressources humaines, finances, informatique, contrôle fiscal, etc. Vous trouverez ci-après un exemple de segmentation du réseau.



Gestion des accès et des droits de l'administrateur

Les pirates informatiques ciblent les comptes d'utilisateurs privilégiés et d'administrateur pour réaliser leurs activités, par exemple extraire des données des bases de données et exfiltrer des données, car ces comptes sont normalement capables de détourner toutes les restrictions. Il est donc important de restreindre les droits et les accès de l'administrateur par une gestion appropriée.

Il est fortement recommandé de mettre en œuvre une authentification à plusieurs facteurs (abordée plus en détail dans la SE 3.2.3 sur la gestion d'accès) pour les comptes administrateur des administrations fiscales, de désactiver ou de renommer tous les comptes système intégrés et de mettre en place une politique qui garantit dès que possible la restriction de l'accès des administrateurs.

De plus, les comptes des utilisateurs privilégiés ne doivent pas être autorisés à lire des courriels et accéder à l'Internet d'une façon générale, notamment pour obtenir et télécharger des fichiers via des services en ligne. De même, des « serveurs de rebond » peuvent être utilisés comme rebond pour que les administrateurs accèdent aux systèmes critiques. Un serveur de rebond se compose d'un serveur dédié sécurisé situé dans une zone DMZ, et qui n'autorise que quelques protocoles de communication pour permettre aux administrateurs de s'authentifier en utilisant une authentification forte, puis d'accéder à des ressources spécifiques situées sur le réseau interne.

Les contrôles de base ne sont pas statiques : des contrôles, qui n'étaient pas encore très courants il y a peu, peuvent être aujourd'hui considérés comme des contrôles de base pour de nombreuses administrations fiscales. C'est par exemple le cas des solutions de gestion des informations et événements de sécurité (SIEM).

Contrôles supplémentaires

Une administration fiscale peut décider d'appliquer des contrôles supplémentaires pour atténuer les risques identifiés, sur la base de son évaluation de l'importance relative ou de la gravité de ces risques et de ses décisions de traitement du risque.

Encadré 24. **Exemple de contrôle supplémentaire : le test d'intrusion des interfaces externes**

Le test d'intrusion est un élément essentiel pour comprendre s'il existe des faiblesses dans l'environnement informatique. Aussi connu sous le nom de « piratage éthique », il simule les actions d'un pirate informatique contre l'organisation. Son objectif principal consiste à déceler les vulnérabilités exploitables avant toute autre personne, de façon à les corriger et les supprimer en conséquence. Lors d'un test d'intrusion, les risques sont normalement identifiés et un score est attribué en fonction d'une matrice de risque. Les scores sont généralement les suivants :

- Faible
- Moyen/modéré
- Important/sérieux
- Élevé/grave/critique/catastrophique

Les points d'intégration et services multiples qui existent dans les environnements informatiques modernes signifient que l'absence de tests d'intrusion des interfaces externes et internes pourrait mettre à mal la sécurité des données, notamment les informations échangées (il peut exister des risques sur les informations échangées s'il existe un certain niveau d'intégration avec des environnements système essentiels de l'administration fiscale).

Si un test interne est très important, il est particulièrement important de tester les interfaces externes, car les pirates informatiques du monde entier peuvent les cibler directement. Une interface externe est simplement tout service qui réagit à une entrée externe. Il peut s'agir d'un formulaire en ligne sur la TVA, d'un portail du contribuable ou d'un serveur avec protocole de transfert de fichier. Le test d'intrusion est davantage détaillé dans la SE 3.2.6.4 sur la gestion des vulnérabilités.

Les contrôles informatiques supplémentaires complètent les contrôles de base, et incluent de façon similaire des contrôles administratifs, des contrôles techniques et des contrôles physiques qui de concert visent à atteindre l'objectif final de confidentialité. Cette approche est décrite à la section « Défense en profondeur ». L'encadré 24 donne un exemple d'un type courant de contrôle supplémentaire.

Contrôles renforcés

Les contrôles renforcés peuvent aussi être utilisés pour protéger l'infrastructure informatique contre les menaces avancées, telles que des méthodes sophistiquées d'exfiltration des données. Les administrations fiscales déploient des contrôles renforcés en fonction de la maturité de leurs processus et contrôles de sécurité existants, et du niveau global de risque en rapport avec les atteintes potentielles à la sécurité des données (en relation avec les données fiscales nationales, et les informations échangées).

Encadré 25. **Exemple de contrôle renforcé : la prévention de fuite de données**

La prévention de fuite de données (Data Loss Prévention - DLP) détecte les éventuelles atteintes à la sécurité des données, dont les transmissions complexes d'exfiltration des données, et les évite en surveillant, détectant et bloquant les données sensibles quand elles sont en cours d'utilisation (actions sur les terminaux), en déplacement (trafic du réseau) et au repos (stockage des données). La prévention des fuites de données détecte les données sensibles qui quittent et transitent au sein de l'administration fiscale quand elles n'ont pas à le faire, et entreprend des actions sur ces données, par exemple le blocage, l'autorisation ou l'émission d'alertes.

Une solution de prévention des fuites de données est une combinaison de deux outils DLP :

- La prévention des fuites de données sur les terminaux, qui se compose d'un logiciel installé sur tous les ordinateurs portables et postes de travail et qui analyse les données stockées sur l'équipement, et empêche l'utilisateur de réaliser des actions interdites, par exemple de copier un fichier sur un périphérique de stockage externe.
- La prévention des fuites de données sur le réseau, qui évite les fuites de données lorsque celles-ci transitent sur le réseau d'une administration fiscale, par exemple lorsqu'un courriel est envoyé à un destinataire externe.

Pour qu'une solution DLP donne les meilleurs résultats, il est essentiel de marquer correctement toutes les données (en fonction de la classification des données par l'administration fiscale : voir la SE 3.2.5.1 sur la protection des informations). Pour être efficaces et correctement configurés, les systèmes DLP exigent des techniciens hautement qualifiés.

Voir l'encadré 25 pour un exemple de contrôle renforcé.

Évaluer l'efficacité des contrôles de sécurité

Les administrations fiscales doivent prendre des mesures pour évaluer l'efficacité des contrôles de sécurité (de base, supplémentaires et renforcés), car si ces contrôles ont été mis en œuvre, ils peuvent ne pas fonctionner parfaitement dans la pratique (par exemple un programme de sensibilisation est mis en place, mais après analyse, l'organisation apprend qu'il n'a été suivi que par 5 % de la population ciblée). Les outils utiles pour mesurer l'efficacité incluent les indicateurs clés de performance, les tests d'intrusion, les évaluations des vulnérabilités et les tests sur des jeux de données (voir la SE 3.2.6.4 sur la gestion des vulnérabilités pour obtenir davantage de détails).

Sous-exigence 3.2.4.3. Gestion des actifs et services informatiques, et gestion du niveau de service

La SE 3.2.4.3 concerne la gestion opérationnelle des actifs informatiques des administrations fiscales. La gestion des actifs est pertinente pour la confidentialité des informations, car les actifs peuvent contenir des informations, et des informations sur les actifs sont nécessaires pour soutenir les enquêtes sur les incidents de sécurité.

Chaque actif informatique doit être identifié et géré, car il représente une menace potentielle pour la sécurité, et par conséquent un risque.

La gestion des actifs peut être divisée en deux fonctions, généralement réalisées par des secteurs séparés d'un service informatique :

- **Gestion des actifs et services informatiques**, traitée habituellement par les responsables des actifs informatiques dédiés.
- **Gestion du niveau de service**, ou gestion des relations qui sous-tendent la fourniture des actifs et services informatiques à leurs utilisateurs de l'administration fiscale. Celle-ci est généralement liée aux responsables des fonctions métiers.

Tableau 17. **Cycle de vie de la gestion des actifs**

Composant de la gestion des actifs	Description du composant	Exemples d'éléments à inclure	Exemples de détails à enregistrer
Inventaire des actifs	Liste qui détaille chaque actif informatique détenu par l'administration fiscale, avec sa description et un identifiant unique.	Postes de travail, disques durs, ordinateurs portables, écrans, appareils mobiles, routeurs, pare-feu, casques, licences logicielles	Identifiant - description - numéro de série - classification - état « utilisé » ou « disponible pour être utilisé »
Propriétaire des actifs	Spécification du propriétaire de l'actif	Entité, personne, service, tiers	Propriétaire - fonction - dernière révision
Gestion de la configuration des actifs	Garantit que les systèmes sont correctement configurés et prêts à l'emploi	Garantie, gestion des licences logicielles, gestion des correctifs, déploiement, vérification des codes	Version du progiciel - dernière mise à jour - propriétaires précédents - état « configuration en cours » - état du correctif, état de la garantie, état de la maintenance
Gestion de la capacité des actifs	Fournit un plan permettant de gérer la capacité des technologies de l'information, de garantir qu'il y a suffisamment d'actifs à utiliser et qu'ils sont aptes à évoluer	Capacité du centre de données, équipement disponible pour les nouveaux employés, capacité des bandes de sauvegarde, disponibilité des informations	Capacité matérielle (%) - dernière mise à niveau du matériel - stockage restant - consommation électrique - charge du serveur - bande passante
Destruction/cession des actifs	Comment l'administration fiscale gère la destruction/cession actifs	Renouvellement des ordinateurs portables, des imprimantes, destruction/cession des équipements, politique de nettoyage	Mise à jour de l'état en « non utilisé », « nettoyer », « vendu »

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Gestion des actifs et services informatiques

Le tableau 17 décrit les composants de la gestion des actifs qu'une administration fiscale devrait suivre. Les composants peuvent aussi être considérés comme les différentes phases de cycle de vie de la gestion des actifs.

Dans l'idéal, tous les actifs doivent être gérés selon une norme similaire, sans tenir compte du nombre d'actifs détenus, afin de garantir des mesures correctes, des données cohérentes, ainsi qu'une surveillance et un audit plus simples. La gestion des actifs est généralement soutenue par des outils informatiques (voir l'encadré 26).

Certaines variables cependant peuvent influencer la façon dont les administrations fiscales gèrent les actifs :

- **Les actifs peuvent être gérés selon différents niveaux de détail**. Un ordinateur de bureau par exemple peut être enregistré en tant qu'actif unique, ou être documenté jusqu'au niveau du composant. Si les deux approches sont considérées comme valides, l'approche doit être suffisamment détaillée pour permettre d'identifier les attributs pertinents de l'actif. Ainsi, il ne suffit pas d'enregistrer uniquement le nombre d'ordinateurs détenus par un bureau particulier sans aucune information sur les attributs des ordinateurs (par exemple numéro de série, modèle, marque, informations techniques).

- **La gestion des actifs informatiques peut être externalisée**. Si une administration fiscale externalise la gestion des actifs informatiques, elle doit évaluer et garantir elle-même que le prestataire effectue le travail correctement et efficacement. Si l'externalisation allège la tâche de l'administration fiscale, elle peut exiger un effort plus important pour surveiller le prestataire.

Un certain nombre de processus de l'administration fiscale peuvent se baser sur les informations sur les actifs, et les administrations fiscales doivent être en mesure de soutenir ces processus et d'apporter des changements aux services sans mettre en péril la confidentialité. Par exemple, si l'apport de modifications à un logiciel affecte des actifs tels que les navigateurs, l'administration fiscale peut avoir besoin de vérifier si les modifications ont été testées sur tous les types et toutes les versions des navigateurs utilisés au sein de l'administration. Les administrations fiscales doivent être en mesure d'identifier les versions logicielles utilisées, les appareils sur lesquels elles le sont, et que toutes sont des versions en cours qui vont prendre en charge les mises à jour de sécurité.

Gestion du niveau de service

La gestion du niveau de service consiste à englober les relations entre les divisions fiscales opérationnelles qui commandent des services informatiques et les entités en charge de la fourniture des services informatiques (à savoir le service informatique des administrations fiscales, ou un prestataire externe).

Ces relations sont essentiellement exprimées par le biais d'un accord de niveau de service. Les accords de niveau de service sont un accord entre ces parties sur les seules exigences non fonctionnelles du service informatique. Les exigences fonctionnelles concernent les objectifs des divisions métiers (à savoir ce qu'une application ou un service informatique doit faire) alors que les exigences non fonctionnelles reposent sur le service (à savoir la disponibilité minimum acceptable de service).

Les accords de niveau de service font partie des accords de fournisseurs, que le fournisseur soit le service informatique (ou une sous-fonction de celui-ci) lui-même, ou que le service soit externalisé par le service informatique.

La gestion du niveau de service, en plus des accords de niveau de service, couvre :

- **Les accords sur le niveau opérationnel**, réalisés entre des entités internes d'une administration fiscale lorsque le service informatique dépend d'un autre service pour fonctionner pleinement.

- **Les contrats de sous-traitance**, qui sont identiques à des accords de niveau opérationnels mais pour lesquels un fournisseur informatique se base aussi sur des services fournis par un sous-traitant.

Encadré 26. **Les outils informatiques de gestion des actifs**

Dans l'idéal, la gestion des actifs sera réalisée en utilisant des outils tels qu'une base de données de gestion de la configuration (Configuration Management DataBase - CMDB), qui enregistre l'ensemble des différents actifs, y compris PC, ordinateurs portables, périphériques, logiciels commerciaux, etc., et est mise à jour de façon automatisée. Cet outil présente toutes les informations pertinentes sur le cycle de vie de chaque actif (par exemple date d'achat, version, emplacement et propriétaire actuels, date de fin de vie, etc.). Ces informations sont très utiles dans un contexte de sécurité car en cas d'incident ayant trait à la sécurité, une CMDB à jour permettra à la personne qui enquête sur l'incident de se plonger rapidement au cœur du problème. Un tel outil permet aussi d'atténuer les risques associés à la gestion des modifications, et permet au service informatique d'offrir aux utilisateurs un meilleur service.

Accords de niveau de service

Les accords de niveau de service des administrations fiscales garantissent que les services informatiques répondent aux exigences de toutes les parties intéressées au sein de l'administration, y compris les directeurs et autres responsables des processus fiscaux soutenus par les services informatiques, les employés qui utilisent les systèmes et l'OSSI.

Les exigences non fonctionnelles des accords de niveau de service contiennent généralement :

- **Un ensemble d'exigences de sécurité de base**, telles que la gestion de l'accès du fournisseur (interne ou externe) aux systèmes de l'administration fiscale.
- **Des exigences supplémentaires spécifiques** qui peuvent avoir été identifiées pour un système particulier, et qui complètent les exigences de base. Il peut s'agir de spécifier la façon selon laquelle le fournisseur doit traiter des types de données spécifiques, par exemple les informations échangées ou les données financières.

Certaines exigences non fonctionnelles seront intégrées à la conception des services informatiques et de l'environnement de l'infrastructure (par ex. pare-feu, renforcement de serveur ou antivirus) quand d'autres ne seront pas intégrées et devront être surveillées par le service informatique (par exemple l'accès aux données). Dans les deux cas, les exigences de sécurité devront être gérées efficacement pour obtenir de bons résultats de sécurité. Ces deux types doivent être abordés dans les accords de niveaux de service.

Les exigences non fonctionnelles des accords de niveau de service, qui ne concernent pas directement la sécurité, sont :

- une description du service, notamment les résultats et livrables principaux
- la disponibilité du service et d'autres objectifs de performance
- les dispositions associées à la maintenance
- les règles associées aux arrêts planifiés, notamment les périodes pendant lesquelles des arrêts doivent être évités
- les durées de récupération
- les règles associées à un changement de système
- les dispositions liées au rapport d'incidents
- les points de contact.

Les principaux points à considérer pour la mise en œuvre d'un accord de niveau de service sont :

- Les dispositions globales, en particulier s'il existe un unique ensemble d'exigences standard, ou des exigences séparées supplémentaires pour chaque système.
- La nature des accords, à savoir s'il s'agira d'un accord de niveau de service direct entre les services fiscaux opérationnels et le service informatique interne, ou quelque chose de plus complexe impliquant des prestataires externes.
- Les dispositions relatives aux rapports, écrits et via des réunions régulières des parties prenantes (les deux devant être stipulés dans l'accord de niveau de service).
- S'il existe ou non un ensemble normalisé d'exigences de sécurité, par exemple deux ou plusieurs ensembles de normes pour différents types de processus, ou des dispositions différentes pour chaque système différent.
- Si les systèmes qui gèrent les informations échangées, par exemple sous la norme d'EAR, ont leurs propres accords de niveau de service. Dans la négative, s'il existe un processus dans le cadre d'un accord de niveau de service global qui permet à l'équipe chargée de l'échange de renseignements de valider que tous les contrôles de sécurité pertinents sont en place et fonctionnent, en coopération avec le fournisseur concerné (interne ou externe) des services informatiques.
- Les actions nécessaires dans des circonstances exceptionnelles, en particulier le signalement des incidents. En particulier, si le service informatique identifie un incident de sécurité, celui-ci doit être signalé de la façon prescrite.
- La nomination de points de contact tant au sein du département informatique que dans l'ensemble de l'administration fiscale.

L'encadré 27 montre un modèle d'accord de niveaux de service de base.

Un point important à considérer est l'utilisation d'un accord de niveau de service unique ou de plusieurs accords de niveau de service. Certaines administrations peuvent prendre une décision centrale selon laquelle toutes les applications informatiques doivent être créées sur une plateforme d'infrastructure unique et avec un accord de niveau de service unique, quand d'autres peuvent opter pour des accords de niveau de service séparés pour chacune des différentes applications de gestion fiscale.

Dans la pratique, les administrations fiscales utilisent un mélange des deux. Une administration fiscale dispose généralement de différentes plateformes préexistantes. Gérer les technologies de l'information peut s'avérer complexe dans ces circonstances, si bien que les administrations fiscales peuvent envisager la normalisation des services informatiques sur une plateforme unique moderne. Les nouvelles applications peuvent alors être générées sur cette plateforme, et les applications plus anciennes vont migrer si et dès que les circonstances le permettent. Un nouveau paradigme informatique se fait généralement jour après quelques années, et le processus recommence.

Plusieurs facteurs différents devront être envisagés pour décider de la structure de l'accord de niveau de service la plus appropriée pour l'administration fiscale.

Dans tous les cas, des accords de niveau de service multi-niveaux sont le plus souvent utilisés, et ils sont composés de différents niveaux :

Niveau organisationnel

Ce niveau traite de toutes les questions générales pertinentes pour l'organisation, et qui sont identiques sur l'ensemble de l'organisation. Par exemple, dans les conditions de sécurité d'un accord de niveau de service au niveau de l'organisation, il peut être demandé à chaque employé de créer un mot de passe de 8 caractères, qui doit être modifié tous les mois ; ou il peut être demandé à chaque employé d'avoir une carte d'accès avec photographie imprimée.

Niveau du client

Ce niveau traite des questions spécifiques à un utilisateur ou un « client » du service informatique. Par exemple, les exigences de sécurité d'un ou de plusieurs services au sein de l'organisation peuvent être supérieures à celles d'autres services, par exemple une division financière ou une division d'échange de renseignements qui exige des mesures de sécurité renforcées du fait de son rôle associé à la gestion d'informations et de ressources particulièrement sensibles.

Niveau du service

Ce niveau traite des questions pertinentes pour un service spécifique (en relation avec l'utilisateur ou le client). Il s'applique à tous les utilisateurs ou clients qui bénéficient du même service - par exemple contracter des services d'assistance informatique pour chaque personne qui utilise un prestataire de téléphonie IP particulier.

L'utilisation d'une telle structure multi-niveaux pour l'accord de niveau de service d'une grande organisation peut réduire la duplication des efforts tout en fournissant une personnalisation pour différents utilisateurs et services au sein de l'organisation.

Le tableau 18 donne un exemple des dispositions d'assistance à l'utilisateur ou au client qu'un prestataire de service peut garantir dans le cadre d'un accord de niveau de service, en fonction de la gravité ou de l'urgence d'un problème. Plus la gravité ou l'urgence est importante, plus le temps de réponse est court. Dans cet exemple, l'assurance est fournie pour 90 % des incidents ou problèmes rapportés, ce qui signifie qu'à la fin de la période de service convenue pertinente, il conviendra d'effectuer un calcul des problèmes ayant généré une réponse. Si le score de résolution dans les temps est inférieur à 90 %, des pénalités financières ou une compensation pourront être imposées au fournisseur. Par conséquent, le prestataire de service comme le bénéficiaire des services doivent surveiller et comparer les chiffres.

Encadré 27. **Modèle de base de ce que l'on doit attendre d'un document d'accord de niveau de service**

Un accord de niveau de service type se compose de :

- Une introduction, soulignant l'objet de l'accord.
- Une description des services, soulignant le ou les services que l'accord prend en charge et les détails du ou des services.
- Les responsabilités mutuelles, à savoir le responsable pour chacune des parties du ou des services.
- Une esquisse du champ d'application de l'accord de niveau de service.
- Les heures de service applicables, à savoir de quelle heure à quelle heure le ou les services sont disponibles conformément à l'accord.
- La disponibilité du service, à savoir l'étendue selon laquelle le ou les services sont disponibles au cours de la fenêtre de service et en-dehors de la fenêtre de service.
- La fiabilité du service.
- Les dispositions liées à l'assistance au client.
- Les points de contact et procédure d'escalade, notamment une matrice de communication.
- Les indicateurs de performance du service.
- Les exigences de sécurité.
- Les coûts et la méthode de facturation utilisée.

Tableau 18. **Exemple des dispositions d'assistance à l'utilisateur ou au client dans le cadre d'un accord de niveau de service**

Priorité/ Description	Faible	Normale	Élevée	Critique
Gravité de l'incident	Aucun obstacle au travail de l'administration fiscale.	Interruption du travail de l'administration fiscale ; solution de remplacement disponible.	Interruption de processus critiques affectant les utilisateurs individuels ; aucune solution de remplacement disponible.	Interruption de processus critiques de l'administration fiscale affectant plusieurs utilisateurs ; aucune solution de remplacement disponible.
Urgence de résolution	L'administration fiscale n'a pas besoin de réparation immédiate.	L'administration fiscale n'a pas besoin de réparation immédiate.	L'administration fiscale a besoin d'une réparation immédiate.	L'administration fiscale a besoin d'une réparation immédiate.
Objectifs de l'accord de niveau de service				
90 % du temps de réaction inférieur à	2 jours	1 jour	4 heures	2 heures
90 % du temps de résolution inférieur à	2 semaines	1 semaine	3 jours	24 heures (correctif immédiat)

Sous-exigence 3.2.4.4. Gestion de la fourniture de service du prestataire

La SE 3.2.4.4 aborde la garantie de sécurité lors du recours à l'externalisation et à des chaînes d'approvisionnement par une gestion attentive des relations de l'administration fiscale avec les fournisseurs. Il s'agit d'une exigence très importante, car plusieurs incidents de sécurité notoire ont été attribuées à des déficiences du réseau des fournisseurs.

De nombreuses administrations fiscales cherchent à garantir que toutes les données des contribuables restent à tout moment au sein des bâtiments, qu'elles sont utilisées et contrôlées par elles-mêmes et/ou d'autres agences gouvernementales avec une étroite surveillance de l'accès à ces données par des tiers. Néanmoins, les administrations fiscales autorisent de plus en plus des fournisseurs informatiques tiers à accéder à leurs centres de données pour fournir un développement, une maintenance ou une mise à jour à distance. Dans ces cas-là, les types d'accès autorisés doivent être clairement établis et des contrôles appropriés doivent être en place. Un processus de gestion des fournisseurs est résumé dans la figure 13.

Les contrats de l'administration fiscale avec les fournisseurs doivent comporter des exigences spécifiques pour traiter des risques de sécurité des informations associés aux services informatiques et à la chaîne d'approvisionnement. À titre d'exemple, pour un système de messagerie basé sur le cloud (nuage) ou une application de ressources humaines externalisée, le contrat doit garantir que le fournisseur respecte aussi toutes les exigences et sauvegardes de sécurité applicables, en particulier quand il traite des données et des informations (voir l'encadré 28).

Au vu de la nécessité qu'il y a à traiter des risques de la sécurité des informations dans le contexte d'un recours à des fournisseurs, les administrations fiscales doivent généralement définir une politique de sécurité des informations pour protéger les actifs et les données qui sont accessibles par les fournisseurs. Cette politique doit

FIGURE 13. **Processus de gestion des fournisseurs**

être convenue avec les fournisseurs et être documentée. Cela implique que les risques spécifiques doivent être identifiés et nécessiteront l'application de contrôles de sécurité, tel que décrit dans la SE 3.2.4.2 sur le déploiement d'un nombre approprié de contrôles de sécurité. Certains contrôles peuvent être mis en place par l'administration fiscale elle-même, quand d'autres seront mis en œuvre par les fournisseurs. De tels contrôles peuvent comporter :

Encadré 28. **La sécurité dans les contrats avec les fournisseurs**

Il est fortement recommandé que les administrations fiscales s'accordent formellement sur des exigences de sécurité avec chaque fournisseur pouvant accéder à, traiter, sauvegarder, communiquer ou fournir des composants ou services informatiques et/ou accéder à leurs données. Les éléments suivants sont couramment documentés dans les contrats avec les fournisseurs :

- Une description des informations fournies au fournisseur, ou auquel il a accès, et des méthodes de fourniture ou d'accès aux informations.
- La classification des informations.
- Les exigences légales et réglementaires relatives à la confidentialité et la sécurité.
- Les obligations de chaque partie pour mettre en œuvre les contrôles de sécurité pertinents, et le cas échéant le respect d'une norme internationale reconnue sur la sécurité des informations.
- Les règles sur les utilisations acceptables et inacceptables des informations.
- Si cela est approprié, une liste du personnel du fournisseur autorisé à accéder à ou à recevoir les informations de l'administration fiscale (ou les conditions et procédures pour obtenir une telle autorisation).
- Les politiques de sécurité des informations de l'administration fiscale applicables au contrat.
- Les dispositions pour traiter les situations pour lesquelles le fournisseur devient incapable de fournir son produit ou service, afin d'éviter tout problème et tout retard dans l'activité de l'administration fiscale.
- Les processus de résolution des conflits.

Il convient d'observer que les contrats pourraient impliquer d'autres parties, tels que des sous-traitants, de même que les contrats peuvent varier significativement entre différents types de fournisseurs.

- l'identification, le classement et la documentation de tous les fournisseurs, ainsi que la définition du type d'information auxquels ils pourront avoir accès.
- Une sensibilisation du personnel de l'administration fiscale à la confidentialité relative aux informations qu'il manipule en conjonction avec des fournisseurs, et à la façon dont le personnel doit interagir avec les fournisseurs.
- Des accords de niveau de service.
- Des accords de confidentialité.
- Des procédures et processus de gestion des incidents.

Surveillance et examen des services fournis

Les administrations fiscales doivent régulièrement surveiller, examiner ou garantir d'une façon ou d'une autre que la fourniture de service par les fournisseurs est soumise à un audit afin de s'assurer que les termes et conditions de la confidentialité et de la sécurité des informations sont respectés, et que les incidents et problèmes sont correctement gérés.

Il peut aussi être approprié de disposer d'un processus de gestion des relations de services qui :

- Surveille les niveaux de performance du service.
- Demande et examine les rapports de service que doivent produire les fournisseurs.
- Prévoit des audits du fournisseur (via l'administration fiscale elle-même ou un auditeur indépendant).
- Examine les historiques et enregistrements des événements de sécurité des informations du fournisseur, les problèmes opérationnels, les défaillances, le suivi des pannes et interruptions associés au service fourni.
- Garantit que le fournisseur entretient une capacité de service suffisante et assure les niveaux de continuité de service convenus.

Encadré 29. **Fournisseurs non spécialistes des technologies de l'information**

Il est fréquent que l'atteinte à la sécurité des données ne concerne pas des prestataires informatiques mais des fournisseurs d'autres services. Des atteintes à la sécurité peuvent par exemple s'être produites quand des sous-traitants en charge du nettoyage ont accédé aux systèmes des ressources humaines du client (afin de mettre à jour les détails relatifs aux agents de nettoyage et nécessitant un accès au bâtiment) et que des pirates informatiques ont alors exploité une vulnérabilité dans les systèmes informatiques du fournisseur pour accéder à distance aux systèmes de l'organisation. Il est donc important de disposer de contrôles de sécurité pour les fournisseurs de service hors informatique si ces fournisseurs ont accès à l'infrastructure, à distance ou de toute autre façon.

Les administrations fiscales sont encouragées à conserver un contrôle global et une visibilité suffisants sur tous les aspects de la sécurité associés aux informations sensibles ou critiques, ou aux installations traitant de ces informations, auxquels les fournisseurs ont accès, qu'ils traitent et qu'ils gèrent. Cette visibilité peut être obtenue en mettant en place des rapports périodiques édités par les fournisseurs sur leur gestion du changement, gestion des vulnérabilités et de la réponse aux incidents de sécurité.

La responsabilité ultime de la gestion des relations avec les fournisseurs doit être attribuée à une personne ou une équipe de gestion de service dédiée, qui doit prendre les actions qui s'imposent en cas d'observation de déficiences dans la fourniture du service.

Sous-exigence 3.2.4.5. Assurer la continuité des services informatiques sur la base des accords de niveau de service

Comme cela est expliqué dans la SE 3.2.1, la sécurité des informations ne se résume pas à empêcher un accès non autorisé à des informations, mais aussi à s'assurer que les utilisateurs légitimes qui ont besoin d'un accès peuvent en disposer quand ils en ont besoin (concept de « disponibilité » dans le trio « confidentialité, intégrité, disponibilité »). Si le personnel ne peut pas faire confiance aux services formels d'accès aux informations quand il en a besoin pour effectuer son travail, il peut chercher à se procurer cet accès par lui-même, par exemple en téléchargeant des sous-ensembles d'une base de données sur son propre système privé de stockage de fichiers.

Une disponibilité insuffisante génère par conséquent des pratiques dangereuses et des voies d'accès informelles, ce qui génère alors des risques de sécurité incontrôlés. Il est essentiel de garantir que la continuité des services opérationnels, dont le service informatique, soit aussi efficace que possible.

Cette section concerne la garantie de bonnes pratiques de continuité du service informatique, en se focalisant sur trois aspects essentiels :

- récupération et résilience.
- sauvegarde des données.
- planification, mise en œuvre et vérification de la continuité de la sécurité des informations.

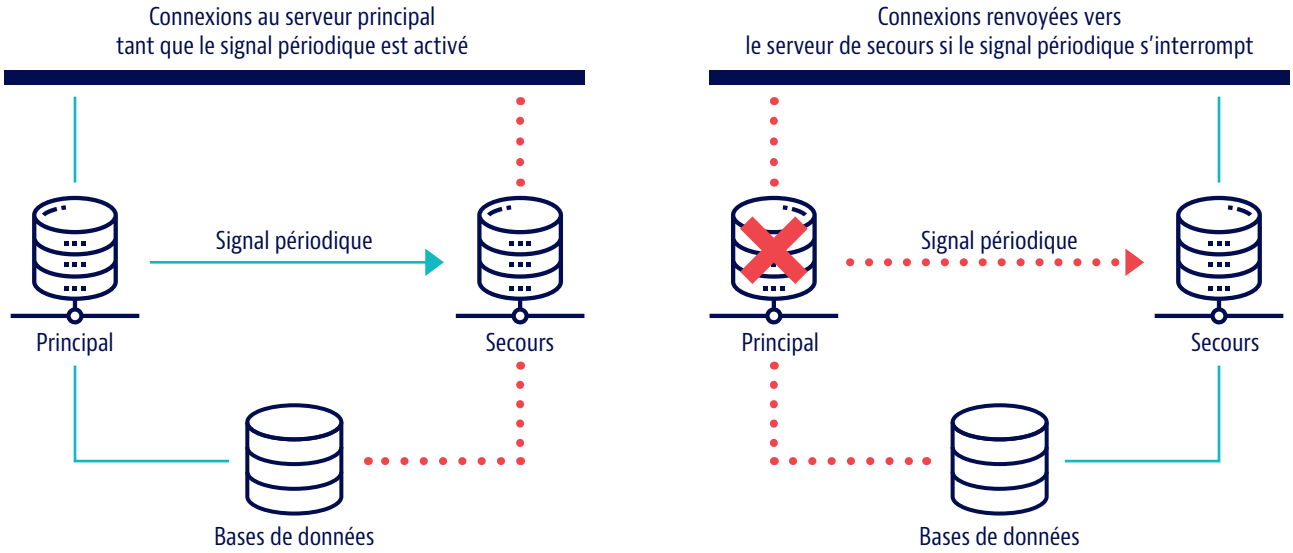
Récupération et résilience

La résilience fait référence à l'atténuation du risque d'interruption de service, quand la récupération concerne la restauration d'un service qui a été interrompu.

Toute approche de continuité du service informatique inclura des éléments de ces deux concepts. De plus, de nombreux contrôles de sécurité individuels comporteront des éléments de récupération et de résilience (voir la figure 14, qui montre un exemple de mise en œuvre d'une récupération et de résilience via un accord de basculement).

La résilience présente l'avantage d'être plus efficace pour réduire le nombre d'interruptions de service. Sur la base

FIGURE 14. **Exemple d'un accord de basculement**



Note: il existe dans ce cas un serveur primaire (actif) et un serveur secondaire (passif) (donc sans équilibrage de charge). Le serveur actif émet un « signal périodique » régulier au serveur de secours, et le basculement est déclenché en cas d'absence du signal périodique.

des bonnes pratiques internationales reconnues, les étapes que peut suivre une administration fiscale pour améliorer la résilience, et par conséquent la disponibilité du service, consistent entre autres choses à :

- Garantir la résilience au niveau du composant et des niveaux de service. Quand les services sont créés ou modifiés, il est important de s'assurer que les éléments du service et les composants qui soutiennent les éléments de service sont sélectionnés, conçus, mis en œuvre et entretenus d'une façon qui améliore la résilience et réduit le risque d'interruption de service.

- Garantir des une redondance du même service. Disposer de deux instances parallèles du même service signifie qu'en cas de défaillance d'un composant dans une des instances, le traitement est commuté vers l'instance fonctionnelle.

- Garantir une alimentation électrique de secours. Au niveau du centre de données, il existe différents points de dysfonctionnement, comme l'alimentation en eau, en air conditionné et en électricité. Il doit si possible exister une alimentation électrique de secours, provenant d'un réseau séparé ou d'un type d'alimentation de secours sans coupure. L'assurance de la disponibilité dans les centres de données est appelée « Tier » (niveau). Il existe 4 niveaux et le choix est fonction du temps d'indisponibilité que peut accepter une administration fiscale. Cette classification est fournie par The Uptime Institute, fondé en 1993.

  - Un centre de données de niveau **Tier 1** a une voie unique d'alimentation et de refroidissement, et peut éventuellement avoir quelques composants redondants et de secours. Il a une durée de disponibilité attendue de 99,671 % (28,8 heures de temps d'arrêt annuel).

  - Un centre de données de niveau **Tier 2** a une voie unique d'alimentation et de refroidissement, et quelques composants redondants et de secours. Il a une durée de disponibilité attendue de 99,741% (22 heures de temps d'arrêt annuel).

  - Un centre de données de niveau **Tier 3** a plusieurs voies d'alimentation et de refroidissement, et des systèmes en place pour le mettre à jour et l'entretenir sans avoir à le mettre hors ligne. Il a une durée de disponibilité attendue de 99,982 % (1,6 heure de temps d'arrêt annuel).

  - Un centre de données de niveau **Tier 4** est conçu pour être totalement tolérant aux pannes et dispose d'une redondance pour chaque composant. Il a une durée de disponibilité attendue de 99,995 % (26,3 minutes de temps d'arrêt annuel).

- Garantir le fonctionnement des services depuis plusieurs centres de données. Les juridictions de taille petite à moyenne doivent envisager de disposer d'installations de sauvegarde au niveau desquelles au moins certains traitements sont réalisés de jour comme de nuit, même si ces installations n'ont pas une taille identique à celle du centre de données principal. Les administrations les plus grandes travailleront quoi qu'il en soit depuis plusieurs centres de données, et il est souhaitable de concevoir les centres de données pour que le traitement puisse passer sans problème d'un centre à l'autre. Une option est alors un centre de données de secours qui n'est pas activement utilisé, mais peut l'être dans l'éventualité d'une urgence. L'avantage d'une telle disposition est qu'il est possible de partager le secours avec d'autres organisations, de façon à mieux gérer les coûts. L'inconvénient de telles dispositions est que le secours ne fonctionne que si les autres organisations n'ont pas besoin du centre de secours en même temps, ce qui peut pourtant se produire en cas de désastre environnemental.

- Utiliser un site dédié pour redémarrer les opérations en cas de défaillance grave. Une administration fiscale, en fonction de ses coûts et de ses besoins, peut choisir une solution de centre de secours graduel, intermédiaire, immédiat ou mobile :

  - Un **centre de secours graduel** propose des installations, l'air conditionné, l'alimentation, des racks et le câblage.

  - Un **centre de secours intermédiaire** propose les caractéristiques du centre graduel plus du matériel et des logiciels dédiés similaires à une infrastructure d'administration fiscale, mais pas de données.

  - Un **centre de secours immédiat** est une réplication en temps réel du centre de données de l'administration fiscale, qui contient exactement les mêmes équipements et données.

  - Un **centre de secours mobile** est similaire à un centre de secours immédiat mais dans des racks mobiles militaires, et il est donc facilement transportable.

Une administration fiscale peut aussi choisir de répliquer uniquement une partie de ses services opérationnels, ou ceux qui sont les plus critiques ou qui contiennent les données les plus sensibles (par exemple les données des contribuables ou les renseignements échangés).

Sauvegarde des données

Les données d'une administration fiscale doivent être sauvegardées. Pour les juridictions ayant des centres

de données multiples connectés par fibre optique, cela peut être réalisé automatiquement, avec une sauvegarde complète disponible au niveau de chaque centre. D'une façon générale cependant, c'est une sauvegarde hors ligne qui utilise des bandes et/ou des disques qui sera utilisée. Il est ici important de prendre en considération divers aspects :

- la façon dont la sauvegarde est traitée ;
- la ou les personnes responsables de l'opération ;
- le mode de stockage des copies hors ligne ;
- les contrôles existant pour garantir que les données téléchargées ne font pas l'objet d'une utilisation abusive ;
- le processus permettant de tester qu'une copie téléchargée peut être restaurée de façon fiable et précise ;
- la fréquence de réalisation de tels tests.

En relation avec les renseignements échangés automatiquement, la compréhension de la gestion des données dans ces processus et les moyens pour garantir leur protection doivent être clairs.

Enfin, comme les principales préoccupations sont la disponibilité et la confidentialité, il est recommandé que les données très sensibles stockées (au repos), qu'il s'agisse des données réelles ou de sauvegarde, soient cryptées par un mécanisme de chiffrement bénéficiant d'une reconnaissance internationale (voir la SE 3.2.5 sur la protection des informations).

Planification, mise en œuvre et vérification de la continuité de la sécurité des informations

Un point important concernant la continuité du service informatique, comme souvent quand il s'agit de sécurité informatique, est la planification. Tous les aspects précédemment couverts seront généralement abordés au sein des plans de continuité des activités[16] ou des plans de reprise d'activité, ou les deux. En d'autres termes, la continuité du service informatique doit être planifiée avant et après un incident, de façon à ce que la sécurité puisse être gérée en continu.

En l'absence d'une planification de la continuité de service ou de la reprise d'activité, les administrations fiscales devraient partir du principe que les exigences de sécurité informatique restent les mêmes dans des situations de crise que dans des conditions opérationnelles normales. Comme alternative, les administrations fiscales peuvent conduire des analyses d'impact sur leurs activités afin de déterminer les exigences de sécurité informatique applicables aux situations de crise.

Pour les juridictions plus petites, il est conseillé de prendre des mesures de planification lors de l'analyse initiale d'impact sur les activités de continuité de service et/ou de récupération après sinistre.

Lors de la mise en œuvre des plans de continuité des activités/plans de récupération après sinistre, les administrations fiscales sont encouragées à établir, documenter et entretenir des contrôles pour garantir le niveau requis de continuité des services informatiques et de la sécurité des informations. On compte parmi les aspects importants à considérer :

- Disposer d'une structure de gestion adéquate pour préparer, atténuer et réagir à un événement perturbateur. Un exemple courant est la définition d'une cellule de gestion de crise, qui implique des fonctions et personnes pertinentes.
- L'établissement de contrôles compensateurs par rapport aux contrôles de sécurité informatique qui ne peuvent être maintenus lors d'une situation de crise. En cas de panne de courant par exemple, un contrôle d'accès physique peut être réalisé manuellement par le personnel de sécurité si les portillons d'accès ne peuvent fonctionner.
- Documenter les plans, réponses et procédures de récupération telles qu'approuvées par la direction.

Ces contrôles, une fois mis en œuvre, doivent être vérifiés, examinés et évalués à intervalles réguliers afin de garantir qu'ils sont valides et efficaces. Pour atteindre cet objectif, les administrations fiscales peuvent :

- Former et tester les connaissances du personnel et les programmes permettant de réaliser les procédures de continuité informatique, les processus et les contrôles qui garantissent une performance conforme aux objectifs définis.
- Analyser la validité et l'efficacité des mesures de continuité lorsque les systèmes, les processus, les procédures et les contrôles ou les solutions de continuité d'activité/reprise d'activité changent.

La non-réalisation de tels tests peut mener à une défaillance totale des systèmes. Un exemple est l'absence de test et de restauration des sauvegardes de données, qui peut générer une perte totale des données. Il s'agit d'un résultat inacceptable, en particulier si cela concerne des données d'EAR.

16. La gestion de la continuité des activités est abordée dans le détail dans la SE 3.2.1.5

SOUS-EXIGENCE 3.2.5 : PROTECTION DES INFORMATIONS

Il s'agit de protéger les différents types d'informations papier et numériques gérées par les administrations fiscales, qu'elles soient stockées, utilisées ou déplacées entre des environnements et sites de travail, par des contrôles choisis en fonction de leur classification en termes de sensibilité et de confidentialité.

La SE 3.2.5.1 exige que les administrations fiscales gèrent efficacement les informations, conformément à un ensemble de politiques et procédures, sur l'ensemble du cycle de vie des informations (notamment la nomenclature, la classification, la manipulation, le stockage, la surveillance, l'audit et la destruction du document ; et y compris les appareils et supports qui hébergent les informations).

Plus spécifiquement, les contrôles sur l'ensemble du cycle de vie de l'information incluent des contrôles de l'environnement de travail, tels que :

- contrôle de la politique du bureau propre ;
- contrôles de l'imprimante ;
- mécanisme de stockage physique et numérique des informations ;
- chiffrement et contrôles de domaine ;
- contrôles sécurisés des supports d'informations, tels que les périphériques ;
- contrôles en fin de cycle de vie, tels que les politiques de suppression des informations.

La protection des informations *échangées* est la préoccupation spécifique du processus d'évaluation du Forum mondial. On attend donc des administrations fiscales qu'elles garantissent que les contrôles généraux en place permettent cette protection, et que des contrôles améliorés appropriés soient utilisés pour protéger les informations échangées en particulier. Ce dernier point est traité dans la SE 3.2.5.2, qui exige que les administrations fiscales disposent de processus pour les informations reçues d'autres autorités compétentes afin de garantir le respect des obligations découlant des accords d'échange internationaux, notamment la prévention d'un mélange avec d'autres informations.

Il est essentiel de distinguer la SE 3.2.5 d'autres SE, telles que celles qui exigent des contrôles pour l'accès logique aux données (SE 3.2.3.3, 3.2.3.4), pour la sécurité du système informatique (SE 3.2.4) et pour la gestion de la sécurité des opérations (SE 3.2.6). Ces SE décrivent des contrôles qui sont appliqués *d'une façon générale* pour protéger les informations, quand les contrôles du cycle de vie de l'information dans le cadre de la SE 3.2.5 font référence à des contrôles de sécurité qui doivent être appliqués *aux données elles-mêmes* du fait des politiques de classification de la confidentialité.

Tableau 19. **Définitions des principaux concepts**

Concept	Description
Autorité compétente	Il s'agit de la ou des personnes ou de la ou des autorités gouvernementales désignées par une juridiction comme personne compétente pour échanger des informations conformément à tout accord international d'échange de renseignements.
Chiffrement	C'est un mécanisme de protection appliqué à des données et qui les rend accessibles uniquement si une clé de déchiffrement adéquate est fournie.
Classification des informations	Processus d'identification des types d'informations que les administrations fiscales détiennent et de détermination du niveau de protection qu'elles doivent recevoir.
Durée de conservation	Exigence légale de conservation des informations pendant une période fixe même si les informations ne sont plus nécessaires à des fins d'activité fiscale.
Nettoyage des supports	Il s'agit du processus de traitement de données conservées sur un support de stockage et permettant de réduire le risque de récupération et de reconstruction à un niveau acceptable.
Politique du bureau propre	Une politique du bureau propre spécifie la façon dont les employés doivent laisser leur espace de travail lorsqu'ils quittent leur bureau afin de garantir la confidentialité des informations.
Politique d'utilisation acceptable	Ensemble de règles qui établissent les pratiques autorisées et interdites en rapport avec les systèmes d'informations contenant des informations confidentielles.

Cette section est divisée en trois parties :

- une brève présentation des trois étapes du cycle de vie de l'information dans les administrations fiscales ;
- une description des contrôles de sécurité généraux à appliquer à chacune de ces trois étapes (SE 3.2.5.1) ;
- une esquisse des contrôles pertinents du cycle de vie de l'information pour les échanges d'informations (SE 3.2.5.2).

Le tableau 19 présente les définitions des principaux concepts abordés dans la SE 3.2.5.

Le cycle de vie de l'information

Comme illustré dans la figure 15, les contrôles de l'information, qu'elle soit sous forme numérique ou papier, doivent être appliqués au niveau des trois phases générales du cycle de vie de l'information. Des contrôles renforcés sur le cycle de vie doivent s'appliquer aux informations échangées.

Les étapes et contrôles sur les différentes étapes du cycle de vie de l'information sont présentés ici sur la base de la pratique habituelle des administrations fiscales. Les administrations fiscales sont cependant encouragées à adopter l'approche la plus adaptée à leur situation.

Avant de détailler les contrôles associés à la protection des informations au niveau de chaque étape du cycle de vie, il est important de souligner l'importance de la gouvernance et des processus opérationnels pour la protection des informations, comme cela est illustré dans l'encadré 30.

Sous-exigence 3.2.5.1. Contrôles généraux sur le cycle de vie de l'information

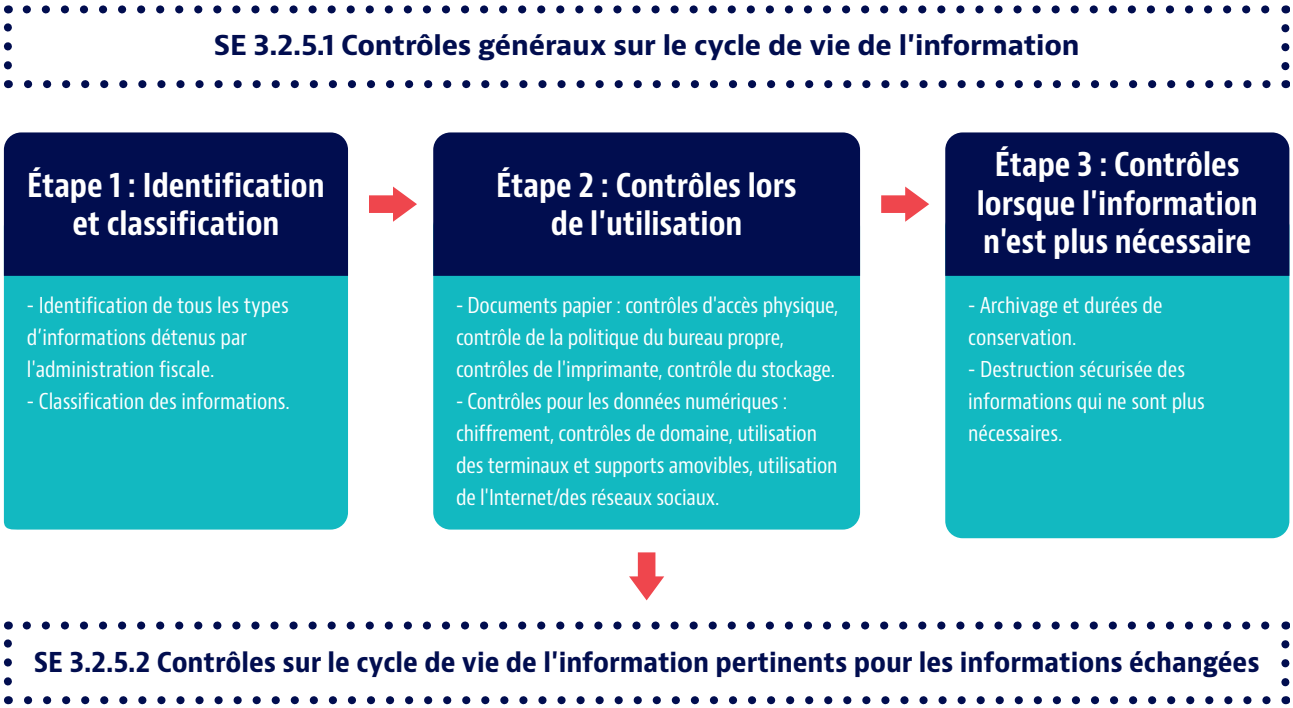
Étape 1. Identification et classification des informations

La classification des informations est le point de départ et le cœur de la gestion du cycle de vie de l'information, d'où découlent tous les contrôles de sécurité ultérieurs. La classification des informations a pour objet de garantir que celles-ci reçoivent une protection appropriée et proportionnée à leur classification.

Les informations gérées par les administrations fiscales proviennent de différentes sources, telles que :

- les déclarations de revenus des contribuables ;
- les tierces déclarations provenant de personnes avec lesquelles un contribuable a une relation commerciale ou d'emploi (par exemple banques, employeur) ;

FIGURE 15. **Gestion du cycle de vie de l'information**



Encadré 30. **Protection des informations, gouvernance et processus opérationnels**

Les informations ne peuvent être protégées sur leur cycle de vie que si elles sont convenablement gérées, en respectant des règles de gouvernance claires. Dans l'idéal, il doit exister des lignes claires de responsabilité pour tous les actifs informationnels, chaque type d'information ayant un responsable désigné.

De plus, les informations fiscales doivent être gérées et manipulées par les utilisateurs en respectant des processus opérationnels établis et définis. Par exemple, les données sensibles des contribuables sont généralement manipulées dans le cadre de processus opérationnels fiscaux prédéfinis, comme la collecte et le recouvrement de créances. Dès que possible, des processus opérationnels doivent être mis en place pour toutes les façons dont les données sensibles, y compris les informations échangées, sont utilisées. Cette mesure est importante car :

- Elle permet à l'administration fiscale de gérer efficacement, par le biais de politiques et de procédures bien définies, la façon dont les utilisateurs accèdent aux données et les utilisent, en les protégeant mieux d'un accès non autorisé ou d'une utilisation abusive.
- S'il existe des processus définis, il est plus simple d'évaluer l'efficacité du processus pour protéger les données, et d'identifier et de réaliser les améliorations qui rendront la protection encore plus efficace.
- En cas d'absence de processus opérationnels définis, il est probable que les pratiques ne soient pas homogènes et que surviennent des méthodes de manipulation des données qui s'avèrent risquées.

- les rapports d'autres agences gouvernementales, par exemple service de la sécurité sociale ;
- l'échange international de renseignements.

Tous ces types d'informations sont associés à un certain niveau de sensibilité et de confidentialité, et doivent être classées en conséquence pour que des niveaux de protection supérieurs soient appliqués aux informations les plus sensibles.

Si les informations ne sont pas classées, ou si elles ne sont pas classées en fonction de leur niveau de confidentialité et de sensibilité, deux scénarios non souhaités peuvent se produire : tout est protégé au même niveau élevé ou tout est protégé de façon inadéquate.

La protection de tous les types d'informations selon les mêmes niveaux élevés serait trop coûteuse et pourrait entraver la disponibilité des informations, quand la protection de toutes les données à un moindre niveau exposerait les informations sensibles à une utilisation abusive et pourrait générer des atteintes à la sécurité par des personnes qui ne devraient pas avoir accès à ces informations.

Identifier tous les types d'informations détenues

Avant d'opérer un classement, les administrations fiscales doivent d'abord connaître et clairement identifier les types d'informations qu'elles détiennent. Les principaux actifs informationnels détenus par les administrations fiscales, que ce soit sous forme physique ou numérique, peuvent être :

- les déclarations de revenu des personnes ou des entreprises ;
- les informations provenant d'employeurs ;
- la correspondance avec les contribuables ;
- les informations échangées (automatiquement, spontanément et sur demande) ;
- les avis d'imposition et rescrits ;
- les directives à destination du personnel (et les directives à destination des contribuables) pour remplir les déclarations d'impôt ;
- les directives sur la conduite des contrôles fiscaux et autres activités de conformité ;
- les informations en relation avec des enquêtes criminelles en cours ;
- les notes internes, prise de position et recherches ;
- les informations sur les technologies de l'information qui pourraient être utilisées pour accéder aux informations opérationnelles, telles que :
  - les identifiants d'accès, dont les mots de passe système ;
  - le code source ;
  - la configuration de la passerelle et des serveurs de domaine.

Classification des informations

Quand les administrations fiscales ont identifié tous les types d'informations qu'elles détiennent, elles doivent les classer, préciser comment chaque catégorie doit être gérée et contrôlée et refléter ces éléments clairement par une politique correspondante.

Les administrations fiscales peuvent utiliser différents critères de classification. Quatre approches sont généralement utilisées, aucune n'en excluant une autre (voir le tableau 20). Les administrations fiscales peuvent utiliser plus ou moins de critères, en fonction des informations qu'elles détiennent, de leurs lois et pratiques nationales, et de l'étendue de leurs opérations.

Chaque type d'information doit posséder sa propre classification en fonction des critères utilisés. Le tableau 21 montre un exemple simplifié d'une matrice de classification des informations, et il convient de noter que les exemples donnés ne sont pas exhaustifs et sont uniquement présentés à des fins d'illustration. Toutefois, il est important de noter que les informations échangées doivent au moins être classées comme confidentielles au sein de l'administration fiscale afin de garantir les contrôles appropriés.

Étape 2. Contrôles appliqués à la protection de l'information lors de son utilisation

Lorsque les administrations fiscales ont défini les types d'information et les critères applicables à leur classification, elles doivent déterminer les principaux contrôles pour chaque catégorie, et transposer clairement ces éléments dans une politique. Le cadre ainsi défini doit permettre une protection adéquate des informations sensibles et confidentielles, tout en facilitant l'accès aux informations moins sensibles.

Tableau 20. **Critères de classification des informations**

Critère	Description
Sensibilité	Le critère le plus courant est une classification reposant sur la sensibilité, avec des catégories pouvant être les suivantes : ● public (par exemple documents pouvant être utilisés sur un site Web externe) ; ● interne (communications internes d'ordre général) ; ● restreint/confidentiel (catégorie qui inclut généralement les informations sur les contribuables) ; ● secret/top secret (généralement restreint à des situations dans lesquelles il existe une menace importante pour les intérêts individuels ou collectifs, par exemple intérêts vitaux, intérêts commerciaux ou opérationnels, ou intérêt nationaux).
Accès restreint	Généralement utilisé en conjonction avec le critère de la sensibilité, ce critère fait référence à des contrôles supplémentaires reposant sur le principe du besoin d'en connaître plutôt que sur la sensibilité en elle-même. Par exemple, du fait de leur sensibilité, les données d'EAR sont généralement classées comme restreintes/confidentielles (ce sont des données sur les contribuables), mais du fait des obligations découlant de traités, l'accès est davantage restreint sur une base du besoin d'en connaître aux seuls employés devant manipuler les données issues de l'EAR pour réaliser leurs tâches spécifiques.
Échelle/volume	Les fichiers composés d'un grand volume d'informations représentent une vulnérabilité supérieure à un fichier individuel, et des contrôles renforcés doivent être appliqués dès que sont impliqués des fichiers agrégés. Ces critères peuvent être classés en utilisant des « niveaux d'impact », qui font référence à l'impact de la confidentialité et de l'intégrité des données en cas d'accès non autorisé, et au type de contrôles d'accès requis en fonction du niveau d'impact. Par exemple, l'utilisation de l'échelle de 1 à 5, 1 étant le niveau d'impact le plus faible et 5 étant réservé à l'impact le plus élevé en termes de « menace vitale ou aux intérêts de l'État ». Un fichier individuel unique d'échange de renseignements conservé sur un ordinateur portable ou une clé USB cryptée peut avoir un niveau d'impact 2 ou 3 ; la base de données pour l'échange automatique de renseignements peut avoir un niveau d'impact 4. Ces catégories détermineront alors par exemple le type de contrôles d'accès requis, par exemple si les données doivent ou non être cryptées.
Type d'informations	Ce critère peut être utilisé pour classer différents types d'informations, par exemple les fichiers des ressources humaines ou des marchés publics peuvent être classés comme Confidentiel, et les documents informatifs pour les contribuables classés comme Non confidentiel.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Tableau 21. **Exemple de matrice de classification de l'information**

Catégorie	1 – Publique	2 – À usage interne	3 – Confidentielle	4 – Hautement confidentielle
Description	Information qu'il est possible de rendre publique et information interne dont la divulgation non autorisée ne serait pas préjudiciable à l'administration fiscale.	Information interne non sensible, dont la divulgation non autorisée pourrait toutefois s'avérer inappropriée pour l'administration fiscale.	Information interne et sensible, accessible uniquement aux personnes ayant besoin d'en connaître, et dont la divulgation non autorisée pourrait causer un préjudice à l'administration fiscale et aux personnes concernées.	Information interne, hautement sensible, parfois à grande échelle, accessible uniquement à un nombre limité de personnes selon le principe strict du besoin d'en connaître, et dont la divulgation non autorisée pourrait causer un préjudice grave et/ou de grande ampleur à l'administration fiscale et aux personnes concernées.
Information entrant dans cette catégorie	• Notice pour remplir la déclaration de revenus • Site web externe	• Mode opératoire pour la conduite des contrôles fiscaux • Supports de formation du personnel • Notes internes non confidentielles	• Information provenant des employeurs • Correspondance avec les contribuables • Imposition/ rescrits • Contrats, Accords de niveau de service • Notes internes confidentielles.	• Déclarations de revenus des particuliers • Renseignements échangés sur demande • Renseignements échangés automatiquement • Information permettant l'accès aux systèmes opérationnels (code source, ID d'accès)

De manière générale, des contrôles doivent être appliqués :

- **lorsque l'information est en cours d'utilisation ou « en mouvement »**, c'est-à-dire exploitée à des fins fiscales ou déplacée entre différents lieux ou environnements de travail ;
- **lorsqu'elle est stockée ou « au repos »** entre deux utilisations.

Ces contrôles doivent tenir compte des principes d'accès décrits à la SE 3.2.3 (gestion des accès), comme le « besoin d'en connaître » et le moindre privilège. Les informations sensibles, au format physique et numérique, doivent être accessibles uniquement aux personnes ayant un motif professionnel légitime.

Par le passé, les informations sur les contribuables étaient essentiellement gérées sous un format papier. Les évolutions technologiques et la nécessité pour les administrations fiscales d'améliorer leurs activités tout en protégeant les informations ont incité à privilégier le format numérique. Aujourd'hui, les informations détenues par les administrations fiscales les plus avancées technologiquement sont soit reçues au format numérique ou soit numérisées à la réception puis gérées par des processus automatisés. Les administrations fiscales sont à des stades très divers dans la transition du papier au numérique. Pour évaluer le degré de confidentialité, il est important que les deux formats, le cas échéant, soient pris en compte dans la détermination des contrôles à appliquer.

Les sections suivantes présentent un certain nombre d'orientations et de bonnes pratiques en matière de contrôles appliqués par les administrations fiscales pour protéger l'information au format physique et numérique.

Contrôles appliqués à la protection des documents papier

La protection des documents papier dans l'enceinte d'une administration fiscale inclut essentiellement des mesures pour l'accès physique des employés aux documents papier, des contrôles de la politique du bureau propre, des contrôles sur les imprimantes, et des contrôles au niveau du stockage lorsque les informations sont « au repos » (i.e. lorsqu'elles ne sont pas en cours d'utilisation).

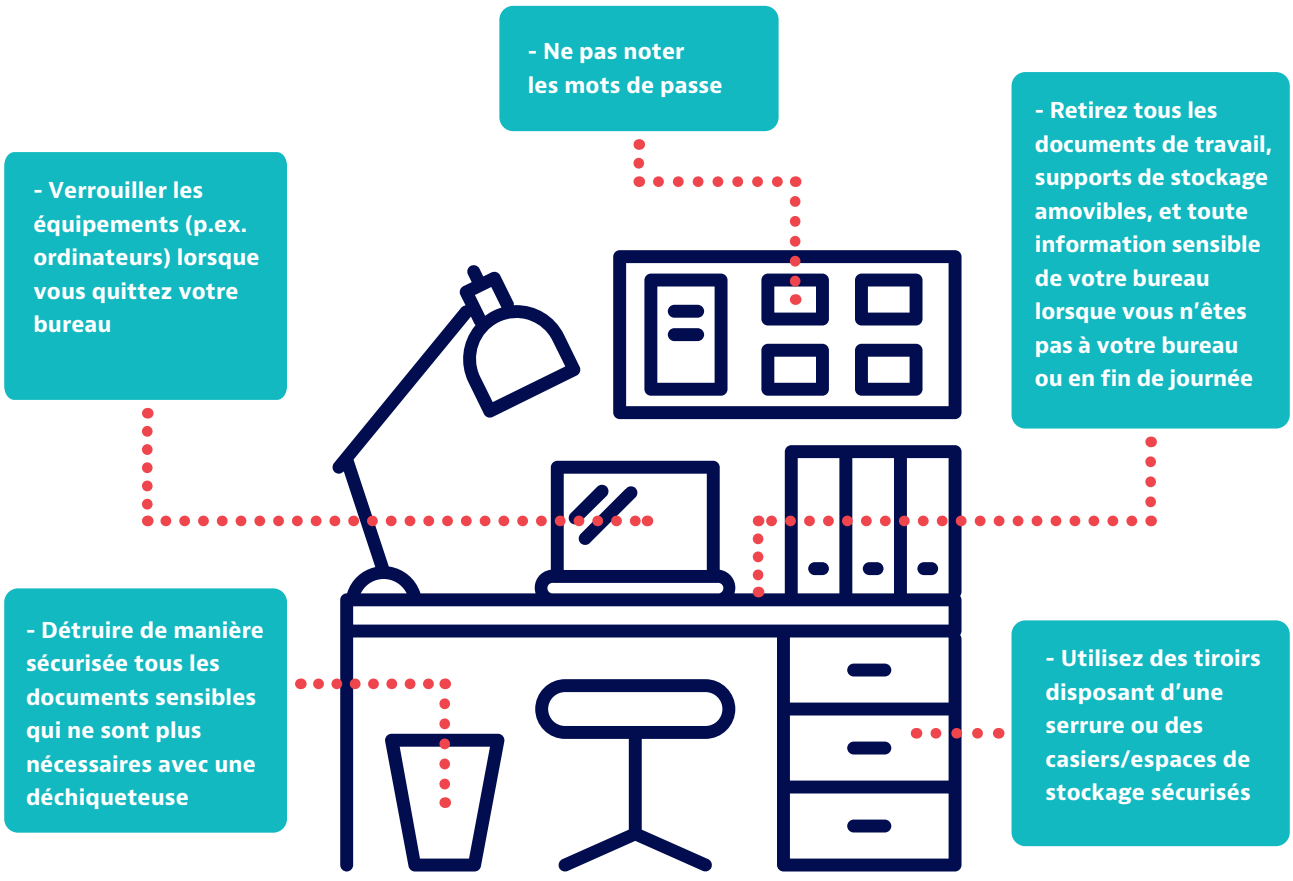
Accès physique des personnes autorisées aux documents papier

Il est plus difficile de gérer l'accès des employés aux documents papier que l'accès aux données numériques, celles-ci pouvant être plus facilement protégées avec des contrôles d'accès logique (voir les SE 3.2.3.3 et 3.2.3.4 pour les contrôles régissant l'accès logique).

Les mesures suivantes sont généralement appliquées pour restreindre l'accès aux documents papier :

- Restriction de l'accès aux bâtiments et locaux aux seules personnes autorisées et mise en œuvre de contrôles permettant de séparer les espaces de travail dans l'enceinte de l'administration fiscale. Les mesures de sécurité peuvent inclure l'obligation pour les employés autorisés d'utiliser un badge électronique ou un identifiant photo, ou l'installation de systèmes à code pour pénétrer dans tout ou partie des locaux, y compris l'unité d'échange de renseignements ou tout(e) autre zone ou espace de stockage où des informations sensibles sont conservées. Ce système de contrôle primaire peut être complété par un système secondaire, par exemple la présence d'agents de sécurité, la vidéosurveillance et l'accompagnement obligatoire des visiteurs. Ces aspects ont été couverts de façon approfondie dans la section relative aux exigences en matière d'accès (sécurité physique) – SE 3.2.3.1 et 3.2.3.2.
- Établissement de règles claires concernant le périmètre des informations sur les contribuables accessibles par les employés, en fonction des besoins. Lorsqu'une demande d'informations porte sur un élément précis des affaires d'un contribuable, l'agent en charge du dossier doit accéder uniquement aux informations relatives à cet élément, et non à l'ensemble du dossier physique.
- Identification des documents classifiés confidentiels. Le mode d'accès ou de manipulation par les employés des documents identifiés ou estampillés « confidentiels » doit être défini dans une politique.

FIGURE 16. **Contrôles : la politique du bureau propre**



Politique du bureau propre

Les contrôles appliqués aux documents physiques ne se limitent pas à la gestion des documents papier : ils impliquent aussi une gestion et un contrôle efficaces de l'espace de travail.

Une politique du bureau propre définit de quelle manière les employés doivent ranger leur espace de travail lorsqu'ils s'absentent ou terminent leur journée. L'objectif est de garantir le respect du principe du besoin d'en connaître et d'empêcher l'accès par des utilisateurs non autorisés à des informations qu'ils ne sont pas censés voir. La politique du bureau propre limite l'exposition des informations aux employés sans droit d'accès, ainsi qu'aux tiers (par ex. : agents d'entretien ou de sécurité, réparateurs).

La politique du bureau propre prévoit par exemple l'obligation (voir Figure 16) :

- de retirer du bureau tout(e) information sensible, dossier, dispositif de stockage portable (clé USB, disque dur externe) lorsque l'employé s'absente de son bureau et en fin de journée ;
- de verrouiller les postes de travail en cas d'absence ou de les éteindre en fin de journée ;
- de ne pas écrire les mots de passe ;
- d'utiliser des tiroirs à clé, ou des casiers ou espaces de stockage séparés ;
- de conserver les clés en lieu sûr ;
- de détruire (déchiquetage) tout dossier sensible devenu inutile.

Le directeur du centre ou toute autre personne compétente peut avoir pour mission de vérifier les bureaux en fin de journée et de confisquer ou détruire tout dossier, document papier ou support de stockage portable qu'un employé aurait laissé sur son bureau.

Pour être effective, une politique du bureau propre (à l'instar de n'importe quelle politique de sécurité ou de confidentialité) requiert la forme écrite et doit être communiquée aux employés.

Contrôles sur les imprimantes

Le personnel peut être amené à imprimer des informations sensibles. Une fois ces données imprimées, à défaut de contrôles adéquats, l'efficacité des contrôles d'accès logique risque d'être compromise (voir SE 3.2.3.3 et 3.2.3.4 pour les contrôles régissant l'accès logique). Les contrôles sur les imprimantes peuvent inclure :

- La possibilité ou non d'imprimer l'information, le cas échéant en application de règles d'impression codées.
- Si une information sensible est imprimée, la mise en place d'instructions d'utilisation claires et de mentions de confidentialité, par exemple dans l'en-tête/le pied de page ou en filigrane dans le document imprimé.
- Des contrôles permettant de limiter le risque qu'une personne non autorisée récupère le document dans l'imprimante, par exemple en appliquant des contrôles de proximité (l'utilisateur prévu ou autorisé peut effectuer l'impression uniquement s'il est physiquement présent à la machine).
- Le nettoyage ou encodage de la mémoire de stockage de l'imprimante. Les imprimantes possèdent une mémoire de stockage. À défaut de contrôles adéquats, les imprimantes louées pourraient être restituées avec, en mémoire, le contenu des documents imprimés.

Contrôles au niveau du stockage des documents papier « au repos »

Lorsque des documents papier ne sont pas en cours d'utilisation (ils sont stockés ou « au repos »), les administrations fiscales peuvent envisager la mise en place des contrôles suivants :

- Le stockage dans des coffres, des pièces ou des unités de stockage verrouillé(e)s. Les armoires ou coffres doivent être fixes et verrouillés en permanence. L'accès aux clés doit être limité aux seuls employés autorisés. L'utilisation d'armoires multi-verrous est recommandée pour les informations classifiées et sensibles. Toutefois, un accès aux locaux suffisamment sécurisé peut compenser le manque de contrôles par verrouillage.
- L'utilisation de lieux de stockage séparés pour les dossiers de contribuables et autres informations sensibles. Ici, les contrôles de sécurité doivent limiter l'accès aux seuls employés ayant un intérêt professionnel légitime (e.g. utilisation d'un agent de sécurité surveillant l'entrée du lieu de stockage et autorisant l'accès uniquement au personnel autorisé muni d'un identifiant avec photo ; d'un code d'accès ; d'une identification biométrique ; ou de la vidéosurveillance).
- Des inventaires de tous les documents stockés.

L'encadré 31 contient un exemple de contrôles pour les documents papier.

La liste complète des contrôles applicables peut prendre la forme d'une ou de plusieurs matrices, en fonction des différentes classifications de l'information ainsi que de l'ampleur et de la complexité de l'information détenue par une administration fiscale. Le tableau 22 présente un exemple simplifié de matrice de contrôles applicables aux documents papier en fonction de leur classification et de leur niveau de confidentialité.

Cette matrice est fournie à titre d'illustration uniquement et les exemples de contrôle suivent leur l'ordre de présentation de cette boîte à outils. Les administrations fiscales sont encouragées à élaborer des matrices adaptées à leurs propres critères de classification de l'information et procédures organisationnelles.

Contrôles appliqués à la protection de l'information numérique

Les données détenues numériquement, lorsqu'elles sont utilisées, peuvent transiter sur les messageries électroniques du personnel ou entre différents systèmes

Tableau 22. **Exemple de matrice de contrôles pour les informations papier conformément au niveau de confidentialité**

1 – Publique	2 – À usage interne	3 – Confidentielle	4 – Hautement confidentielle
• Aucune identification obligatoire.	• Identifiée « À usage interne uniquement ».	• Identifiée « Confidentielle ».	• Identifiée « Hautement confidentielle ».
• Aucune restriction d'accès ni stockage spécifique obligatoire. Peut être placée dans un tiroir ou une armoire non verrouillé(e).	• Accès restreint à certains groupes ou services spécifiques. • Doit être placée dans un tiroir ou une armoire verrouillé(e).	• Accès limité à certaines personnes, selon le principe du besoin d'en connaître. • Doit être stockée dans une armoire verrouillée ou une pièce accessible uniquement au personnel autorisé.	• Accès limité à certaines personnes, selon le principe du besoin d'en connaître. • Doit être placée dans une armoire fixe munie de cadenas haute sécurité, située dans une pièce sécurisée accessible uniquement au personnel autorisé. • Présence d'agents de sécurité et vidéosurveillance si le stockage est prévu dans des pièces sécurisés.
• Aucune restriction sur la copie et l'impression. • Peut être laissée sans surveillance sur un bureau ou une imprimante.	• Peut être copiée et imprimée uniquement par les groupes ou services autorisés. • Ne peut pas être laissée sans surveillance sur un bureau ou une imprimante.	• Peut être copié et imprimé uniquement par les personnes autorisées. • Lors de la copie ou impression, ne doit pas être laissée sans surveillance sur le bureau ou l'imprimante.	• Peut être copiée et imprimée uniquement par les personnes autorisées, avec l'autorisation d'un supérieur hiérarchique, donnée au cas par cas. • Lors de la copie ou impression, ne doit pas être laissée sans surveillance sur le bureau ou l'imprimante. • Toutes les copies doivent être numérotées et consignées.
• Peut être jetée avec les autres déchets papier.	• Déchiquetage après utilisation.	• Déchiquetage après utilisation.	• Déchiquetage (micro-coupe ou coupe transversale) après utilisation.

Encadré 31. **Exemple de contrôles pour les documents papier**

Dans la juridiction A, toutes les informations confidentielles de l'administration fiscale, par exemple les informations sur les contribuables, sont clairement identifiées comme étant « confidentielles ».

L'accès aux documents papier confidentiels est limité aux personnes ayant besoin d'en connaître. Ces documents doivent être stockés dans des armoires verrouillées ou dans une pièce accessible uniquement au personnel autorisé. Les informations confidentielles peuvent être copiées et imprimées uniquement par les personnes autorisées. Lorsqu'un employé s'absente de son bureau, les copies papier de ces informations confidentielles doivent être rangées dans les tiroirs du bureau, fermés à clé. Toutes les informations confidentielles doivent être détruites (déchiquetage) après utilisation.

Tous les ordinateurs doivent être éteints en fin de journée. Le dernier agent à quitter les bureaux de l'administration fiscale en fin de journée doit vérifier tous les bureaux et éteindre tous les appareils encore en veille et supprimer tous les documents encore présents dans le photocopieur/l'imprimante. Les contrôles de la politique du bureau propre et les contrôles sur les imprimantes sont clairement exposés dans la Politique relative à la sécurité de l'information de l'administration. Des sanctions s'appliqueront en cas de non-respect.

Les informations échangées reçus au format papier sont séparées des autres informations sur les contribuables reçues par voie numérique et les dossiers sont conservés dans une pièce de stockage sécurisée, accessible uniquement au personnel de l'unité d'échange de renseignements ayant besoin d'en connaître. Les informations échangées doivent être systématiquement replacées dans la pièce de stockage en fin de journée et tous les accès consignés. L'accès à la salle des dossiers est activé avec l'identifiant électronique de l'agent autorisé.

d'information ou juridictions (par ex. : données en matière d'échange de renseignements). Le personnel peut aussi utiliser les données sur des supports amovibles. Une information numérique peut aussi être « au repos », stockée dans une base de données du centre de données ou enregistrée sur un serveur de fichiers.

Une violation de données fiscales numériques (e.g. données d'EAR) pourrait avoir des conséquences graves. Les contrôles de droit d'accès sont donc très importants et doivent, si possible, être basés sur le risque. Les contrôles spécifiques incluent :

- Chiffrement.
- Contrôles de domaine.
- Contrôles des points de terminaison (postes de travail), supports amovibles et périphériques.
- Politique d'utilisation acceptable.
- Renforcement des serveurs et ordinateurs.
- Contrôles relatifs à l'utilisation d'internet et des réseaux sociaux.

Ces contrôles s'apparentent à ceux décrits à la SE 3.2.4.2. Ces derniers se rapportent toutefois aux contrôles de sécurité du système d'information principal déployés dans l'environnement et la structure informatiques, tandis que ceux décrits dans cette section s'appliquent aux données elles-mêmes.

Chiffrement

Les données sont davantage exposées à un accès non autorisé lorsqu'elles sont en mouvement. Les normes internationales prévoient le chiffrement des données confidentielles lorsqu'elles sont utilisées et déplacées d'un point à un autre, par exemple entre deux systèmes d'information ou par courriel ou sur un support amovible.

Lorsque les données sensibles sont « au repos » (base de données), leur chiffrement n'est pas nécessaire si d'autres protections adéquates sont mises en œuvre pour garantir leur non-compromission. Ces protections peuvent prendre la forme de contrôles de domaine, décrits à la section suivante.

Lorsqu'elles décident de chiffrer des données « au repos », les administrations fiscales doivent prendre en compte les éléments suivants :

- **Analyse des risques**. L'approche doit être basée sur le risque et implique une parfaite appréhension des menaces.
- **Performance des données**. Le chiffrement peut nuire à la performance, par exemple retarder l'affichage des données ; il y a donc un compromis entre confidentialité et disponibilité. Toutefois, l'administration fiscale peut juger ce retard acceptable pour une information hautement sensible et si elle estime son intégrité menacée.

Correctement exécuté, le chiffrement protège parfaitement les données. Cependant, même si le chiffrement concerne des données « au repos », il convient d'appliquer des contrôles de domaine complémentaires aux bases de données, y compris des tests d'intrusion pour les systèmes et applications.

Certains contrôles de chiffrement recommandés sont présentés dans l'encadré 32 :

Encadré 32. **Contrôles de chiffrement pour les données numériques « en mouvement » et « au repos »**

Données en mouvement

- Contrôles permettant la transmission de l'information via des applications web (par ex. : portails de contribuables), comme Transport Layer Security (TLS) ou Hypertext Transfer Protocol Secure (HTTPS).
- Contrôles permettant la transmission de l'information durant les échanges numériques (par ex. : vidéoconférences, messagerie mobile), comme le chiffrement de bout en bout.
- Contrôles permettant la transmission de l'information par courriel, comme StarTLS.

Données au repos

- Contrôles permettant de prévenir la violation de données détenues dans des bases de données, comme les standards de chiffrement symétrique.

Contrôles de domaine

À l'instar de l'information papier, que l'on protège généralement en la plaçant dans un lieu unique (par ex. : coffre), les données numériques sont stockées dans des bases de données centralisées, dont l'accès est géré par des serveurs. Les administrations fiscales doivent protéger de façon adéquate ces bases de données et serveurs afin de garantir la non-compromission des données sensibles et confidentielles. Ces protections sont appelées « contrôles de domaine ».

Ces contrôles sont décrits de manière approfondie à la SE 3.2.4.2 relative à l'environnement de sécurité du système d'information dans son ensemble et à la SE 3.2.6 relative à la gestion des opérations (journalisation et vérification). En général, ils incluent :

- Ségrégation des environnements d'infrastructure.
- Pare-feu et antivirus.
- Contrôles d'accès renforcés, comme l'authentification multiple, l'authentification unique et l'accès limité dans le temps, notamment pour les comptes avec privilège.
- Renforcement du système d'exploitation, notamment par la désactivation des ports.
- Journalisation et vérification renforcées.
- Scan et audit des vulnérabilités.

Renforcement des ordinateurs, maintenance logicielle

La protection de l'information numérique implique aussi des contrôles au niveau des ordinateurs et de tout l'éventail des applications logicielles utilisées par le personnel. Cette protection se traduit par un renforcement des ordinateurs et une maintenance logicielle. Ces contrôles s'appliquant non seulement aux données gérées par les ordinateurs et applications logicielles mais aussi à la sécurité de tout l'environnement informatique de l'administration fiscale, ils sont traités de manière approfondie à la SE 3.2.4.2 sur les contrôles de sécurité informatique.

Points de terminaison, supports amovibles et périphériques

Cette partie concerne les contrôles des appareils utilisés par les utilisateurs finaux au niveau du bureau, notamment :

- Points de terminaison, par ex. ordinateurs personnels et ordinateurs portables.
- Supports amovibles, par ex. clés USB ou disques durs externes.
- Périphériques, par ex. souris, clavier, webcam.

Si ces appareils ont accès aux données sensibles et qu'ils sont mobiles, alors des contrôles doivent être appliqués. Ces contrôles incluent généralement :

- Chiffrement des clés USB.
- Effacement des informations sensibles transférées sur le support amovible, lorsque l'objectif du transfert est accompli.
- Utilisation d'un client de sécurité pour les points de terminaison.
- Systèmes d'alerte en cas d'utilisation de périphériques non approuvés.
- Systèmes de prévention des fuites de données.

Utilisation d'internet, des réseaux sociaux et de la messagerie électronique

Le social hacking (piratage social) est une méthode utilisée pour accéder de façon illicite aux données numériques. Les pirates peuvent chercher à violer des données en envoyant des courriels de phishing (hameçonnage) au personnel de l'administration fiscale dans le but de propager des logiciels malveillants via ses réseaux. Ces logiciels pourraient aussi pénétrer les systèmes de l'administration fiscale via les plateformes ou réseaux sociaux.

Si un œil averti peut facilement repérer un courriel de phishing basique (souvent rudimentaire), les pirates ont aussi recours à la technique du social engineering (ingénierie sociale) pour obtenir des informations sur des personnes – le but ultime étant de lancer des attaques plus sophistiquées, parfois appelées spear phishing (harponnage). Ces attaques s'inspirent souvent du contenu des courriels internes, ce qui les rend d'autant plus difficiles à repérer. Les adresses électroniques des agences gouvernementales suivent souvent un format standard. Les pirates les plus habiles n'ont donc aucune difficulté à contourner les contrôles formels.

En définitive, ce sont donc les humains qui contrôlent l'utilisation de l'équipement informatique. D'où la nécessité pour les employés de bien comprendre ce qu'ils ont le droit (ou l'interdiction) de faire lorsqu'ils utilisent un point de terminaison, un support amovible, un périphérique, internet ou un réseau social. La capacité d'une administration fiscale à gérer correctement l'équipement et les services qui contiennent les informations dépend donc, avant toute chose, de l'adhésion de ses employés à sa politique de sécurité. Cette adhésion est généralement obtenue en déployant une politique d'utilisation acceptable (PUA).

Les administrations fiscales peuvent faire le choix d'adopter ce type de règles ou de ne pas s'exposer aux risques, par exemple en interdisant l'utilisation des supports amovibles, de la messagerie personnelle et des plateformes ou réseaux sociaux. Dans les faits, les administrations fiscales n'exercent qu'un contrôle et une influence limités sur les employés. Si l'option des PUA est retenue, il est donc primordial de prévoir une formation aux risques liés à l'utilisation des supports amovibles, d'internet et des réseaux sociaux, ainsi que des campagnes de sensibilisation, afin de garantir une mise en œuvre efficace de ces règles. Mieux vaut anticiper en formant le personnel qu'appliquer des sanctions disciplinaires a posteriori.

Quelques éléments spécifiques à intégrer dans la PUA :

- Partir du principe qu'un courriel est toujours une menace, sauf si l'on est certain de son authenticité. Un courriel est considéré comme authentique s'il est attendu et que son expéditeur et l'adresse de celui-ci sont connues et authentiques.
- Ne jamais ouvrir de pièces jointes, sauf si elles sont considérées comme authentiques. Vérifier si nécessaire auprès de l'expéditeur avant ouverture.
- Ne jamais cliquer sur un lien. Si un lien est jugé pertinent, il est recommandé à l'employé de se connecter au site web de l'organisation en question pour accéder au lien via la page d'accueil.

Encadré 33. **Principes suggérés pour la définition d'une politique d'utilisation acceptable (PUA)**

Quelle que soit la finalité des PUA (utilisation des supports amovibles ou des réseaux sociaux), les administrations fiscales doivent tenir compte des considérations suivantes :

- **Champ d'application et justification**. Avant toute chose, il est important d'expliquer ce qui justifie l'élaboration de telles règles, à savoir la protection de l'information et le droit des contribuables au respect de la vie privée. Mieux l'utilisateur comprendra la finalité de ces règles, plus il sera disposé à les respecter et à collaborer à leur mise en œuvre.
- **Droits et responsabilités des utilisateurs**. Les PUA définissent en général les droits et les responsabilités du personnel, notamment lorsqu'il s'agit de garantir la protection de l'information.
- **Utilisations acceptables**. Dans la mesure du possible, ces PUA doivent prendre en compte les besoins des employés, par exemple la nécessité d'effectuer des recherches sur internet dans un cadre professionnel ou même de gérer des urgences personnelles. Si ces PUA autorisent une utilisation non professionnelle, elles doivent définir ce que recouvre cette utilisation et préciser les circonstances dans lesquelles elle est autorisée.
- **Utilisations interdites**. L'utilisation d'internet et des réseaux sociaux, par exemple, peut inclure des recherches spécifiques sur internet, le téléchargement de contenus, la navigation et la publication de commentaires. En général, les PUA interdisent l'utilisation ou le contenu illégal, préjudiciable ou offensant, ainsi que les pratiques totalement illicites comme les manœuvres frauduleuses, le phishing, le contenu injurieux ou haineux, l'introduction de virus, la violation du droit d'auteur ou du droit de propriété intellectuelle, l'atteinte à la vie privée, la calomnie et la diffamation, l'accès aux systèmes sans autorisation, l'utilisation au-delà des droits accordés, l'extraction de listes de diffusion et l'envoi de courriels indésirables (spams).
- **Normes de confidentialité**. Les PUA doivent intégrer des clauses de confidentialité et d'utilisation responsable des données. Elles peuvent définir quels sont les types de données sensibles et pourquoi, et préciser les conditions d'accès et d'utilisation de ces données.
- **Sanctions**. Les PUA doivent indiquer les possibles violations et conséquences liées au non-respect de leurs clauses.

Encadré 34. **Exemple de contrôles appliqués à l'information numérique**

Dans la Juridiction B, l'information confidentielle détenue numériquement par l'administration fiscale peut uniquement être transmise après chiffrement. Les données confidentielles, y compris les renseignements échangés, peuvent uniquement être envoyées à un domaine de messagerie de l'administration fiscale de B ou transmises par les personnes autorisées à des adresses de messagerie externes fiables en appliquant une technologie de chiffrement de bout en bout.

L'accès logique à l'information confidentielle est limité aux personnes ayant besoin d'en connaître et les droits d'accès des utilisateurs et administrateurs sont limités par l'authentification multiple.

Les données sensibles ne sont consultables que sur les appareils autorisés de l'administration fiscale. La PUA inclue une liste de tous les dispositifs de stockage portables dont l'utilisation est autorisée par l'administration fiscale. Les supports amovibles contenant des informations confidentielles doivent être rangés dans des tiroirs ou armoires fixes munis de cadenas haute sécurité ou dans une pièce accessible uniquement au personnel autorisé. Une équipe dédiée au sein du service informatique contrôle régulièrement l'usage par le personnel des points de terminaison, supports de stockage portables et périphériques.

L'information numérique confidentielle peut être imprimée uniquement avec l'autorisation d'un supérieur hiérarchique, doit porter la mention « Confidentielle » en filigrane et ne doit pas être laissée sans surveillance après impression.

L'information confidentielle est protégée grâce au déploiement de systèmes DLP et de protections aux points de terminaison. L'utilisation des réseaux sociaux et d'internet est bloquée dans l'unité d'échange de renseignements ; les procédures et sanctions correspondantes sont énoncées dans les PUA.

- Toujours tenir compte des notifications de l'antivirus.
- Toujours faire attention à ce que les employés publient sur les réseaux sociaux.
- Même si l'administration fiscale n'autorise pas l'utilisation des réseaux sociaux pendant les heures de travail, il peut s'avérer utile d'insister sur les risques associés.
- Seuls doivent être utilisés les appareils approuvés et mis à disposition par l'administration fiscale. Ces appareils doivent être cryptés, comme le prévoient les politiques de classification des données de l'administration fiscale.
- Leur utilisation doit être strictement limitée à l'usage prévu par ces politiques.

L'encadré 33 énonce quelques principes utiles pour la définition d'une PUA.

Les PUA doivent être communiquées aux employés dans le cadre de leur processus d'intégration et des campagnes de formation et de sensibilisation du personnel. Elles font partie des contrôles sur les ressources humaines décrits à la SE 3.2.2.

Il est important également de surveiller les activités des employés et que les cadres participent à cette surveillance et à la mise en œuvre de ces règles. Il existe deux niveaux de contrôle :

- Les cadres mettent l'accent sur l'importance de la sécurité, y compris en ce qui concerne l'utilisation de l'équipement de travail, et adoptent une attitude exemplaire.
- Les équipes de sécurité procèdent à des vérifications ponctuelles.

Comme pour l'information papier, les contrôles applicables à l'information numérique peuvent être présentés sous forme d'une ou de plusieurs matrices. Le tableau 23 présente un exemple simplifié de matrice conformément au niveau de confidentialité de l'information numérique. L'encadré 34 donne quelques exemples de contrôles appliqués dans une administration fiscale.

Étape 3. Contrôles appliqués lorsque l'information n'est plus nécessaire : périodes de conservation et destruction

Cette section traite de la dernière partie du cycle de vie de l'information, lorsqu'elle n'est plus utile à l'administration fiscale et doit être éliminée.

Une bonne pratique en matière de sécurité de l'information consiste à détruire ce type d'information. La détention d'une information, et notamment d'une information sensible, comporte par essence des risques. En général, ce risque est proportionnel à la sensibilité de cette information et à la période pendant laquelle elle est détenue.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Tableau 23. **Exemple de matrice de contrôles pour l'information numérique conformément au niveau de confidentialité**

1 – Publique	2 – À usage interne	3 – Confidentielle	4 – Hautement confidentielle
• Aucun chiffrement. • Peut être envoyée par courriel entre employés et stockée sur un appareil mobile en interne.	• Aucun chiffrement. • Peut être envoyée par courriel entre employés d'un même groupe ou service.	• Chiffrement obligatoire pour la transmission. • Peut être envoyée par courriel ou transférée uniquement après chiffrement, par les personnes autorisées.	• Chiffrement obligatoire pour la transmission. • Peut être envoyée par courriel ou transférée uniquement après chiffrement, par les personnes autorisées, avec l'autorisation d'un supérieur hiérarchique, donnée au cas par cas.
• Aucune restriction sur l'accès logique.	• Accès logique limité à certains groupes ou services.	• Accès logique limité à certaines personnes, selon le principe du besoin d'en connaître. • Les droits d'accès des utilisateurs et administrateurs sont limités par l'authentification multiple.	• Accès logique limité à certaines personnes, selon le principe du besoin d'en connaître. • Les droits d'accès des utilisateurs et administrateurs sont limités par l'authentification multiple.
• S/O	• S/O	• Bases de données séparées des autres informations. • Conservée sur des serveurs sécurisés protégés par pare-feu, antivirus et mot de passe.	• Bases de données séparées des autres informations. • Conservée sur des serveurs sécurisés protégés par pare-feu, antivirus et mot de passe.
• Peut être détenue sur des appareils mobiles. • Les supports amovibles contenant ce type d'information peuvent être rangés dans des tiroirs ou armoires non verrouillés.	• Peut être détenue sur des appareils mobiles au sein d'un groupe ou service. • Les supports amovibles contenant ce type d'information doivent être rangés dans des tiroirs ou armoires verrouillés.	• Peut être détenue sur des supports amovibles uniquement après chiffrement. • Les supports amovibles contenant ce type d'information doivent être rangés dans des tiroirs ou armoires verrouillés ou dans une pièce accessible uniquement au personnel autorisé.	• Peut être détenue sur des supports amovibles autorisés uniquement avec l'autorisation d'un supérieur hiérarchique. • Les supports amovibles contenant ce type d'information doivent être rangés dans des armoires fixes munies de cadenas haute sécurité ou dans une pièce accessible uniquement au personnel autorisé ayant besoin d'en connaître. • Utilisation de systèmes de protection des points de terminaison et supports amovibles. • Utilisation de systèmes DLP.
• Aucune restriction d'impression.	• Peut être imprimée, avec la mention « À usage interne uniquement » en filigrane, et ne doit pas être laissée sans surveillance après impression.	• Peut être imprimée, avec la mention « Confidentielle » en filigrane, et ne doit pas être laissée sans surveillance après impression.	• Peut être imprimée uniquement avec l'autorisation d'un supérieur hiérarchique, donnée au cas par cas.

Si une information sensible est utile, alors l'intérêt de la conserver l'emporte sur le risque. Si cette information n'a plus de réelle valeur, il est d'usage de la détruire pour éliminer tout risque potentiel. Il se peut néanmoins que les administrations fiscales aient l'obligation légale de conserver cette information pour une période prédéfinie, même si elle n'a plus d'utilité.

Les administrations fiscales doivent définir clairement leur politique de destruction de l'information, par référence aux périodes de conservation et aux exigences applicables en matière de destruction des documents (papier comme numériques). La politique doit définir :

- Les différents types de documents détenus par l'administration fiscale.
- La classification des documents par niveau de sécurité.
- Les raisons de la conservation des documents.
- La durée obligatoire de conservation des documents.
- Les mécanismes de conservation.
- Les méthodes et procédures de nettoyage ou destruction.

Cette politique doit prévoir des procédures d'évaluation permettant de s'assurer, tout au long du cycle de vie des documents, que ces derniers sont toujours utiles et utilisés et, lorsque tel n'est plus le cas, un plan d'action pour leur élimination.

Le fait que l'information ne soit plus utile ne signifie pas pour autant qu'elle doit être systématiquement détruite. La politique peut prévoir une procédure d'évaluation avant destruction ou élimination.

Si la décision est prise de conserver cette information ou de la détruire, il convient de tenir un registre précisant :

- quelle est l'information conservée ou détruite ;
- le motif de sa conservation ou destruction ;
- la date de la prochaine évaluation, si l'information est conservée.

La décision de conserver ou détruire l'information doit être prise par un supérieur hiérarchique ou le responsable de l'information (personne responsable de l'activité de l'administration fiscale concernée ou du type d'information considéré).

Périodes de conservation

Si les règles de bonne pratique exigent en général qu'une information inutile soit détruite, il se peut que l'administration fiscale ait l'obligation légale de la conserver pendant une durée prédéterminée, même si l'information n'a plus d'utilité d'un point de vue fiscal. Dans certain cas, cette durée est illimitée. Parfois, l'administration fiscale a l'obligation de transférer une partie des informations sur les contribuables aux archives nationales.

Lorsqu'il existe un délai légal de conservation, l'administration fiscale doit évaluer le risque lié à la détention de cette information et prendre les mesures adéquates pour ramener ce risque à un niveau acceptable. Il est important que le responsable de l'information assume la responsabilité de ce risque et veille à la mise en œuvre effective de ces mesures d'atténuation. Ces mesures incluent, notamment :

Documents papier

- **Tri ou élimination**. Conserver uniquement les documents papier dont la conservation est strictement obligatoire.
- **Stockage sécurisé**. Les documents papier qui sont encore régulièrement consultés peuvent être conservés dans un lieu conçu pour en faciliter l'accès. Les documents devenus inutiles peuvent être archivés dans un lieu davantage sécurisé.
- **Numérisation des documents papier et stockage des copies électroniques hors ligne**. Cette mesure s'applique uniquement s'il n'existe aucune raison légale ou judiciaire de conserver la version papier. Certaines juridictions refusent la preuve numérique et imposent la présentation du document original dans les procédures judiciaires. Par conséquent, il est important de définir si la loi de la juridiction concernée prévoit cette obligation et, le cas échéant, de conserver le document papier original.

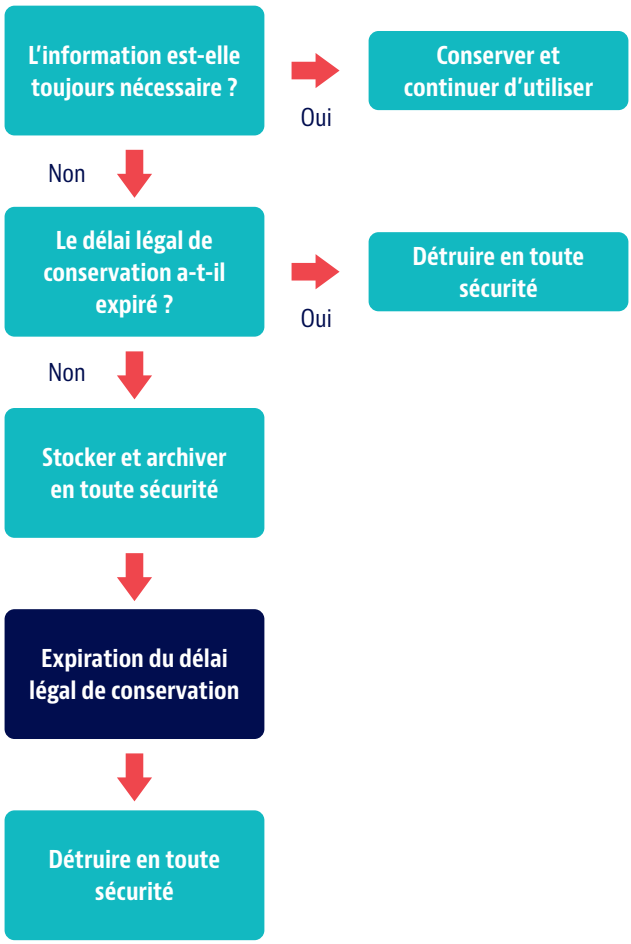
Documents numériques :

- **Chiffrement des données**. Le chiffrement peut limiter le risque lié à la conservation de l'information.
- **Déplacement de jeux de données plus anciens vers un stockage hors ligne**. Avec un stockage hors ligne, le dispositif de stockage n'est pas connecté à l'environnement d'exploitation, mais il peut l'être si nécessaire. Il peut s'agir d'une base de données séparée ou d'un support amovible, par exemple un disque dur externe. Il est important que cette base de

données ou ce support soit stocké en toute sécurité et régulièrement contrôlé.

Les administrations fiscales doivent maintenir des registres appropriés de tous les documents, physiques ou numériques, qui sont conservés. Voir la figure 17 pour un exemple de procédure de conservation et de destruction de l'information.

FIGURE 17. **Exemple de procédure de conservation et de destruction de l'information**



Élimination sécurisée de l'information

Les administrations fiscales doivent utiliser des méthodes de destruction ou de nettoyage proportionnelles au niveau de sensibilité de l'information. Ces méthodes doivent garantir l'impossibilité pour une personne de récupérer des éléments de donnée après destruction ou nettoyage. Des procédures claires doivent également permettre de déterminer les critères d'identification et de sélection de l'information (ou du support contenant l'information) nettoyée ou détruite.

S'agissant d'informations détenues par des tiers ou prestataires externes, les administrations fiscales doivent en outre définir les conditions de la destruction/élimination et intégrer celles-ci dans les contrats ou accord de niveau de service.

Encadré 35. **Nettoyage des supports de stockage - Pourquoi est-ce important ?**

Il s'agit du processus de traitement de données conservées sur un support de stockage et permettant de réduire le risque de récupération et de reconstruction à un niveau acceptable. Certaines formes de nettoyage permettront aux administrations fiscales de réutiliser le support. D'autres en revanche sont par nature destructives et rendront le support inutilisable.

À quel moment nettoyer le support ?

Les administrations fiscales peuvent être amenées à envisager un nettoyage des supports de stockage dans plusieurs cas :

- Réutilisation : un dispositif est affecté à un autre utilisateur ou d'autres fins au sein de l'administration fiscale.
- Réparation : un dispositif défectueux est renvoyé au fournisseur pour être réparé ou remplacé.
- Élimination ou destruction : nettoyage des supports non désirés avant leur élimination ou leur destruction, en particulier si l'administration fiscale a passé un contrat avec un tiers pour l'élimination ou la destruction du matériel.

Dans tous les cas, le support est sorti de son environnement d'exploitation habituel ; il est donc accessible à d'autres utilisateurs (des tiers ou des personnes/organisations jugées moins fiables) et davantage exposé au risque.

Les risques en l'absence de nettoyage

Si le support de stockage n'est pas correctement nettoyé, certaines données sensibles risquent d'être encore accessibles, avec pour conséquences :

- l'impossibilité de localiser certaines données sensibles et la perte de contrôle sur ces informations ;
- la possibilité que des données relatives aux contribuables soit récupérées et utilisées à des fins de fraude ou d'usurpation d'identité.

Source : www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

Les méthodes de destruction ou nettoyage de l'information incluent :

Documents papier

En règle générale, les documents papier sont déchiquetés et/ou incinérés. Plusieurs niveaux de déchiquetage peuvent être envisagés (zone et largeur des morceaux) en fonction de la classification du document.

Supports magnétiques

Le traitement et l'élimination des informations d'un support magnétique doivent toujours tenir compte des données les plus sensibles qu'il a pu contenir. Un support non réutilisé (par ex. : clés USB, disques SSD, disques durs et autres disques) doit être détruit (broyé) dans un équipement spécialisé jusqu'au stade où plus aucun élément n'est exploitable.

Si le support n'est pas détruit mais réutilisé en interne, il convient de prendre des mesures appropriées pour supprimer les informations existantes avant sa réutilisation, ou nettoyer le support. Un support amovible incorrectement nettoyé pourrait compromettre la sécurité des données sensibles en la rendant accessible à des utilisateurs non autorisés. L'encadré 35 illustre l'importance du nettoyage des supports de stockage. Les administrations fiscales peuvent opter pour différentes méthodes, par exemple l'écrasement des données, ou se reporter aux normes internationales sur le nettoyage des supports amovibles pour plus d'information.

Il peut s'avérer difficile de supprimer toute trace de données sur un disque. Par conséquent, il est généralement déconseillé de réutiliser un disque ayant contenu des informations hautement confidentielles. En tout état de cause, il est recommandé aux administrations fiscales de conserver des registres contenant l'historique d'utilisation de chaque dispositif. Voir l'inventaire des actifs (SE 3.2.4.3 relatif aux contrôles de gestion des actifs).

L'encadré 36 contient des exemples de procédures de destruction.

Sous-exigence 3.2.5.2. Protection des renseignements échangés

Cette section couvre les mesures prises pour mettre en pratique les clauses de confidentialité et d'utilisation appropriée contenues dans les accords internationaux d'échange de renseignements et dans les législations nationales applicables en la matière (voir EF 3.1).

Encadré 36. **Exemple de procédures de destruction sécurisée de l'information confidentielle devenue inutile**

Dans la juridiction C, l'administration fiscale entreprend une opération massive de destruction des documents physiques et numériques au minimum une fois par an ou dès lors que la quantité de documents accumulée le justifie. Elle a recours aux services d'un prestataire qui assure le déchiquetage (micro-coupe ou coupe transversale) et/ou broyage au moyen d'un équipement spécialisé. Ce processus est décrit dans une procédure de destruction et d'élimination des informations officielles de l'administration fiscale :

- Le document (support papier ou magnétique) est consigné dans un journal des documents à détruire. Ce journal permet de suivre les documents jusqu'à leur destruction effective et de consigner la vérification et validation de l'opération par le personnel désigné par l'administration fiscale, nommé par un supérieur hiérarchique.
- Les documents sont transportés en toute sécurité vers le site concerné pour y être stockés en toute sécurité jusqu'à leur destruction. Ce journal indique l'emplacement actuel du document en attente de destruction et l'identité de la personne responsable du document au moment considéré. Cette personne a la responsabilité de veiller à ce que le document soit stocké en toute sécurité, en procédant aux contrôles appropriés.
- Lorsqu'un document doit être physiquement détruit et qu'il s'écoule un certain délai avant cette opération, le support de stockage est d'abord nettoyé en toute sécurité, puis stocké en préparation de la destruction.
- Une liste détaillant tous les documents concernés est établi en amont de la destruction. Une copie est envoyée à un témoin indépendant, qui donne son aval pour la destruction. Ce témoin est présent tout au long du processus de destruction, d'abord pour vérifier la liste à mesure que chaque élément est retiré du lieu/support de stockage sécurisé, puis pour contrôler que chaque élément est détruit conformément à la procédure, et enfin pour confirmer la destruction effective de tous les éléments listés.

Cadre de gestion de la sécurité de l'information conforme aux normes et bonnes pratiques reconnues internationalement (Exigence fondamentale 3.2)

Pour protéger les renseignements échangés, les administrations fiscales peuvent :

- leur appliquer les politiques et pratiques définies pour garantir la confidentialité à des fins fiscales nationales, par exemple en utilisant les types de contrôles décrits à la SE 3.2.5.1 ;
- élaborer des politiques et pratiques renforcées et sur mesure. Ces politiques sont parfois intégrées dans le manuel d'échange de renseignements. Elles incluent généralement :
  - Classification en fonction du niveau de confidentialité et identification des renseignements échangés.
  - Contrôles de l'accès aux dossiers d'échange de renseignements numériques et physiques.
  - Transmission sécurisée de renseignements aux autorités compétentes étrangères.
  - Transmission sécurisée de renseignements en provenance d'institutions financières, dans le cas de la norme d'EAR.
  - Transmission sécurisée de renseignements en provenance de l'autorité compétente ou de l'unité d'échange de renseignements vers d'autres points de l'administration fiscale ou des tiers.

Classification et identification des renseignements échangés

Les renseignements échangés (envoyés ou reçus) doivent être classifiés confidentiels et clairement identifiés comme tels. Cette mention peut être tamponnée, pour les dossiers papier ou le courrier traditionnel, ou apparaître en filigrane dans la correspondance électronique (la mention précise que l'information a été échangée conformément à un accord international d'échange de renseignements et qu'elle est soumise à des restrictions particulières d'utilisation et de divulgation, décrites à l'EF 3.1).

Le libellé peut être le suivant :

« LES PRÉSENTS RENSEIGNEMENTS SONT COMMUNIQUÉS EN VERTU DES DISPOSITIONS D'UNE CONVENTION FISCALE ET LEUR UTILISATION COMME LEUR DIVULGATION SONT RÉGIES PAR LES DISPOSITIONS DE LADITE CONVENTION. »

Contrôles de l'accès aux dossiers d'échange de renseignements physiques et numériques reçus d'autorités compétentes étrangères

Ces contrôles peuvent inclure les restrictions suivantes :

- Seules les personnes expressément autorisées ont accès aux locaux de l'unité d'échange de renseignements, avec une identification personnelle (par ex. : une carte électronique ou un identifiant photo). Les autres employés ont accès à l'unité d'échange de renseignements uniquement avec l'autorisation du responsable de l'unité en question. Le public n'a en aucun cas accès à ces locaux.
- Les agents de l'unité d'échange de renseignements font l'objet d'une vérification renforcée de leurs antécédents professionnels avant toute prise de fonction, voire de contrôles de sécurité renforcés (voir SE 3.2.2 relative aux contrôles sur les ressources humaines). Le personnel informatique chargé de la gestion des bases de données contenant des renseignements échangés sont également soumis à des contrôles renforcés sur les ressources humaines.
- Une politique du bureau propre stricte s'applique à tous les renseignements échangés sous forme de documents papier ou sur appareils mobiles. Ces derniers doivent être stockés dans des tiroirs ou armoires verrouillés.
- Les copies papier de renseignements échangés peuvent être imprimées uniquement par les personnes autorisées au sein de l'unité d'échange de renseignements. Un tampon doit être apposé renvoyant à la convention et l'obligation de confidentialité.
- Les copies papier de renseignements échangés doivent être détruites (déchiquetage) en toute sécurité lorsqu'elles ne sont plus nécessaires.
- Des contrôles de domaine renforcés sont mis en place pour les bases de données contenant des renseignements échangés.
- L'accès aux systèmes et bases de données relatif à l'échange de renseignements est limité au personnel expressément autorisé, selon le principe du besoin d'en connaître (voir EF 3.2.3 sur la gestion des accès).
- Toutes les demandes d'information entrantes et toutes les informations reçues sont enregistrées dans un système de gestion de l'information interne, accessible uniquement au personnel autorisé sur saisie d'un identifiant et d'un mot de passe. Les accès sont journalisés et vérifiés (voir SE 3.2.6.2 sur la gestion des journaux).

Transmission sécurisée d'information aux autorités compétentes étrangères

La transmission est au cœur de l'échange de renseignements. Des contrôles spécifiques doivent s'appliquer lorsqu'une information est envoyée à une autorité compétente étrangère, ou reçue par celle-ci, qu'il s'agisse d'échange sur demande, automatique ou spontané.[17] Ces contrôles doivent être étendus à tous les documents, communications et informations contextuelles y afférents. Les contrôles suivants peuvent être envisagés :

- Pour l'échange de renseignements sur demande, s'assurer que l'interlocuteur étranger à l'origine de la demande est bien l'autorité compétente ou son représentant désigné en vertu de l'accord international d'échange de renseignements applicable (et donc autorisé à faire la demande et recevoir l'information) et s'assurer que les nom et adresse postale/électronique sont exacts avant toute communication de données.
- Sécuriser la transmission entre autorités compétentes, par exemple :
  - La transmission électronique, sur demande ou automatique, doit toujours être sécurisée par un niveau de chiffrement adéquat.
  - Seules les personnes autorisées à gérer des renseignements échangés doivent pouvoir accéder à la messagerie utilisée pour l'échange de renseignements, protégée par mot de passe.
  - La correspondance écrite doit être exclusivement envoyée par l'intermédiaire de systèmes postaux assurant un suivi international.
  - Le courrier reçu d'une autorité compétente étrangère doit être remis directement à l'unité d'échange de renseignements.
  - Le courrier d'accompagnement adressé à l'autorité compétente étrangère doit souligner la nature confidentielle de l'information, en incluant une référence aux clauses de restriction d'utilisation et de divulgation de la convention applicable (voir exemple ci-dessus).

Transmission sécurisée des informations relatives à l'EAR provenant d'institutions financières

La transmission électronique d'informations des institutions financières aux administrations fiscales, dans le cadre de la norme d'EAR, doit être convenablement chiffrée.

Des mécanismes doivent en outre être mis en place pour certifier et authentifier les institutions financières. Ces mécanismes prennent généralement la forme d'une authentification multiple et/ou d'une signature numérique.

Transmission sécurisée d'informations en provenance de l'autorité compétente ou de l'unité d'échange de renseignements vers d'autres secteurs de l'administration fiscale ou des tiers

L'autorité compétente ou l'unité d'échange de renseignements doit souvent communiquer des informations à d'autres agents ou autorités de l'administration fiscale ou à des tiers (par ex. : le ministère de la Justice). Il convient de tenir un registre permettant de déterminer à qui l'information a été divulguée, combien d'exemplaires des documents ont été tirés et qui en possède une copie à un moment donné.

Dans de nombreux cas, l'autorité compétente ou l'unité d'échange de renseignements reçoit de grandes quantités d'informations concernant de nombreux contribuables, et souvent, seule une partie de ces informations est nécessaire pour un vérificateur ou un agent de l'administration fiscale particulier dans une certaine région du pays. Il incombe au personnel de l'autorité compétente ou de l'unité d'échange de renseignements de s'assurer que seules les informations nécessaires sont communiquées aux agents concernés, et que l'on ne se contente pas de les transmettre en bloc.

Comme évoqué précédemment, les autorités compétentes utilisent des tampons et d'autres avertissements pour protéger la confidentialité des renseignements qu'elles échangent. Elles le font aussi lorsqu'elles communiquent ces renseignements au sein de l'administration fiscale. Elles indiquent que les renseignements sont confidentiels et qu'ils ont été obtenus aux termes d'une convention fiscale, et précisent parfois qu'ils ne doivent pas être divulgués en vertu de la législation sur la liberté d'information, ni sans avoir consulté l'autorité compétente au préalable. Il s'agit de se prémunir ainsi contre toute divulgation non autorisée.

Dans certains pays, l'avertissement figure en couverture du document, dans d'autres, il est reproduit sur chaque page pour le cas où les pages seraient dispersées. Quand l'accord d'échange de renseignements permet d'utiliser les renseignements à des fins non fiscales, les organismes chargés de l'application de la loi et les autorités judiciaires doivent les traiter confidentiellement, conformément aux dispositions de l'accord concerné (voir EF 3.1).

17. Pour de plus amples informations sur les politiques et pratiques nécessaires à la protection de la confidentialité des renseignements échangés, voir « Garantir la confidentialité : Le guide de l'OCDE sur la protection des échanges de renseignements à des fins fiscales », www.oecd.org/fr/fiscalite/echange-de-renseignements-fiscaux/rapport-garantir-la-confidentialite.pdf

Encadré 37. **Exemple de contrôles applicables aux renseignements échangés**

Dans la juridiction A, tout le personnel de l'administration fiscale qui traite des renseignements échangés possède une accréditation de sécurité et reçoit une formation à l'échange de renseignements. Les données d'échange de renseignements sont classifiées « Confidentielles ». Les contrôles de sécurité sont conformes à cette classification et toutes les informations au format physique ou numérique sont clairement identifiées comme étant « protégées par une convention ».

Les demandes d'échange de renseignements entrantes et sortantes sont gérées par l'équipe d'échange de renseignements sur demande et les échanges de renseignements en vertu de la norme d'EAR sont gérés par l'équipe d'EAR. Le manuel sur l'échange de renseignements guide les agents dans la gestion des demandes d'échange de renseignements entrantes et sortantes, ainsi que les EAR.

Les informations sur demande reçues sont séparées des autres informations sur les contribuables et sont accessibles uniquement selon le principe du besoin d'en connaître. Les informations reçues via le système d'EAR sont stockées séparément des autres bases de données relatives aux contribuables et accessibles aux administrateurs autorisés, selon le principe du besoin d'en connaître, par une authentification multifactorielle.

Les documents papier, dossiers et supports de stockage (par exemple, CD et clés USB) reçus des partenaires sont protégés par des mesures d'accès physique, mais aussi conservés en toute sécurité dans des armoires fixes multi-verrous dans les locaux des équipes en charge de l'échange de renseignements sur demande et de l'EAR.

Les informations envoyées aux partenaires par voie électronique sont systématiquement chiffrées.

En ce qui concerne les demandes de renseignements reçues des partenaires, seules les informations spécifiées dans le courrier de demande d'échange de renseignements sont divulguées et transférées aux centres des impôts locaux, afin de permettre aux vérificateurs fiscaux d'accéder à ces informations. Les vérificateurs fiscaux doivent confirmer par écrit que la confidentialité des données sera préservée et que celles-ci seront utilisées uniquement dans le respect de l'accord d'échange de renseignements correspondant. Les vérificateurs fiscaux sont en outre formés à l'utilisation du manuel sur l'échange de renseignements et aux procédures de gestion des renseignements échangés.

Lorsque des informations sont transférées aux centres des impôts locaux, elles sont accompagnées de l'avertissement suivant : « Toutes les informations reçues aux termes des dispositions sur l'échange de renseignements d'une convention ne peuvent être utilisées qu'à des fins fiscales et doivent être tenues strictement confidentielles. La divulgation de ces documents, y compris en vertu de la loi sur la protection de la vie privée ou de la loi sur la liberté de l'information, doit être discutée avec l'équipe d'échange de renseignements sur demande avant la divulgation. La section 1 du manuel d'échange de renseignements fournit de plus amples informations ».

Lorsqu'ils ne sont plus nécessaires à des fins professionnelles, les renseignements échangés sont archivés pendant 10 ans, délai à l'issue duquel ils sont détruits. Un employé désigné de l'administration fiscale est présent pendant l'intégralité du processus de destruction.

L'encadré 37 présente des exemples de contrôles (renforcés) applicables aux renseignements échangés.

SOUS-EXIGENCE 3.2.6 : CADRE DE GESTION DES OPÉRATIONS, NOTAMMENT GESTION DES INCIDENTS, GESTION DES CHANGEMENTS, SURVEILLANCE ET AUDIT

La SE 3.2.6 porte sur l'étape « contrôler » du cycle PDCA, c'est-à-dire les dispositions opérationnelles prises par les administrations fiscales pour s'assurer du bon fonctionnement du système de GSI et de ses contrôles.

Si les opérations de sécurité peuvent être très étendues, les évaluations de confidentialité en matière d'EAR portent plus spécifiquement sur certains des contrôles et processus critiques que les administrations fiscales sont supposées mettre en place, notamment dans le domaine informatique. Ces contrôles opérationnels couvrent les domaines suivants, en commençant par une présentation générale du cadre de gestion des opérations que les administrations fiscales ont déployé, puis des directives sur les contrôles à appliquer dans six domaines de la gestion des opérations :

- SE 3.2.6.1 : Cadre général de gestion des opérations.
- SE 3.2.6.2 : Gestion des journaux.
- SE 3.2.6.3 : Gestion du risque informatique.
- SE 3.2.6.4 : Gestion des vulnérabilités.
- SE 3.2.6.5 : Gestion des changements.
- SE 3.2.6.6 : Gestion des incidents.
- SE 3.2.6.7 : Audit interne et audit externe.

Le tableau 24 présente les définitions des principaux concepts abordés dans la SE 3.2.6.

Sous-exigence 3.2.6.1. Présentation générale du cadre de gestion des opérations de sécurité

Une coordination efficace des activités de sécurité opérationnelle est indispensable au bon fonctionnement des processus stratégiques, comme le système de GSI et la gestion des risques. L'administration fiscale doit avoir une visibilité sur les messages véhiculés par les processus opérationnels, notamment en ce qui concerne les contrôles de sécurité (y compris ceux qui protègent les renseignements échangés). La SE 3.2.6.1 exige donc que les administrations fiscales soient conscientes des contrôles qui protègent les informations échangées et qu'elles disposent de plans appropriés pour les gérer.

Tableau 24. **Définitions des principaux concepts**

Concept	Description
Audit	Vérification complète et objective permettant d'évaluer la conformité avec les processus définis dans les politiques et procédures relativement au système de GSI. Les résultats et conclusions de l'audit doivent être directement soumis au directeur de l'administration fiscale.
Centre des opérations de sécurité	Équipe d'experts et systèmes pour la surveillance et l'analyse permanentes de la sécurité de l'administration fiscale.
Gestion des changements	Gestion contrôlée du développement de nouveaux systèmes et services ainsi que des changements majeurs apportés aux systèmes et services existants.
Gestion des incidents	Identification, documentation et gestion des incidents de sécurité, dans les domaines informatique et non-informatique.
Gestion des journaux	Politiques et processus collectifs utilisés pour administrer et faciliter la création, la transmission, l'analyse, le stockage, l'archivage et l'élimination finale des volumes importants de données de journalisation créées dans un système informatique.
Gestion des vulnérabilités	Processus et procédures pour l'identification et la gestion des vulnérabilités.
Journal	Un journal, en langage informatique, désigne l'historique des événements relatifs à un système informatique donné, produit de façon automatique et horodaté. Il est possible également de créer manuellement des journaux pour les activités non-informatiques.
Journalisation	Opération consistant, pour les administrations fiscales, à enregistrer et conserver une trace de tous les accès aux données protégées, y compris l'accès aux installations et espaces où les données sont conservées, et notamment aux systèmes contenant les dossiers des contribuables et autres informations sensibles.

Un « cadre de gestion des opérations de sécurité » peut être défini comme un recueil de pratiques opérationnelles liées entre elles, qui contribuent à préserver la sécurité de l'administration fiscale. Il s'agit des mécanismes mis en œuvre pour la surveillance et la gestion des aspects de sécurité relatifs aux ressources informatiques, au personnel et aux processus.

L'ampleur de ce cadre dépendra de la taille de l'administration fiscale et de la complexité de ses opérations, par exemple :

- Dans les administrations fiscales de taille importante, avec des opérations complexes et variées, les différentes fonctions (journalisation, risques de sécurité, gestion des vulnérabilités, gestion des changements, gestion des incidents, audit…) peuvent être réparties sur plusieurs systèmes informatiques, services ou équipes de support, avec une unité centralisée chargée de la gestion des menaces pour les opérations.

- Dans les administrations fiscales de taille plus modeste, l'absence de complexité des opérations peut ne pas justifier une planification centralisée. La responsabilité de chaque fonction de la gestion des opérations sera alors confiée à un manager opérationnel.

Quelle que soit la taille de l'administration fiscale, il est important que les activités de gestion des opérations soient planifiées et coordonnées de façon efficace.

Par conséquent, l'administration fiscale doit adopter une approche globale de la gestion des opérations de sécurité, clairement énoncée dans un ensemble de politiques par domaine (voir la description à la SE 3.2.1) exposant le contexte général du cadre de GSI.

Les politiques spécifiques par domaine doivent inclure des dispositions de reporting en vertu desquelles les responsables opérationnels fournissent des rapports périodiques au RSSI, ou émettent des alertes sur la performance des contrôles de sécurité spécifiques à un domaine afin de garantir la mise en œuvre régulière des actions nécessaires pour limiter efficacement les risques (et les risques doivent être reflétés dans un registre des risques sur une base continue, comme décrit à la SE 3.2.1.4).

Dans la pratique, la gestion des opérations est souvent centralisée dans un centre des opérations de sécurité. Ce centre se compose d'une équipe d'experts et de systèmes pour le suivi et l'analyse permanents de la sécurité de l'organisation. La mission de l'équipe du centre des opérations de sécurité est de détecter et

analyser les incidents de sécurité, puis d'y répondre, en s'appuyant sur un éventail de mesures et de solutions technologiques.

Les sections suivantes présentent les principales fonctions de la gestion des opérations.

Sous-exigence 3.2.6.2. Gestion des journaux

La journalisation consiste, pour les administrations fiscales, à enregistrer et conserver une trace de tous les accès aux données protégées, y compris l'accès aux installations et espaces où les données sont conservées, et notamment aux systèmes contenant les dossiers des contribuables et autres informations sensibles. La gestion des journaux désigne les politiques et processus collectifs utilisés pour administrer et faciliter la création, la transmission, l'analyse, le stockage, l'archivage et l'élimination finale de volumes importants de données de journalisation créées dans un système informatique.

Les administrations fiscales doivent veiller à ce que l'accès soit journalisé et suivi, et le journal conservé pendant une durée suffisante pour remplir les exigences de contrôle, comme la surveillance des transactions, la gestion des incidents et l'audit.[18]

La journalisation répond au moins à deux objectifs : suivre l'efficacité des contrôles et fournir une preuve en cas d'incident.

La SE 3.2.6.2 prévoit donc pour les administrations fiscales l'obligation de mettre en place la journalisation et la surveillance, y compris pour détecter tout accès, utilisation ou divulgation non autorisé(e) de l'information.

Les administrations fiscales doivent en particulier définir leur approche de la journalisation et de la surveillance des renseignements échangés. Ces mécanismes peuvent s'inscrire dans le cadre général de la journalisation ou faire l'objet d'une approche dédiée.

Les administrations fiscales doivent :

- **Enregistrer les journaux**. L'enregistrement des journaux est une étape proactive très importante. Elle permet à l'administration fiscale de se référer aux journaux en cas d'activité malveillante ou d'accès illicite et de remonter jusqu'à son auteur. Correctement enregistrés et conservés, les journaux peuvent servir de preuve dans le cadre de procédures de sanction (administratives ou pénales).
- **Surveiller les journaux**. La surveillance des journaux permet d'identifier une activité suspecte et de prendre les mesures appropriées avant qu'un incident majeur ne se produise. Par exemple, cette opération permet d'identifier certaines activités qui, si elles ne constituent pas un incident, peuvent néanmoins être jugées préoccupantes (par exemple des demandes récurrentes de réinitialisation de mot de passe). Cette activité ne constitue pas en soi une violation de la politique de sécurité mais pourrait traduire une méconnaissance des bonnes pratiques et la création par les employés de mots de passe dont ils ne peuvent pas se souvenir, ou un manque de clarté des instructions données par le service informatique pour créer des mots de passe conformes aux critères de complexité.
- **Protéger et stocker les journaux**. Les journaux constituent une ressource importante, qu'il convient de protéger et stocker dans le respect des exigences de sécurité et des prescriptions légales. La loi prévoit parfois des délais de conservation pour les journaux, qui doivent être définis et documentés. En l'absence de délai légal, il est recommandé de prévoir une durée de conservation de 3 mois minimum, coïncidant avec la revue périodique des journaux. Les administrations fiscales doivent avoir la capacité d'extraire les journaux et de les interpréter en tant que de besoin, et cette capacité doit être régulièrement testée. Les exigences de sécurité peuvent inclure la mise en œuvre de contrôles d'accès aux journaux, la revue périodique des droits d'accès, la sauvegarde des journaux, le hachage pour le contrôle d'intégrité, la destruction des journaux, etc.[19]

Les administrations fiscales doivent aussi clairement identifier les activités à journaliser et définir des procédures de surveillance des journaux et de gestion des preuves.

Quelles activités journaliser ?

À partir d'une évaluation des risques liés à la sécurité de l'information (voir SE 3.2.1.4 sur la gestion des risques) et en collaboration avec le responsable du service informatique, un RSSI doit identifier :

- les activités à journaliser ;
- la fréquence de revue périodique des journaux ;
- les paramètres de surveillance pour déclencher une alerte en cas d'incident suspect.

18. La journalisation et la surveillance font également partie des contrôles informatiques de base décrits à la SE 3.2.4.2 sur les contrôles de sécurité informatique.

19. La destruction des journaux doit suivre une procédure prédéfinie pour la destruction ou l'élimination en toute sécurité, décrite à la SE 3.2.5 relatif à la protection de l'information.

L'enregistrement et la surveillance des journaux peuvent couvrir un certain nombre d'activités (informatiques ou non), par exemple :

- **Trafic internet**. Le suivi de l'origine des adresses IP, notamment des adresses IP étrangères, est important, tout particulièrement dans le contexte d'une administration fiscale, où la grande majorité des connexions sont en général nationales et/ou conformes à certains types.

- **Outils de prévention des logiciels malveillants**. La surveillance des journaux créés par les logiciels antivirus permet de déterminer si un virus a infecté un système à plusieurs reprises, et d'alerter sur la nécessité de bloquer l'origine du virus. Inversement, si les journaux font ressortir un faible nombre de virus bloqués, cela peut vouloir dire que le logiciel n'a pas été mis à jour avec la dernière liste de définition de virus.

- **Pare-feu**. Le suivi des flux de données sortant de l'administration fiscale permet d'identifier des flux inattendus nécessitant d'être vérifiés (par exemple déterminer si un flux à destination d'une société privée ou d'une agence de presse est légitime).

- **Gestion des accès**. La surveillance des journaux de domaine doit permettre d'identifier les accès autorisés et non autorisés. Une attention particulière peut être accordée aux accès depuis des appareils non enregistrés ou inattendus (par exemple un utilisateur autorisé depuis un appareil personnel) ou aux tentatives répétées d'accès non autorisé (par exemple les attaques par intrusion ou par refus de service).

- **Bases de données**. La surveillance des journaux de base de données permet de détecter des modifications inattendues ou non autorisées de données, un accès à des bases de données sensibles par un utilisateur autorisé et/ou une tentative d'accès par un utilisateur non autorisé.

- **Accès physique**. Le suivi des systèmes de vidéosurveillance et autres contrôles d'accès électroniques, ainsi que l'accès aux documents papier confidentiels ou locaux d'accès restreint (par ex. ceux de l'unité d'échange de renseignements) permet de détecter les intrusions. Il est possible de conserver manuellement ces types de journaux et de limiter le nombre de processus automatisés. Les procédures de vérification, de surveillance et de stockage doivent toutefois être identiques à celles des journaux automatiques.

- **Respect des contrôles de sécurité dans l'environnement de bureau**. Journalisation de la certification des extincteurs, distribution de clés, etc.

Surveillance des journaux et gestion des preuves

Les administrations fiscales doivent surveiller régulièrement les enregistrements de journaux. Il peut s'agir d'une surveillance passive (après un événement ou un incident) ou active (surveillance systématique ou en temps réel) à l'aide de systèmes de gestion des journaux.

La surveillance active peut intervenir à différents niveaux, par exemple :

- **Alertes**. Des paramètres peuvent être définis pour que, si certains événements se produisent, il soit possible d'identifier ces événements, d'enquêter sur ces derniers et, si nécessaire, de les corriger . Il peut s'agir d'une hausse imprévue du trafic internet, d'un type de trafic inattendu ou d'une exfiltration de volumes importants de données. Certains outils peuvent être utilisés pour générer des alertes, par exemple une solution de prévention des fuites de données.

- **Surveillance générale**. La surveillance en temps réel des systèmes de vidéosurveillance est un parfait exemple. Cette surveillance générale peut aussi prendre la forme d'une simple surveillance du trafic internet afin de déceler les événements imprévus, pour lesquels aucune alerte n'a été mise en place.

- **Listes de tâches**. Des seuils de déclenchement sont définis pour les événements qui nécessitent d'être contrôlés. Lorsque ces seuils sont atteints, une notification est ajoutée dans une liste de tâches et l'événement est contrôlé pendant les heures de travail habituelles, si possible sous 24 heures. Cette activité concerne les événements qui nécessitent une action ou un contrôle, mais n'ont pas un caractère critique, par exemple parce qu'ils affectent un seul enregistrement. Cette surveillance active est qualifiée de surveillance « en temps quasi réel » et s'apparente presque à une surveillance passive.

Une organisation adoptera en général des méthodes de surveillance passive et/ou ative en fonction de certains facteurs, notamment :

- les risques évalués ;

- les exigences de sécurité ou liées à l'activité ;

- les compétences du personnel en charge de la surveillance ;

- la capacité de stockage des journaux ;
- la quantité de journaux, et la dynamique de création de ces derniers, ce dernier facteur ayant de possibles répercussions sur le budget.

Pour la surveillance des journaux et la gestion des preuves, les administrations fiscales doivent aussi envisager les pratiques suivantes :

- **Définition de paramètres établissant une distinction entre les événements considérés comme nécessitant un reporting urgent ou prioritaire et les événements non urgents qu'il est inutile de prioriser.** Par exemple, des alertes peuvent être créées pour les journaux sensibles uniquement (par exemple journaux des accès aux bases de données de l'EAR), ces derniers impliquant des conséquences plus graves. Les alertes déclenchées par le système de contrôle d'accès pourraient être reliées à la procédure de gestion des incidents décrite à la SE 3.2.6.6.
- **Mise en place de contrôles pour protéger l'intégrité des journaux lors de leur utilisation et analyse.** Ces contrôles incluent le hachage (pour garantir l'intégrité des journaux), la sauvegarde régulière des journaux et l'application d'un contrôle d'accès strict pour les personnes susceptibles de voir ou gérer les journaux.
- **Vérification des contrôles de surveillance.** Ces contrôles doivent être régulièrement vérifiés pour apporter d'éventuels ajustements aux critères d'alerte.
- **Définition claire des rôles et fonctions des personnes concernées.** Sont concernées, notamment, les personnes en charge de la surveillance des journaux, de la vérification des droits d'accès et accès aux fichiers-journaux et de la détermination des contrôles nécessaires à la protection de l'intégrité des fichiers-journaux. Il peut s'agir du RSSI, des responsables informatiques, du centre des opérations de sécurité ou d'un prestataire externe, le cas échéant. L'organisation doit documenter dans quelles circonstances ces personnes sont autorisés à utiliser et analyser les fichiers journaux (par exemple le RSSI pour analyser un incident ou mesurer l'efficacité des contrôles de sécurité, ou l'Audit interne pour enquêter sur un incident lié à une utilisation abusive de l'information).
- **Définition de politiques ou pratiques pour la conservation des journaux et la gestion des preuves.** Cette mesure permet de conserver une « chaîne de responsabilité » pour les données ou documents impactés, facilitant ainsi le déroulement des enquêtes menées dans le cadre des procédures disciplinaires internes ou par les organismes chargés de l'application de la loi. Ces politiques ou pratiques incluent des politiques de gestion des journaux avec des contrôles relatifs à la conservation, l'intégrité et l'accès, ainsi que des procédures détaillées pour la conservation et la protection des preuves à l'aide de la copie, du chiffrement et de la sauvegarde.

Les activités de journalisation et de surveillance peuvent être étendues et gérées à l'aide d'outils tels que les systèmes de gestion des informations et événements de sécurité (SIEM), sous réserve d'un rapport coût-bénéfice intéressant pour l'administration fiscale. Voir l'encadré 38 pour un exemple d'approche de la journalisation et de surveillance dans une administration fiscale.

Encadré 38. Exemple d'approche de la journalisation et de la surveillance

Dans la juridiction A, tous les systèmes de l'administration fiscale consignent tous les accès (ou tentatives d'accès) aux données. Un système de journalisation centralisé consigne et enregistre toutes les activités. L'accès aux journaux est également consigné. Certaines protections spécifiques permettent de préserver l'intégrité des journaux et de prévenir toute modification non autorisée des fichiers journaux. Les journaux sont conservés pendant 18 mois.

La surveillance des journaux et sa fréquence sont fonction du système de classification des données de l'organisation. La surveillance des journaux des systèmes contenant des données classifiées « sensibles » ou « confidentielles » et accessibles uniquement aux utilisateurs ayant le statut d'administrateur (par ex. : systèmes relatifs à l'EAR) est réalisé au moyen d'un système de surveillance en temps réel, qui déclenche une alerte lorsqu'une activité suspecte est détectée. Il existe une approche de surveillance plus passive pour les systèmes non sensibles et les comptes sans privilèges. Ce suivi intervient selon un calendrier prédéfini ou en fonction des besoins.

Le RSSI effectue une surveillance régulière des journaux des différents systèmes afin de vérifier l'efficacité des contrôles mis en place pour chacun d'entre eux. En collaboration avec le responsable de la gestion des incidents, le RSSI contrôle également les journaux dans le cadre de l'analyse et du traitement d'un incident. Son objectif est de comprendre non seulement la cause et l'impact de l'incident, mais aussi le problème sous-jacent responsable de l'accroissement des risques.

Sous-exigence 3.2.6.3. Gestion opérationnelle des risques en matière de sécurité informatique

La gestion opérationnelle des risques pesant sur la sécurité informatique est une activité essentielle dans l'environnement d'une administration fiscale, car les menaces informatiques peuvent avoir des impacts profonds et étendus si les bases de données contenant des informations confidentielles sont compromises.

L'approche d'une administration fiscale concernant la gestion des risques de sécurité informatique doit être compatible avec le processus général de gestion des risques employé, tel que décrit à SE 3.2.1.4, c'est-à-dire la méthodologie globale de gestion du risque, qu'il s'agisse des activités informatiques ou autres.

Les administrations fiscales doivent prendre en compte les aspects spécifiques suivants (pour un exemple de gestion des risques de sécurité informatique, voir l'encadré 39) :

- **L'implication du département informatique dans le processus global de gestion des risques.** L'implication du département informatique dans les processus de gestion des risques de l'administration fiscale est cruciale, car la grande majorité, si ce n'est l'intégralité des principaux risques liés aux opérations a une dimension informatique. Ceci est particulièrement important pour l'identification des contrôles les plus appropriés, ainsi que l'évaluation de l'impact ou de l'efficacité de ces contrôles dans la diminution des risques identifiés. Idéalement, le registre des risques informatiques s'intègre au registre des risques liés aux opérations. Cette intégration peut apporter une plus grande visibilité sur les risques informatiques dans le domaine général de la prévention des risques, et une meilleure compréhension de l'impact des changements des risques liés aux opérations sur les contrôles informatiques et de sécurité.

- **Les conséquences informatiques des décisions concernant la gestion des opérations.** Le rôle croissant de l'informatique dans tous les domaines opérationnels des administrations fiscales fait que la plupart des décisions opérationnelles a une implication informatique, c'est-à-dire qu'elles exigent le changement ou la modification d'un système informatique existant. Ces implications doivent être convenablement analysées et prises en compte dans la sécurité des données. Les décisions opérationnelles concernant le financement du département informatique peuvent avoir un impact significatif sur la sécurité, car celle-ci est basée sur des contrôles gérés par le département informatique sur le plan opérationnel.

- **Les conséquences des risques sur les décisions en matière d'informatique.** Lors de la conception, du développement et de la mise en place de nouvelles applications ou infrastructures informatiques, ou lors d'améliorations routinières des systèmes informatiques, le personnel informatique doit continuellement envisager les changements dans l'environnement global de gestion des risques impliqués par ces développements ou modifications, et retranscrire leurs conclusions de manière appropriée dans le registre des risques.

- **La supervision et la réévaluation régulières des risques informatiques et des contrôles de sécurité informatiques.** Comme l'environnement informatique est en constante évolution, les informaticiens identifient continuellement de nouveaux risques et de nouvelles menaces et vulnérabilités émergents. Par conséquent, le personnel informatique doit quotidiennement superviser les développements et régulièrement évaluer les risques informatiques et la fiabilité des contrôles en place (voir également la SE 3.2.6.4 sur la gestion des vulnérabilités).

Encadré 39. **Exemple de gestion des risques en matière de sécurité informatique**

La gestion des risques de sécurité informatique de l'administration fiscale de la Juridiction B est assurée par une équipe chargée de l'évaluation des risques comprenant le RSSI et des représentants du département informatique et des différents domaines opérationnels. Sous la direction du RSSI, les membres de cette équipe identifient ensemble les risques liés à la sécurité informatique, et ils évaluent la probabilité que ces risques surviennent et leurs conséquences potentielles. Les critères d'acceptation du risque sont prédéfinis par les cadres supérieurs, sur les conseils du RSSI, et ils reflètent l'évaluation des risques de l'équipe. Tous les risques exclus de ces critères d'acceptation doivent être traités au moyen de contrôles.

Le département informatique apporte une assistance technique et propose des contrôles visant à réduire les risques identifiés, tandis que le RSSI s'assure que ces contrôles sont conformes aux politiques et procédures applicables en matière de sécurité de l'information. Les représentants des domaines d'activité apportent leur contribution en garantissant que les contrôles n'affectent pas la performance globale de leurs processus opérationnels.

L'évaluation des risques et les contrôles sélectionnés sont inscrits dans un registre des risques. L'équipe examine régulièrement l'évaluation, et un responsable informatique est chargé d'effectuer le suivi de la mise en place des contrôles de réduction des risques informatiques et de leur efficacité.

- **L'approche vis-à-vis des fournisseurs de services informatiques externes.** Lorsque l'informatique est gérée en dehors de l'administration fiscale, des contrats ou accords de niveau de service appropriés doivent régir la relation avec les fournisseurs externes et leur prestation de services informatiques, notamment la façon dont les risques sont gérés et signalés dans la prestation de ces services. Ces risques doivent être intégrés à la gestion des risques de l'administration fiscale.

Sous-exigence 3.2.6.4. Gestion des vulnérabilités

La SE 3.2.6.4 prévoit que les administrations fiscales mettent en œuvre des processus et procédures pour l'identification et la gestion des vulnérabilités. La gestion des vulnérabilités consiste en un examen périodique de l'environnement informatique de l'organisation afin d'identifier les vulnérabilités qui pourraient poser un risque significatif. Des contrôles de sécurité informatique appropriés doivent être déployés pour traiter les vulnérabilités identifiées (voir la discussion à la SE 3.2.4.2).

La fréquence et l'ampleur de l'examen des vulnérabilités dépend de la complexité et de l'étendue des opérations informatiques d'une administration fiscale, des risques identifiés et du budget disponible. Indépendamment de sa fréquence et de son ampleur, l'analyse des vulnérabilités doit être approfondie pour permettre l'identification des politiques ou des contrôles du système de GSI qui requièrent une amélioration. Bien qu'il existe différents outils disponibles pour l'identification des vulnérabilités, la SE 3.2.6.4 se concentre sur l'analyse des vulnérabilités et les tests d'intrusion des environnements informatiques.

Examen des vulnérabilités

L'examen des vulnérabilités consiste en une identification des défaillances dans la conception des systèmes informatiques qui sont susceptibles d'être utilisées de manière abusive par des agents malveillants internes ou externes. Un outil d'analyse vérifie automatiquement les possibles points d'entrée pouvant permettre aux pirates de pénétrer dans les programmes, les services ou les ports, et les défauts de conception d'une infrastructure informatique.

Il existe différents types d'outils d'analyse des vulnérabilités, selon l'étendue et la profondeur souhaitées de l'analyse. Ils peuvent porter sur :

- **L'analyse des vulnérabilités du réseau** : vérification de tous les ordinateurs et systèmes sur le réseau pour détecter les failles de sécurité.
- **Analyse authentifiée et non authentifiée** : la vérification des systèmes pour détecter les vulnérabilités peut être réalisée en simulant un pirate externe sans identifiant d'utilisateur (vérification non authentifiée) ou avec identifiant d'utilisateur (vérification authentifiée), cette dernière représentant le cas où un pirate possède déjà un accès au système en tant qu'utilisateur.

Un rapport d'analyse des vulnérabilités doit être immédiatement examinée, et les vulnérabilités identifiées doivent être traitées par les contrôles appropriés.

Tests d'intrusion

Le test d'intrusion, également dénommé « piratage éthique », est un type de test de vulnérabilité particulier qui vérifie le périmètre et la profondeur possibles d'un accès par un utilisateur non autorisé à un moment déterminé. Toutes les administrations fiscales, indépendamment de leur taille, doivent réaliser des tests d'intrusion réguliers sur leurs interfaces internes et externes. Les interfaces permettant l'EAR doivent être fréquemment soumises à des tests d'intrusion.

Pour que ces tests soient efficaces, les administrations fiscales doivent prendre en compte les aspects suivants :

- **Réaliser des tests d'intrusion sur les interfaces internes et externes.**
  - **Interfaces externes.** Ces tests d'intrusion analysent les connexions entre le monde et le système informatique de l'administration fiscale.
  - **Interfaces internes.** Ces tests d'intrusion analysent les connexions internes au sein de la plateforme ou du système informatique de l'administration fiscale afin de vérifier l'implémentation adéquate des principes « d'accès limité aux besoins d'en connaître » et « d'accès offrant le moins de privilèges ».
- **Effectuer des tests d'intrusion périodiques.** Un test d'intrusion analyse la vulnérabilité des systèmes au moment où il est réalisé. Ce test est donc particulièrement approprié lorsque l'on analyse de nouveaux systèmes ou les modifications importantes d'un système, à la fois avant et après leur implémentation. Les interfaces les plus importantes doivent être testées régulièrement : au moins une fois par an, ou plus fréquemment en fonction de leur importance.
- **Faire appel à des prestataires de tests d'intrusion indépendants et fiables.** Dans l'idéal, les tests d'intrusion doivent être réalisés par un prestataire de tests d'intrusion tiers, indépendant de l'administration fiscale. Il est important de faire appel à des prestataires de bonne réputation et dotés d'une expérience et d'une connaissance avérées des techniques les plus récentes. Il est conseillé de recourir à des prestataires de piratage éthique certifiés.

- **Établir les principales exigences avec le prestataire de tests d'intrusion.** La réussite des tests d'intrusion dépend étroitement du degré d'engagement auprès du prestataire. Les administrations fiscales devraient toujours conclure un contrat avec le prestataire de test d'intrusion avant que les tests ne soient effectués, et établir un accord de non-divulgation concernant les informations que le testeur pourrait éventuellement et dont il ne doit pas un usage abusif. Le contrat doit inclure les contraintes prédéterminées avec lesquelles le prestataire devra travailler, comme le type d'équipement à utiliser et les catégories d'informations sur le système à tester qui seront communiquées au prestataire. Selon les paramètres définis, les tests peuvent être « en boîte noire » (aucune information n'est donnée sur le système hormis l'adresse du site Web) ou « en boîte blanche » (l'infrastructure et la configuration du système sont portées à la connaissance du prestataire). Les exigences relatives aux tests doivent être ouvertement discutées avec le prestataire des tests, en lui donnant la possibilité de prendre en compte le contexte des activités opérées par l'administration fiscale et de faire des suggestions. De par leur expérience, les prestataires de tests d'intrusion peuvent avoir une meilleure connaissance des menaces actuelles, et être en capacité de faire des suggestions quant à l'approche et la portée d'un test.

Pour un exemple de contrôles de la gestion des vulnérabilités, voir l'encadré 40.

Sous-exigence 3.2.6.5. Gestion des changements

La gestion des changements consiste en une gestion contrôlée du développement de nouveaux systèmes et services ainsi que des changements majeurs apportés aux systèmes existants. Elle couvre la conception, l'essai et le contrôle des versions des solutions, et constitue le moyen de garantir que la sécurité informatique est intégrée dans les modifications des systèmes.

La SE 3.2.6.5 exige que les administrations fiscales disposent d'un processus de gestion des changements, dans lequel la sécurité est intégrée. Le processus peut être documenté dans une politique ou une procédure, selon le niveau de détail nécessaire, et doit être revu par le RSSI à intervalles réguliers.

Encadré 40. **Exemple de contrôles en matière de gestion des vulnérabilités**

L'administration fiscale de la juridiction C analyse tous ses systèmes, applications et bases de données afin de détecter de potentielles vulnérabilités, qui pourraient être exploitées par un pirate, et applique les contrôles en conséquence. Tout le trafic entre le Web, les applications et les bases de données est contrôlé 24h/24, 7j/7, par des pare-feu physiques et des systèmes spécialisés qui fournissent des mises à jour en temps réel sur les potentielles attaques, afin que celles-ci puissent être détectées et traitées rapidement.

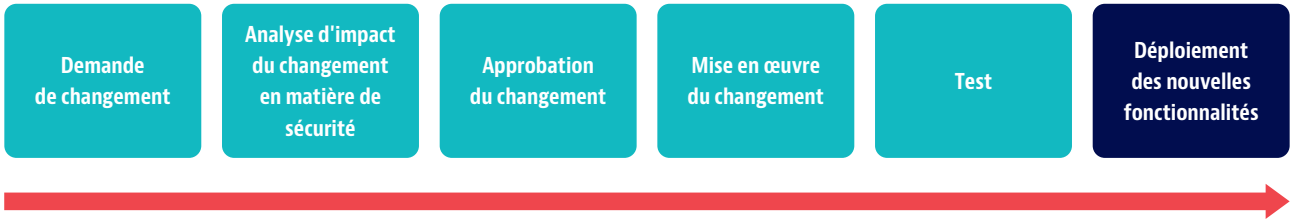
L'administration fiscale fait également appel à des entreprises spécialisées dans la sécurité pour réaliser des piratages éthiques sur les interfaces internes et externes. Les systèmes d'EAR sont soumis à des tests d'intrusion tous les ans. Toutes les nouvelles applications font également l'objet d'un test d'intrusion avant d'être implémentées, et toutes les constatations et vulnérabilités détectées doivent être résolues avant le déploiement.

Du point de vue de la sécurité, le processus de gestion du changement lui-même comporte des risques importants. Modifier des systèmes sans adopter une approche de la sécurité informatique adéquate peut résulter en des systèmes vulnérables et engendrer d'importantes violations de la sécurité. Cela peut être le cas lorsque les changements sont précipités en raison de contraintes budgétaires ou temporelles et en l'absence de rigueur, de tests adéquats et de prise en compte des avertissements.

Une approche rigoureuse de la gestion du changement doit donc être développée et mise en œuvre conjointement par le département informatique, les responsables et utilisateurs des systèmes liés aux opérations et le RSSI. Cette approche doit incorporer la séquence d'étapes clés décrite dans la figure 18 :

- **Demande de changement.** Toutes les demandes de changement doivent être documentées et inclure une description des bénéfices attendus de la modification, les systèmes ou processus concernés, les problèmes

FIGURE 18. **Étapes de la gestion du changement**



pouvant être résolus (si le changement est motivé par un incident ou une vulnérabilité connue), l'urgence et la date d'échéance, et le niveau de priorité et d'importance pour les processus opérationnels. Les administrations fiscales doivent définir clairement les types de changement pouvant être demandés, et les critères appliqués à chacun d'entre eux. Les deux principaux types sont les suivants :

- **Changements ordinaires.** Il s'agit des changements qui peuvent être planifiés, priorisés, approuvés, testés et déployés. Le cas échéant, ces changements peuvent être classifiés selon leur ampleur (mineure ou majeure).

- **Changements d'urgence.** Il s'agit des changements qui doivent être immédiatement mis en œuvre pour résoudre une déficience majeure, lorsque les délais d'implémentation pourraient aggraver les dommages. Les étapes ordinaires du processus de changement sont ignorées et appliquées postérieurement à l'implémentation du changement. Dans de nombreux cas, les changements d'urgence résultent d'un incident. Le processus de gestion des incidents est décrit à la section suivante, le la SE 3.2.6.6.

- **Analyse d'impact en matière de sécurité.** Les diverses implications du changement sur les processus opérationnels, les systèmes informatiques et la sécurité doivent être analysées par le personnel impliqué dans chacun de ces aspects. Il convient de trouver un équilibre entre les fonctionnalités requises par les opérations, les contrôles pour la réduction des risques recommandés par le responsable de la sécurité des systèmes d'information, et les avancées ou restrictions technologiques imposées par le système.

- **Approbation du changement.** La responsabilité de l'approbation des changements, généralement attribuée au RSSI ou à l'encadrement supérieur, peut être définie dans le cadre des rôles et responsabilités de la politique de gestion de la sécurité de l'information (SE 3.2.1.2).

- **Mise en œuvre du changement.** Lors de la phase de mise en œuvre, les équipes impliquées doivent s'assurer du respect des exigences de sécurité avant le déploiement. Par exemple, si des modifications sont apportées au code source d'un logiciel, l'intégrité du code source doit être géré à l'aide d'outils de gestion des versions. Si le changement implique des processus ou des procédures, cela doit se faire conformément à la politique globale de GSI et autres politiques applicables.

- **Test.** Il est essentiel que les modifications soient testées, notamment si elles sont implémentées sur les systèmes informatiques. Dans la mesure du possible, ces tests ne doivent pas être réalisés directement dans l'environnement de production. En cas de modification logicielle, les tests doivent avoir lieu dans un environnement isolé, avec des données fictives. Cela permet de déceler les erreurs sans mettre en péril les données réelles ni le fonctionnement des processus en cours. Les politiques doivent fournir des orientations claires quant à l'utilisation de données dans les tests et les critères de déploiement des éléments modifiés.

- **Déploiement des nouvelles fonctionnalités (déploiement des éléments modifiés).** Dans la mesure du possible, le déploiement de toute nouvelle fonctionnalité doit être planifié. Cela signifie que le déploiement doit être opéré à une période au cours de laquelle les perturbations des opérations de l'administration fiscale seront minimes. Il est recommandé de déployer les éléments modifiés en ayant un plan de restauration, c'est-à-dire un moyen de revenir au mode d'opération précédent ou de le restaurer en cas d'échec du déploiement dans l'environnement de production.

Les changements incorrectement implémentés sont souvent à l'origine des incidents, notamment les incidents de sécurité. Il est donc impératif d'appliquer une gouvernance adéquate. L'un des moyens d'y parvenir consiste à mettre en place une entité chargée d'autoriser formellement le déploiement des éléments modifiés, par exemple le RSSI ou, dans les organisations plus complexes, une commission de contrôle des changements ou tout organe équivalent, qui comprenne des représentants de différents domaines opérationnels, notamment la sécurité. Cette entité élabore généralement un calendrier des

Encadré 41. **Exemple de gestion du changement**

L'administration fiscale de la juridiction A s'est dotée de principes directeurs détaillés pour la gestion du changement et la modification des codes informatiques. Ces principes prennent en considération les exigences des utilisateurs du système et celles du département informatique, notamment la sécurité de l'information.

Tous les changements, y compris les modifications des codes source, sont d'abord testés par les développeurs dans un environnement de développement. Les cadres responsables de l'informatique réalisent ensuite de nouveaux tests dans un environnement de test auquel les développeurs n'ont pas accès. Les nouveaux éléments ne peuvent être déployés dans l'environnement de production qu'à la suite de ces deux tests.

Tous les codes source sont stockés dans un répertoire sécurisé avec privilèges d'accès aux seules personnes qui ont un besoin d'en connaître.

changements à venir, périodiquement transmis à toutes les parties prenantes concernées, afin d'offrir une visibilité sur les changements prévus et d'éviter de trop fortes perturbations des activités opérationnelles.

Le RSSI doit régulièrement réévaluer l'approche de l'organisation en matière de gestion du changement, afin d'en vérifier l'efficacité. Pour un exemple d'approche en matière de gestion du changement, voir l'encadré 41.

Sous-exigence 3.2.6.6. Gestion des incidents

La SE 3.2.6.6 prévoit que les administrations fiscales mettent en œuvre un système de gestion des incidents qui couvre tous types d'incidents de sécurité. La gestion des incidents implique l'identification, la documentation et la gestion des incidents de sécurité, à la fois dans les domaines informatique et non informatique.

Un incident est, pour l'essentiel, l'occurrence d'un événement qui n'est pas censé survenir. Même lorsque les administrations fiscales appliquent correctement les contrôles, il est toujours possible que les choses ne se déroulent pas comme prévu. Un système de gestion des incidents doit être mis en place pour deux raisons principales :

- Pour solutionner les incidents aussi rapidement et efficacement que possible, afin de minimiser leur impact potentiel.
- Pour prévenir l'occurrence de nouveaux incidents.

Les incidents à travers les différents domaines d'une administration fiscale doivent être traités de manière similaire, même s'ils ne sont pas tous gérés par les mêmes personnes. Par exemple, les incidents informatiques sont généralement traités par le centre d'assistance informatique. Les incidents non informatiques, tels que les incidents en matière d'intrusion physique ou de badge/carte d'accès, peuvent être gérés par l'unité chargée de la gestion des bâtiments et des infrastructures. D'autres incidents peuvent être placés sous la responsabilité du département des ressources humaines ou de l'audit interne.

Quoi qu'il en soit, une politique ou procédure documentée doit définir l'approche de gestion de tous les incidents de sécurité affectant l'administration fiscale. Cette approche sert principalement à ce que l'équipe de sécurité et les autres parties prenantes puissent envisager les possibles liens entre différents types d'incidents, afin de rechercher des tendances pouvant faire apparaître des risques qui n'auraient pas encore été pris en compte.

L'approche en matière de gestion des incidents de l'administration fiscale doit être clairement communiquée à tout le personnel. En outre, l'attribution précise des responsabilités dans la gestion des incidents doit être documentée dans les rôles et responsabilités de la politique de GSI (voir SE 3.2.1.2) en lien avec le cadre de sécurité global.

L'approche de gestion des incidents doit généralement suivre une série d'étapes pouvant être traduite sous la forme d'un processus, comme l'illustre la figure 19.[20]

- **Identification des incidents informatiques et non informatiques.** Le personnel doit être incité à signaler tout événement pouvant être interprété comme un incident de sécurité, qu'il soit lié à l'informatique ou non. Les voies de signalement des incidents doivent être accessibles à tout le personnel, et les procédures ne doivent pas être fastidieuses. Le signalement des incidents doit être abordé lors de formations d'intégration ou de sensibilisation à la sécurité dispensées à tout le personnel. Les incidents sont également identifiés dans le cadre des activités de surveillance des journaux (voir SE 3.2.6.2).
- **Catégorisation des incidents.** La ou les personnes responsables de la gestion des incidents doit analyser les incidents signalés et les catégoriser afin que les mesures adéquates soient prises. Les catégories, qui doivent être documentées dans les politiques, peuvent inclure :
  - Les incidents de sécurité de l'information, ou les événements pouvant avoir des conséquences négatives du point de vue de la sécurité de l'information, c'est-à-dire lorsqu'ils compromettent la confidentialité ou l'intégrité des données. Par exemple, un périphérique USB contenant des données confidentielles est perdu ou volé, ou l'identifiant électronique d'un membre de l'unité d'échange de renseignements est perdu.

20. Pour des orientations complémentaires, consulter les normes internationales telles que ISO20000 ou ISO27035.

FIGURE 19. **Processus de gestion des incidents**

- Les autres types d'incidents, comme les incidents informatiques n'affectant pas la sécurité des données (par exemple, une imprimante en mauvais état de fonctionnement).

Selon la catégorie de l'incident, le traitement peut être coordonné par le RSSI, le centre d'assistance informatique, ou les deux conjointement, conformément à la procédure de gestion des incidents.

- **Analyse et hiérarchisation de la priorité des incidents.** En fonction de leur impact potentiel, les incidents de sécurité doivent être analysés et classifiés comme majeurs ou mineurs, afin que leur traitement soit priorisé. Le critère de définition de la priorité peut comprendre le type d'incident (par exemple, un identifiant électronique perdu, ou un périphérique USB perdu ou volé), le type d'informations affectées (par exemple, une circulaire interne, des données relatives aux contribuables ou des renseignements échangés), la quantité de données confidentielles impliquées (par exemple, une donnée unique ou un ensemble complet de données), et la probabilité de dommages si les informations venaient à être divulguées (par exemple, une fraude financière).

  Selon le degré de priorité, le temps de réponse à un incident de sécurité peut varier, et les incidents majeurs peuvent déclencher une procédure de remontée de l'information.

- **Remontée de l'information relative aux incidents.** Si l'analyse révèle qu'un incident de sécurité majeur a eu lieu, il convient d'en faire remonter l'information et d'enquêter conformément aux procédures établies, afin que les principales parties prenantes soient alertées (par exemple, les personnes concernées par les données affectées, les fournisseurs de données, les autorités, les administrations fiscales étrangères si l'incident implique des renseignements échangés, etc.). La remontée de l'information et la communication aux autres autorités, selon l'ampleur et l'impact d'un incident constituant une violation de la confidentialité, doivent respecter la législation nationale et toute autre exigence légale ou contractuelle. Des orientations plus détaillées sur ces procédures sont fournies au critère principal 3.3, relatif aux dispositions et processus visant à traiter les violations de la confidentialité.

- **Clôture des incidents.** La clôture d'un incident comprend sa résolution, la reprise normale des opérations et une évaluation de suivi de l'incident. En fonction de l'ampleur de l'incident de sécurité, cette évaluation doit en identifier les causes principales, les processus qui ont échoué, les parties impliquées, les systèmes affectés, le délai de résolution, et l'efficacité de la solution mise en œuvre. L'évaluation est importante pour orienter les stratégies à plus long terme afin de réduire la probabilité d'occurrence de nouveaux incidents de sécurité à l'avenir, ou pour diminuer l'impact des dommages provoqués par l'incident. Le cas échéant, des pénalités et sanctions pour non-respect des règles doivent être appliquées, comme le décrit le la SE 3.3.2.

L'approche en matière de gestion des incidents doit prévoir une réévaluation régulière de son efficacité. Le RSSI doit, conjointement avec le responsable du département informatique et les représentants des domaines opérationnels, revoir les événements ayant fait l'objet de rapports, la classification de l'incident et sa clôture. L'analyse doit permettre l'identification des problèmes à la source des incidents récurrents, afin que des solutions plus systématiques soient mises en œuvre.

Sous-exigence 3.2.6.7. La fonction d'audit interne et externe

La fonction d'audit interne joue un rôle important dans la sécurité de l'information de toutes les organisations, notamment les administrations fiscales, car elle permet :

- **La garantie des processus.** L'audit interne peut permettre de déceler les failles des processus qui pourraient accroître le risque de fuite de données ou de renseignements, et d'identifier les améliorations nécessaires.

- **Le (non-)respect des processus.** L'audit interne permet de vérifier si le personnel respecte les processus de gestion de la sécurité de l'information établis dans les politiques et procédures, d'apporter des améliorations lorsque les pratiques diffèrent de ce qui est établi et, le cas échéant, d'appliquer des mesures disciplinaires en cas de non-respect. Bien que les cadres et/ou le département des ressources humaines traitent généralement les problèmes de mauvaise conduite des employés et d'accès illégal aux informations, une fonction d'audit interne efficace aura les ressources et l'expertise permettant souvent d'identifier les indices de non-respect avant qu'ils ne soient décelés par d'autres personnes. L'approche de l'audit interne doit être documentée, et il convient de s'assurer de la compétence des auditeurs internes.

Les administrations fiscales doivent établir des politiques et procédures pour que l'audit interne adopte les principes clés suivants :

- **Indépendance.** Les auditeurs doivent être indépendants de tout intérêt personnel particulier autre que les objectifs globaux de l'administration fiscale, tels que définis par la législation et les politiques clairement établies et mises en place pour atteindre ces objectifs.
- **Accès aux éléments probants.** Les auditeurs doivent obtenir la preuve de la bonne mise en œuvre du système de GSI à travers des interactions avec le personnel responsable des opérations. En cas de suspicion, ils peuvent demander un accès direct aux données, aux systèmes et aux contrôles concernés.
- **Liaison avec les principaux décideurs.** Le responsable de l'audit interne doit être en liaison directe avec le directeur de l'administration fiscale si les circonstances l'exigent.
- **Liberté de décision quant à l'objet des audits.** Bien qu'il soit recommandé que le responsable de l'audit interne se réunisse périodiquement avec l'encadrement supérieur de l'administration fiscale afin d'identifier les processus ou fonctions à auditer, l'unité de l'audit interne doit maîtriser au moins une partie de son programme de travail et être en capacité d'auditer les processus et fonctions qu'elle juge les plus appropriés. Une attention particulière doit être portée aux processus qui génèrent les plus hauts risques, mais, de manière générale, tous les processus doivent être évalués annuellement ou, si cela n'est pas possible, à moyen terme.
- **Rapports d'audit.** Le rapport d'audit doit présenter les résultats d'analyse sur le niveau de conformité aux différents processus liés à la GSI et faire des recommandations d'amélioration. Les mesures correctives proposées doivent être coordonnées avec le RSSI pour leur mise en œuvre. Le rapport doit également présenter l'échantillon de processus qui a fait l'objet d'un audit et le personnel impliqué, et doit être remis l'encadrement supérieur de l'administration fiscale.
- **Fréquence des audits.** Les audits internes doivent être réalisés à intervalles réguliers. Selon la complexité et la taille de l'administration fiscale, les processus qui présentent le plus de risques en matière de sécurité doivent être évalués par l'audit interne au moins une fois par an.

Outre la fonction d'audit interne, les bonnes pratiques internationales recommandent aux administrations fiscales de se soumettre à des audits externes réalisés par d'autres autorités indépendantes en lien avec le système de GSI (par exemple, l'inspecteur général des finances, l'autorité nationale d'audit, l'organe de supervision de la protection des données, etc.).

Dans les juridictions où l'administration fiscale est de petite taille et où il est difficile d'attribuer des ressources à la fonction d'audit interne, il peut être nécessaire de s'appuyer sur les différents audits externes réalisés par les autorités indépendantes du pays ou sur un audit externe effectué par un organisme de certification accrédité.

L'encadré 42 fournit un exemple d'audit interne des processus de GSI.

Encadré 42. **Exemple d'audit interne des processus de GSI**

La fonction d'audit interne de l'administration fiscale de la juridiction B a pour objectif la fourniture d'évaluations objectives et indépendantes de l'efficacité de la gouvernance, de la gestion des risques et des dispositifs de contrôle interne au sein de l'administration fiscale. Les audits sont basés sur les risques et comprennent, entre autres, l'audit des systèmes et processus informatiques, la cyber sécurité, la gestion des données et des renseignements, la gestion des tiers et la sécurité physique.

La fonction d'audit interne rend compte de ses activités au contrôleur général (comptroller general) et dispose d'un accès illimité et d'une liaison avec le chef de l'administration fiscale (commissaire). Les résultats des audits sont présentés au contrôleur général tous les trimestres et au commissaire tous les semestres.

Les audits de processus impliquant un échange de renseignements couvrent l'analyse des journaux et la surveillance et l'intégrité des journaux, notamment l'accès aux renseignements concernant les contribuables, afin de garantir que les contrôles et procédures soient en place et qu'ils fonctionnent tel que prévu pour empêcher les accès non autorisés.

4. Dispositions coercitives et processus pour traiter les violations des obligations de confidentialité (Exigence fondamentale 3.3)

Malgré la mise en place de mesures de GSI et de contrôles de sécurité, l'éventualité que des accès non autorisés ou des violations de la confidentialité des renseignements surviennent ne peut être écartée. Des dispositions coercitives efficaces et des processus bien définis visant à gérer les violations en matière de confidentialité et en tirer des enseignements sont, par conséquent, essentiels pour la fiabilité des mesures de GSI et pour permettre à l'administration fiscale de prévenir les violations ultérieures.

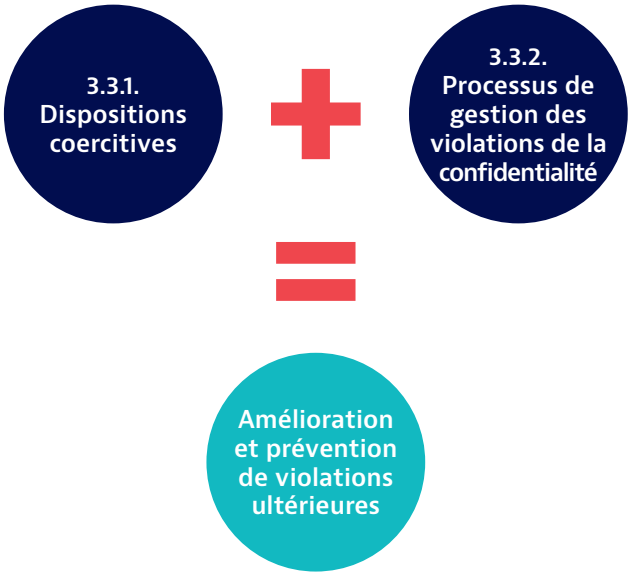
Le critère principal 3.3 requiert donc des juridictions qu'elles mettent en œuvre des dispositions coercitives et des processus destinés à résoudre les violations de la confidentialité. Ce critère est divisé en deux sous-exigences (voir la figure 20) :

- SE 3.3.1 : les juridictions doivent prévoir des pénalités ou des sanctions adéquates en cas de divulgation ou d'utilisation non autorisée des renseignements.
- SE 3.3.2 : les juridictions doivent appliquer des processus adéquats pour traiter des manquements suspectés ou avérés à la confidentialité, notamment via l'application effective de sanctions.

SOUS-EXIGENCE 3.3.1 : SANCTIONS EN CAS DE DIVULGATION OU D'UTILISATION NON AUTORISÉE DE RENSEIGNEMENTS FISCAUX

Afin de s'assurer de l'application des dispositions légales en matière de confidentialité et d'utilisation appropriée des renseignements fiscaux, notamment les renseignements échangés, la loi doit imposer des sanctions suffisamment claires et sévères pour

FIGURE 20. **Composants clés de la résolution des violations de la confidentialité**



Encadré 43. **Exemple de sanctions en cas de divulgation ou d'utilisation non autorisée de renseignements fiscaux**

La loi relative à l'impôt sur le revenu de la juridiction A établit des sanctions pécuniaires et pénales, selon la gravité de l'infraction, pour toute personne, personnel et sous-traitants externes compris, qui viole la confidentialité des renseignements fiscaux couverts par ladite loi. Les violations sont passibles d'une amende allant jusqu'à 15 000 euros ou d'une peine d'emprisonnement pouvant atteindre trois ans.

En vertu du code de conduite de l'administration fiscale de la juridiction A, une divulgation ou utilisation non autorisée des renseignements fiscaux, notamment les renseignements échangés, constitue une faute grave passible de licenciement. Outre le licenciement, l'usage indu d'informations fiscales, par inadvertance ou par négligence, peut entraîner des actions disciplinaires comprenant l'avertissement, la suspension temporaire ou la rétrogradation.

décourager les infractions et les violations.

Les sanctions peuvent être définies dans la législation fiscale, la législation pénale ou celle couvrant l'administration publique, voire une combinaison des trois. Il doit y avoir une combinaison appropriée de pénalités ou des sanctions administratives, civiles et/ou pénales, et que celles-ci couvrent un large éventail de violations de la confidentialité ou d'utilisations abusives des renseignements.

La gravité des sanctions (par exemple, l'avertissement, la suspension des fonctions, la sanction pécuniaire ou l'emprisonnement) est généralement fonction de la gravité et des conséquences des faits ayant entraîné leur application.

Les sanctions peuvent s'appliquer à toute personne en charge du traitement des renseignements fiscaux qui commettrait une violation :

- Le personnel, qu'il s'agisse d'employés permanents (par exemple, fonctionnaires titulaires) ou temporaires (contrats à durée déterminée, nominations temporaires).
- Les sous-traitants externes, qu'il s'agisse de personnes morales ou physiques.

Les sanctions doivent également s'appliquer aux personnes qui faisait anciennement partie du personnel ou des sous-traitants, une fois que leurs fonctions relatives au, ou en lien avec, le traitement des renseignements fiscaux ont cessé. L'encadré 43 donne un exemple de sanctions en cas de divulgation non autorisée de renseignements fiscaux.

SOUS-EXIGENCE 3.3.2 : PROCESSUS DE TRAITEMENT DES VIOLATIONS SUSPECTÉES OU AVÉRÉES OU AUTRES FORMES DE NON-RESPECT DE LA CONFIDENTIALITÉ, NOTAMMENT PAR L'APPLICATION DE SANCTIONS

Les dispositions relatives aux sanctions doivent être accompagnées par les processus et les ressources nécessaires pour garantir leur application effective. Il est également nécessaire de mettre en place des processus qui définissent les actions à entreprendre en cas de violation suspectée ou avérée ou en cas de non-respect des politiques, jusqu'à ce qu'il soit décidé d'appliquer la sanction appropriée (ou jusqu'à ce que la situation soit résolue de toute autre manière, sans qu'une sanction soit requise).

Lorsque la confidentialité des renseignements fiscaux est compromise, cela peut être le résultat d'un acte involontaire, d'une déficience des systèmes ou des procédures de protection de la confidentialité, ou encore le résultat d'actions intentionnelles au profit personnel d'une ou plusieurs personnes (par exemple en cas de corruption).

Qu'il s'agisse d'actions intentionnelles ou non, toute violation de la confidentialité doit être prise au sérieux et traitée immédiatement. Les actions requises dépendront des circonstances de la violation. Lorsque l'infraction résulte d'un acte intentionnel à des fins personnelles, il convient généralement de la signaler aux autorités compétentes pour d'éventuelles poursuites pénales.

Le fait de planifier et de se préparer à l'avance aux violations de la confidentialité - c'est-à-dire de disposer de processus pour les traiter - permet aux juridictions de gérer les situations avec davantage de rapidité et d'efficacité. Un système efficace de gestion des violations requiert des processus établissant les modalités de signalement, de remontée de l'information, d'enquête et de discipline, ainsi que le rôle et les responsabilités des parties prenantes à chaque étape. Ces processus doivent prévoir différents scénarios de violation, assortis de divers degrés de gravité. Le cas échéant, ils doivent être revus et améliorés sur la base de l'expérience acquise suite à leur application.

La SE 3.3.2 exige la mise en place de quatre types de processus en matière de violation, notamment ceux qui concernent les renseignements échangés, comme décrit dans la figure 21.

Le Forum mondial a préparé des orientations plus détaillées sur les bonnes pratiques en matière de traitement des violations de données et les exigences de la SE 3.3.2, ces conseils pouvant être transmis aux juridictions sur demande.

Dispositions coercitives et processus pour traiter les violations des obligations de confidentialité (Exigence fondamentale 3.3)

Sous-exigence 3.3.2.1. Processus en cas de violation suspectée ou avérée, pour assurer le signalement et l'enquête

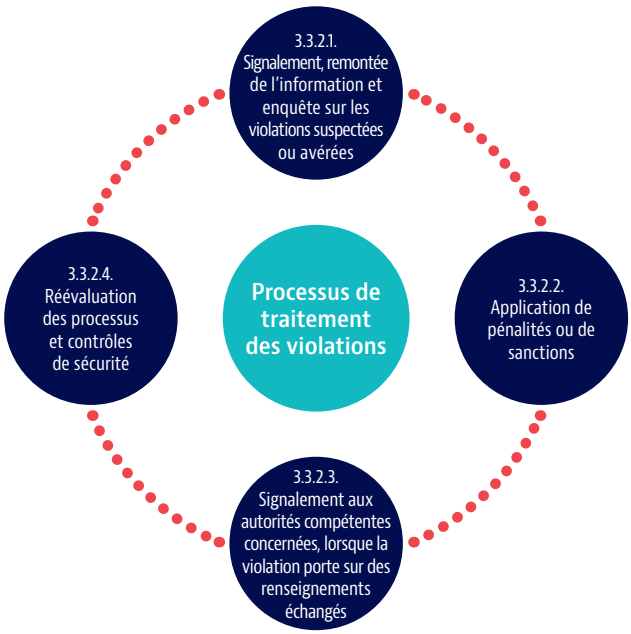
La SE 3.3.2.1 exige que les juridictions mettent en place des processus à suivre en cas d'accès, d'utilisation ou de divulgation non autorisés, suspectés ou avérés, qui visent à garantir que ces infractions sont signalées et font l'objet d'une enquête. Ces aspects sont examinés ci-après.

Processus de signalement

Les processus des administrations fiscales doivent prévoir des mesures pour que le personnel signale les violations suspectées ou avérées des données confidentielles, notamment les renseignements échangés, et les étapes relatives au signalement et à l'enregistrement d'un incident, et à la remontée des informations. Ces processus doivent être documentés et mis à la disposition du personnel pour en faciliter la consultation, afin que chacun ait connaissance de la chaîne pertinente de signalement ou de remontée des informations. Le personnel doit également être formé. Le département de la sécurité au sein des administrations fiscales est généralement chargé de recevoir les signalements.

Par exemple, les processus peuvent prévoir que le personnel signale par écrit les violations de confidentialité suspectées ou avérées à leur supérieur direct, ou au responsable désigné qui, si nécessaire ou selon la gravité de l'incident, fera remonter l'information à l'encadrement supérieur, comme le directeur de l'administration fiscale.

FIGURE 21. **Principaux éléments de la gestion des violations de la confidentialité**



Ces processus peuvent également prévoir que le responsable désigné fasse une enquête préliminaire auprès de la personne à l'origine du signalement et de la personne visée et/ou leurs responsables, avant de décider s'il y a lieu de déclencher une procédure de traitement de violation formelle, adossée à une enquête officielle.

Les processus peuvent exiger que le personnel émettant un signalement doive rendre compte de tous les faits ou éléments probants pertinents en leur possession, afin d'étayer leur suspicion ou leur déclaration. Il est également possible de prévoir un suivi auprès du personnel effectuant un signalement, pour obtenir toute information supplémentaire à cet égard.

Processus d'enquête

Lorsqu'un incident signalé requiert une enquête, celle-ci doit être menée de façon suffisamment large pour permettre de déterminer :

- Les circonstances qui ont entraîné l'infraction ou la violation.
- La ou les personnes responsable(s).
- Si possible, la cause de la violation.

Par conséquent, les processus des administrations fiscales doivent également comprendre des procédures d'enquête et de recueil des faits afin d'évaluer l'étendue et la gravité de la violation signalée. L'enquête ne doit entraver aucune mesure pouvant être immédiatement prise pour minimiser l'impact de la violation, comme la suppression de l'accès de l'auteur des faits aux systèmes d'information ou l'isolement de l'environnement physique ou informatique contenant les données compromises.

Les processus d'enquête couvrent généralement les aspects suivants :

- **Enquête préliminaire visant à déterminer la gravité d'une violation.** L'enquête préliminaire peut permettre de définir le type de violation (par exemple, une cyber-attaque, un vol de données par une personne interne à l'organisation, la perte de documents ou de supports d'information), l'étendue de la violation (quelques renseignements ou un ensemble complet de données), le type des renseignements concernés (données fiscales nationales, informations dans le cadre de l'EAR ou de l'échange de renseignements sur demande), ou toute juridiction partenaire en d'échange de renseignements impactée.
- **Identification de la ou des personnes chargées de l'enquête et des parties prenantes internes**

ou externes devant être impliquées. Le ou les responsables chargés de la supervision et de la coordination de l'enquête doivent être clairement identifiés. Les procédures peuvent également définir la coordination nécessaire entre les différents départements dans le cas où la gravité d'un incident requiert une enquête générale (par exemple, le département informatique, le département des audits internes et les unités opérationnelles concernées, telles que l'unité en charge de l'échange de renseignements). Il est également possible de déterminer la coordination avec les parties prenantes externes (par exemple, les contribuables affectés, les fournisseurs de données, les autorités de protection des données, la police et, si la violation concerne l'échange de renseignements, les autorités étrangères compétentes,). Dans le cas d'une violation grave, il peut être nécessaire de faire établir un rapport de police.

- **Procédures de recueil d'éléments probants.** Les éléments probants sont une partie essentielle du processus d'enquête, car ils permettent d'identifier la ou les personnes responsables et de favoriser la prévention de violations similaires à l'avenir. Ils sont prescrits pour une application adéquate des sanctions, notamment les sanctions pénales, le cas échéant. Des procédures claires doivent donc être mises en place pour la conduite des enquêtes et le recueil d'éléments probants, par exemple lorsqu'ils sont menés par le département des audits ou un département disciplinaire, et en coopération avec les autorités compétentes, le cas échéant.

- **Mesures intérimaires.** Pendant le déroulement d'une enquête, les procédures peuvent autoriser certaines actions administratives appropriées, comme le transfert ou la suspension de la ou des personnes suspectées ou clairement responsables des faits, afin de garantir l'impartialité et la transparence de l'enquête.

À la suite de l'enquête, un rapport doit être rédigé à l'attention l'encadrement supérieur de l'administration fiscale, établissant des recommandations pour toute action ou sanction à prendre à l'encontre de la ou des personnes responsables (les autorités de répression peuvent être impliquées en cas de divulgation intentionnelle suspectée).

Sous-exigence 3.3.2.2. Ressources, processus et procédures pour engager des mesures correctives et appliquer les sanctions appropriées lorsque les faits sont identifiés

Les processus des administrations fiscales doivent également garantir que des pénalités ou sanctions sont appliquées, sur la base du cadre juridique abordé dans la SE 3.3.1.

La SE 3.3.2.2 précise que les juridictions doivent, avec l'aide des ressources, des processus et des procédures administratifs adéquats, garantir que des mesures correctives sont prises lorsque les faits ont été identifiés, et que les pénalités ou sanctions appropriées sont appliquées à l'encontre des employés, sous-traitants ou autres personnes qui enfreignent les règles de confidentialité et les politiques ou procédures de sécurité, afin de décourager les autres de commettre des infractions similaires.

Les processus doivent décrire les étapes administratives conduisant à l'application de sanctions administratives ou disciplinaires telles que les avertissements, les suspensions, les rétrogradations, les baisses de salaire ou les licenciements, en fonction de la gravité de l'infraction.

Il existe généralement une autorité, au sein de l'administration fiscale ou dans le secteur public, chargée de l'application des sanctions administratives ou disciplinaires. Cette autorité détient les pouvoirs nécessaires pour appliquer les sanctions appropriées, ou pour transmettre l'affaire à la police ou aux autorités compétentes, le cas échéant. Les processus de transfert à la police des enquêtes et des poursuites pénales doivent être documentés. Les dispositions juridiques pouvant être invoquées dans l'application de pénalités administratives, civiles ou pécuniaires, ou dans le cadre de poursuites pénales, doivent également être documentées pour en faciliter la consultation.

Sous-exigence 3.3.2.3. Signalement aux autorités compétentes étrangères des violations de la confidentialité portant sur des renseignements échangés

Lorsque la violation de la confidentialité porte sur des renseignements échangés, l'un des aspects essentiels de la gestion et du traitement de cette violation réside dans la communication avec les partenaires en matière d'échange de renseignements.

En vertu des accords d'échange de renseignements, les juridictions sont généralement tenues d'informer rapidement les autorités compétentes partenaires qui ont fourni les renseignements divulgués ou utilisés de manière non autorisée, afin qu'elles puissent prendre les mesures appropriées en vertu de leur cadre juridique interne et des accords applicables[21]. Cette notification émise par la juridiction dans laquelle la violation est survenue a également pour but d'assurer aux partenaires

21. Dans le cas de certains accords multilatéraux, l'autorité compétente de la juridiction dans laquelle une violation des renseignements échangés a eu lieu doit informer le Secrétariat de l'Organe de coordination de l'accord, qui à son tour informera les autorités compétentes des autres parties à l'accord multilatéral afin de faciliter la communication. Il s'agit, par exemple, de l'Accord multilatéral entre Autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers, section 5(2), et de l'Accord multilatéral entre autorités compétentes portant sur l'échange des déclarations pays par pays, section 5(3).

en matière d'échange de renseignements que les causes vont être promptement et soigneusement investiguées, et que des mesures correctives vont être prises. Ces aspects sont essentiels pour maintenir la confiance dans l'échange international de renseignements fiscaux.

Par conséquent, la SE 3.3.2.3 exige que les juridictions disposent de processus de notification aux autres autorités compétentes de toute violation de la confidentialité ou de tout manquement la protection des renseignements échangés, et de toute sanction et mesure corrective qui en résulte.

Les notifications aux autorités compétentes étrangères doivent généralement comporter les éléments suivants :

- Le lieu où la violation est survenue (par exemple, quel organisme, quel département ou système de l'administration fiscale).
- Le type de violation (par exemple, une cyber-attaque, un vol de données par une personne en interne, la perte de documents ou de supports d'information).
- Le type de données concernées (par exemple, un fichier d'échange de renseignements sur demande ou des données échangées automatiquement).
- Les mesures prises pour circonscrire, juguler ou analyser la situation.
- Le point de contact central de l'administration fiscale et les autres interlocuteurs pertinents.

Après la notification initiale, il peut s'avérer judicieux, pour l'administration fiscale concernée, de continuer à communiquer avec ses partenaires en matière d'échange de renseignements pour mieux leur permettre de prendre les mesures adaptées au sein de leur propre juridiction (comme le respect de toute obligation légale nationale en matière de notification des contribuables affectés et des autorités de protection des données). Dans certains cas, il peut être nécessaire de faire des déclarations publiques.

La figure 22 décrit les possibles étapes de la communication requise dans le cas d'une violation de la confidentialité des renseignements échangés.

Sous-exigence 3.3.2.4. Réévaluation des contrôles de sécurité et des processus de surveillance et de sanction en cas de non-respect de la confidentialité

Il est crucial de tirer des leçons des incidents et infractions, afin de poursuivre l'amélioration des processus et contrôles visant à superviser, prévenir et traiter les incidents futurs.

La SE 3.3.2.4 prévoit ainsi que les juridictions réévaluent les processus de surveillance et de sanction en réponse aux cas de non-respect de la confidentialité, et que l'encadrement supérieur s'assurent que les modifications recommandées sont mises en œuvre.

FIGURE 22. **Étapes générales de la communication en cas de violation de la confidentialité de renseignements échangés**

Cela signifie que les administrations fiscales réévaluent fréquemment leurs processus de supervision, et de traitement des violations, ainsi que les contrôles de sécurité pertinents, non seulement dans le cadre des pratiques routinières des opérations de traitement abordées dans la SE 3.2.6, mais également sur la base des leçons tirées des cas de violation concrets.

Afin de favoriser cette réévaluation, les rapports préparés suite à la conclusion de l'enquête sur une violation peuvent recommander, outre les sanctions appropriées pour la ou les personnes responsables :

- Des mesures visant à minimiser les répercussions de la violation.
- Les actions futures pour éviter tout incident ou violation similaire.
- Les améliorations possibles (le cas échéant) des processus disciplinaires, administratifs, de signalement et d'enquête, pour appliquer les sanctions.

Les leçons tirées des cas d'incidents concrets doivent également être prises en compte dans des examens périodiques (par exemple, annuels ou semestriels) visant à :

- Identifier des stratégies à plus long terme pour minimiser plus encore la probabilité que de nouvelles violations aient lieu.
- Améliorer le processus de gestion des violations.

L'autorité chargée de l'enquête, les personnes responsables de la sécurité et de la confidentialité de l'information au sein de l'administration fiscale (par exemple, le RSSI), et/ou l'encadrement supérieur, sont donc responsables du suivi permettant d'assurer la mise en œuvre des recommandations d'amélioration découlant des cas de violation concrets ou de la réévaluation des processus.

La réévaluation des contrôles de sécurité et des processus de surveillance et de coercition peut avoir pour résultat :

- La mise en œuvre de mesures correctives dans les processus ayant fait l'objet d'une violation.
- L'examen des processus de recrutement ou d'implication du personnel (employés et sous-traitants externes).
- La mise en œuvre de programmes de formation périodiques pour un traitement sécurisé des données confidentielles et une meilleure sensibilisation à la sécurité.

Encadré 44. **Résumé d'un exemple de politique en matière de gestion des violations**

En vertu de la politique en matière de signalement des violations de la confidentialité et des incidents de sécurité de l'administration fiscale de la Juridiction B, l'ensemble du personnel et des sous-traitants externes doit signaler par écrit, au RSSI, toute violation suspectée ou avérée de la confidentialité ou tout incident de violation des politiques de sécurité de l'information. La politique définit les responsabilités et les rôles des différents employés et sous-traitants à travers le processus de signalement et d'enquête.

Au terme de l'enquête, le responsable hiérarchique du processus opérationnel affecté doit élaborer un rapport, sur les conseils du RSSI, détaillant l'incident, une évaluation de sa gravité et ses causes probables. Selon la nature, l'étendue et la gravité de l'incident, le responsable hiérarchique des opérations concernées peut décider de faire remonter l'information à l'organisme de protection de l'information et/ou signaler l'incident à la police.

En vertu de cette politique, des mesures correctives doivent être appliquées afin de résoudre la défaillance qui a provoqué la violation. Si la violation implique des renseignements échangés, l'incident doit être signalé au(x) partenaire(s) d'échange de renseignements correspondant(s) et, le cas échéant, au Secrétariat de l'Organe de coordination de l'accord multilatéral d'échange de renseignements applicable.

Le rapport du responsable hiérarchique doit recommander des actions disciplinaires appropriées à prendre à l'encontre du ou des auteur(s) des faits. Ces actions peuvent comprendre l'avertissement, le licenciement, la suspension, la rétrogradation et la baisse de salaire.

Une fois l'incident traité et l'enquête finalisée, le RSSI doit préparer un rapport à l'attention du conseil de l'administration fiscale, en indiquant si des mesures sont recommandées pour améliorer les politiques, les processus ou les contrôles de sécurité concernés.

- L'examen et l'amélioration des contrôles en matière de gestion de la sécurité de l'information, comme les droits d'accès.
- L'exécution d'exercices plus fréquents de réponse aux violations de données.

Pour un exemple de processus visant à traiter les violations de données confidentielles, voir l'encadré 44.

Annexes

Annexe A. Glossaire des concepts

CONCEPT	DESCRIPTION	SE
Accès logique	Accès aux systèmes par les processus d'identification, d'authentification et d'autorisation.	**3.2.3**
Accès physique	Accès à des zones spécifiques sur site.	**3.2.3**
Accord de niveau de service	Accord qui définit le niveau de service minimum qu'une entité proposant un service doit respecter.	**3.2.4**
Accord de non-divulgation	Entente formelle ou contrat définissant les règles de non-divulgation des informations confidentielles à des tiers.	**3.2.2**
Actif	Tout élément de valeur qui contribue à l'exécution de processus et à la production de résultats. Il peut notamment s'agir d'informations, de personnes, de services, d'équipements ou de systèmes.	**3.2.1**
Atténuation des risques	Application active de mesures visant à réduire l'impact d'un risque ou la probabilité qu'il se concrétise.	**3.2.1**
Authentification	Lorsqu'un utilisateur accède aux systèmes informatiques, le processus d'authentification garantit et confirme l'identité de l'utilisateur en se basant sur le principe de non-répudiation.	**3.2.3**
Autorisation	Processus qui permet à un utilisateur authentifié sur un système d'accéder à des ressources selon les principes du « besoin d'en connaître » et du « moindre privilège ».	**3.2.3**
Autorité compétente	Il s'agit de la ou des personnes ou de la ou des autorités gouvernementales désignées par une juridiction comme personne compétente pour échanger des informations conformément à tout accord d'échange international.	**3.1.1, 3.2.5**
Besoin d'en connaître	Principe de la gestion des accès selon lequel les informations sur les contribuables ne doivent être accessibles qu'au personnel ayant un motif professionnel légitime de les consulter.	**3.2.3**
Cadre de GSI	Cadre de gestion de la sécurité de l'information, à savoir les structures organisationnelles et principes généraux de cette sécurité, visant à orienter les administrations fiscales vers la réalisation des objectifs de GSI, selon une approche fondée sur le risque. La responsabilité de ce cadre incombe ultimement à l'encadrement supérieur de l'administration fiscale.	**3.2.1**
Centre des opérations de sécurité	Équipe d'experts et systèmes pour le suivi et l'analyse permanents de la sécurité de l'administration fiscale	**3.2.6**
Chiffrement	Mécanisme de protection des données destiné à faire en sorte qu'elles ne soient accessibles que si l'on possède la clef de chiffrement.	**3.2.5**

Annexes

CONCEPT	DESCRIPTION	SE
Classification des informations	Processus d'identification des types d'informations que les administrations fiscales détiennent et de détermination du niveau de protection qu'elles doivent recevoir.	**3.2.5**
Contrôle	Voir Pratique	**3.2.1**
Contrôle de sécurité informatique	Mesure administrative, technique ou physique mise en œuvre pour atténuer un risque informatique	**3.2.4**
Contrôles d'accès	Contrôles de sécurité garantissant que l'accès aux informations, aux locaux et aux systèmes est accordé selon les principes du « besoin d'en connaître » et des « droits strictement nécessaires ».	**3.2.3**
Contrôles de base	Ensemble de contrôles de sécurité minimum qu'une administration fiscale applique à certains risques, quelle que soit leur gravité.	**3.2.4**
Conventions de dénomination	Règles régissant la manière dont sont désignées les informations afin de les discerner clairement les unes des autres.	**3.2.1**
Durée de conservation	Exigence légale de conservation des informations pendant une période fixe même si les informations ne sont plus nécessaires à des fins d'activité fiscale.	**3.2.5**
Externalisation	Recours à un prestataire externe pour la fourniture de biens et services.	**3.2.4**
Fonction Audit	Vérification complète et objective permettant d'évaluer la conformité avec les processus définis dans les politiques et procédures relativement au système GSI. Les résultats et conclusions de l'audit doivent être directement soumis au directeur de l'administration fiscale.	**3.2.6**
Formation	Accompagnement du personnel de l'administration fiscale (salariés/sous-traitants) pour qu'il acquière et développe les connaissances, les aptitudes et les compétences de base nécessaires pour intégrer la confidentialité et la sécurité dans les processus fiscaux.	**3.2.2**
Fourniture d'accès	Le fait d'accorder l'accès aux informations par la création de comptes utilisateur, la gestion des mots de passe et l'attribution de droits d'accès et d'autorisations spécifiques aux utilisateurs.	**3.2.3**
Gestion de la continuité des activités	Processus de gestion visant à assurer la poursuite des activités dans le cas où un événement quelconque perturberait le fonctionnement normal.	**3.2.1**
Gestion des accès	Politiques, processus et procédures, relevant de la haute direction, pas uniquement de la fonction informatique de l'administration fiscale, qui régissent les accès physiques et logiques, et processus effectifs relatifs à l'octroi et l'audit de l'accès logique et à l'identification et l'authentification des utilisateurs.	**3.2.3**
Gestion des actifs	Processus qui garantit que les actifs de l'administration fiscale sont identifiés et suivis depuis leur création/achat jusqu'à leur destruction/mise au rebut.	**3.2.4**

CONCEPT	DESCRIPTION	SE
Gestion des changements	Gestion contrôlée du développement de nouveaux systèmes et services et apport de modifications majeures aux systèmes et services existants.	**3.2.6**
Gestion des fournisseurs	Processus basé sur le risque et qui garantit qu'un prestataire externe qui accède aux données ou aux bâtiments de l'administration fiscale ne fait pas peser de risque sur la confidentialité et la sécurité.	**3.2.4**
Gestion des incidents	Identification, documentation et gestion des incidents de sécurité, dans le domaine informatique et autres domaines.	**3.2.6**
Gestion des journaux	Politiques et processus collectifs utilisés pour administrer et faciliter la création, la transmission, l'analyse, le stockage, l'archivage et l'élimination finale de volumes importants de données journal créées dans un système informatique.	**3.2.6**
Gestion des vulnérabilités	Processus et procédures pour l'identification et la gestion des vulnérabilités.	**3.2.6**
Hameçonnage	(Phishing en anglais) Type d'escroquerie en ligne au cours de laquelle des criminels envoient des courriels frauduleux conçus pour sembler provenir d'une source légitime et tromper le destinataire de façon à lui extorquer des informations confidentielles telles que des identifiants d'accès aux systèmes.	**3.2.2**
Identification	Processus utilisé par les systèmes informatiques pour identifier un utilisateur doté d'un droit d'accès en l'individualisant.	**3.2.3**
Ingénierie sociale	Pratique de manipulation qui exploite la nature confiante du personnel dans un but malveillant, afin d'obtenir des informations qui peuvent être utilisées à des fins personnelles. Également appelée piratage psychologique.	**3.2.2**
Journal	Un journal, en langage informatique, désigne l'historique des événements relatifs à un système informatique donné, produit de façon automatique et horodaté. Il est possible également de créer manuellement des journaux pour les activités non informatiques.	**3.2.6**
Journalisation	Opération consistant, pour les administrations fiscales, à enregistrer et conserver une trace de tous les accès aux données protégées, y compris l'accès aux installations et espaces où les données sont conservées, et notamment aux systèmes contenant les dossiers des contribuables et autres informations sensibles.	**3.2.6**
Logiciel malveillant	Logiciel à caractère malveillant. Programme créé pour exploiter une vulnérabilité dans un système ciblé afin de l'endommager ou de voler des informations.	**3.2.4**
Mise à disposition de l'accès	Le fait d'accorder l'accès aux informations par la création de comptes utilisateur, la gestion des mots de passe et l'attribution de droits d'accès et d'autorisations spécifiques aux utilisateurs.	**3.2.3**

Annexes

CONCEPT	DESCRIPTION	SE
Moindre privilège	(Droits strictement nécessaires) Principe de la gestion des accès selon lequel l'accès légitime doit être limité aux fonctions spécifiques minimales dont l'utilisateur a besoin pour effectuer son travail.	**3.2.3**
Nettoyage des supports	Il s'agit du processus de traitement de données conservées sur un support de stockage et permettant de réduire le risque de récupération et de reconstruction à un niveau acceptable.	**3.2.5**
Pare-feu	Équipement placé au niveau de points stratégiques d'un réseau (généralement ceux faisant face à un accès externe ou Internet et à des zones internes séparées) et qui autorise ou bloque le trafic en fonction de règles.	**3.2.4**
Politique	Énoncé par lequel une administration fiscale documente la mise en œuvre de processus, procédures et contrôles de sécurité dans un domaine donné. Une politique répond à la question : « quelles mesures doivent être prises ? ». Les politiques doivent être hiérarchisées. Par exemple, une politique d'identification et d'authentification pour les accès aux systèmes informatiques sera subordonnée à une politique générale de gestion des accès. Une politique de Gestion de la sécurité de l'information globale énonçant les principes de sécurité fondamentaux qui s'appliquent à toutes les politiques doit également être élaborée.	**3.2.1**
Politique de GSI	Politique qui formalise les intentions de l'administration fiscale en ce qui concerne son approche de la sécurité de l'information. Elle doit définir le champ d'application du SGSI et les objectifs généraux en matière de gestion de la sécurité de l'information auxquels chacune des autres politiques doit se conformer.	**3.2.1**
Politique du bureau propre	Une politique du bureau propre spécifie la façon dont les employés doivent laisser leur espace de travail lorsqu'ils quittent leur bureau afin de garantir la confidentialité des informations.	**3.2.5**
Politique d'utilisation acceptable	Ensemble de règles qui établissent les pratiques autorisées et interdites en rapport avec les systèmes d'informations contenant des informations confidentielles.	**3.2.5**
Pratique ou contrôle	Mesure spécifique utilisée pour gérer le risque lié à la sécurité de l'information (c'est-à-dire atténuer ou éliminer un risque). Par contrôles, on entend notamment les processus et procédures, mais également les programmes, les outils, les techniques, les technologies et les dispositifs informatiques. S'agissant de contrer un risque identifié, les contrôles sont parfois appelés mesures de protection ou contre-mesures.	**3.2.1**
Procédure	Ensemble documenté d'étapes et d'activités visant à mettre en œuvre des politiques de sécurité. Une procédure répond à la question : « comment appliquer les mesures requises et qui doit s'en charger ? ». Le terme « procédure » est souvent associé au terme « processus » (dans l'expression « processus et procédures »), car une procédure est généralement une représentation plus détaillée de chaque étape d'un processus. Bien souvent, il peut exister plus d'une procédure pour chaque étape d'un processus. Par exemple, un processus peut concerner le dépôt d'une déclaration fiscale, mais comme ce dépôt peut s'effectuer par différentes méthodes, chaque méthode peut être régie par une procédure particulière.	**3.2.1**

CONCEPT	DESCRIPTION	SE
Processus	Séquence reproductible d'actions dont les résultats sont mesurables. Le processus est un concept essentiel pour la GSI. L'amélioration des processus et de la sécurité exige de pouvoir mesurer les résultats et d'agir en conséquence. Les processus peuvent aller de processus administratifs en matière fiscale, tels que le dépôt et l'examen des déclarations de revenu, à la mise à jour de logiciels informatiques. Toute action qui n'est pas couverte par un processus défini constitue par définition un risque pour la sécurité, puisqu'il n'y a aucune garantie de reproductibilité, ni aucune mesure ou amélioration des résultats.	**3.2.1**
Récupération	Fait référence à la restauration des services et des opérations d'exploitation en cas de dysfonctionnement majeur.	**3.2.4**
Résilience	Fait référence à l'atténuation du risque d'interruption de service et à la garantie d'une tolérance aux pannes dans les services en proposant jusqu'à un certain point une continuité du service.	**3.2.4**
Risque posé à la sécurité de l'information	Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un préjudice à l'organisation.	**3.2.1**
Sécurité de l'information	Protection de la confidentialité, de l'intégrité et de la disponibilité des informations.	**3.2.1**
Sensibilisation	Pratique consistant à exposer régulièrement le personnel à des messages les mettant en garde contre les menaces/risques informatiques ou de sécurité, ces messages étant généralement communiqués simultanément à tous les membres du personnel d'un domaine particulier ou de l'ensemble de l'administration fiscale, et même aux tiers externes, etc.	**3.2.2**
SGSI	Système de gestion de la sécurité de l'information regroupant les politiques, procédures et contrôles de sécurité propres à un domaine déployés pour mettre en œuvre le cadre de GSI. La responsabilité du SGSI incombe ultimement à la haute direction de l'encadrement supérieur de l'administration fiscale.	**3.2.1**
Test d'intrusion	Le test d'intrusion simule efficacement les actions d'un pirate informatique contre l'organisation	**3.2.4, 3.2.5**
Utilisateur légitime	Utilisateur qui obtient un droit d'accès spécifique en vertu des principes du « besoin d'en connaître » et du « moindre privilège ».	**3.2.3**
Vulnérabilité	Faille dans la conception d'un actif ou liée à sa nature.	**3.2.1, 3.2.6**

Note : Il peut exister, parmi les sources de référence pertinentes, des définitions officielles de ces concepts, mais les définitions données ici sont celles que nous utilisons aux fins de la boîte à outils sur la gestion de la sécurité de l'information.

Annex B. Ressources utiles

Informations pertinentes sur les normes internationales en matière de transparence fiscale et d'échange de renseignements

- Modèle d'accord entre autorités compétentes aux fins de la norme en matière d'échange automatique de renseignements :
  https://www.oecd.org/fr/fiscalite/echange-de-renseignements-fiscaux/norme-d-echange-automatique-de-renseignement-relatifs-aux-comptes-financiers-en-matiere-fiscale-seconde-edition-9789264268050-fr.htm

- Norme en matière d'échange de renseignements sur demande :
  http://www.oecd.org/tax/transparency/documents/handbook-french-eoi-2016-2020.pdf

- Plan d'action du Forum mondial pour la participation des pays en développement à l'échange automatique de renseignements :
  https://www.oecd.org/tax/transparency/plan-action-aeoi-pays-en-developpement.pdf

- Termes de référence pour le processus d'examen par les pairs de l'échange automatique de renseignements :
  https://www.oecd.org/fr/fiscalite/transparence/documents/termes-de-reference-echange-automatique.pdf

- Termes de référence pour l'examen des mesures de confidentialité et de protection des données :
  https://www.oecd.org/fr/fiscalite/transparence/documents/confidentialite-protection-des-donnees-tdr.pdf

- Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales :
  http://www.oecd.org/fr/fiscalite/transparence/

- Échange de renseignements sur demande :
  http://www.oecd.org/fr/fiscalite/transparence/notre-action/echange-sur-demande/echange-de-renseignements-sur-demande-examen-par-les-pairs.htm

- Échange automatique de renseignements :
  http://www.oecd.org/tax/automatic-exchange/

  https://read.oecd-ilibrary.org/taxation/norme-d-echange-automatique-de-renseignement-relatifs-aux-comptes-financiers-en-matiere-fiscale-seconde-edition_9789264268050-fr

- Norme commune de déclaration :
  https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/

- Assistance technique fournie par le Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales :
  https://www.oecd.org/fr/fiscalite/transparence/notre-action/

- Guide de l'OCDE sur la protection de la confidentialité des renseignements échangés à des fins fiscales :
  https://www.oecd.org/fr/fiscalite/echange-de-renseignements-fiscaux/rapport-garantir-la-confidentialite.pdf

Modèles d'accords d'échange de renseignements à des fins fiscales

- Modèle de Convention fiscale de l'OCDE concernant le revenu et la fortune : https://read.oecd-ilibrary.org/taxation/modele-de-convention-fiscale-concernant-le-revenu-et-la-fortune-2017-version-complete_0faf9b6c-fr

- Modèle d'accord de l'OCDE sur l'échange de renseignements à des fins fiscales : https://www.oecd.org/tax/exchange-of-tax-information/2082215.pdf

- Modèle de convention fiscale des Nations Unies entre pays développés et pays en développement : https://www.un.org/esa/ffd/wp-content/uploads/2015/02/UN_Model2011_UpdateFr.pdf

- Convention concernant l'assistance administrative mutuelle en matière fiscale : https://read.oecd-ilibrary.org/taxation/la-convention-multilaterale-concernant-l-assistance-administrative-mutuelle-en-matiere-fiscale_9789264115682-fr

OCDE

DES POLITIQUES MEILLEURES
POUR UNE VIE MEILLEURE

Pour plus d'informations :

www.oecd.org/fr/fiscalite/transparence

gftaxcooperation@oecd.org

@OECDtax | #TransparenceFiscale