TRANSPARENCY INTERNATIONAL
the global coalition against corruption

SYSTEMES D'ALERTE INTERNE

Grille d'auto-évaluation

Transparency International est un mouvement mondial réuni autour d'une vision : un monde dans lequel les gouvernements, les entreprises, la société civile et la vie quotidienne des citoyens sont exempts de corruption. Avec plus de 100 sections nationales et un secrétariat international à Berlin, nous luttons pour faire de cette vision une réalité.

www.transparency.org

Systèmes d'alerte interne

Grille d'auto-évaluation pour les organisations publiques et privées

Auteur : Marie Terracol

ISBN : 978-3-96076-259-1

Cette publication a été réalisée dans le cadre du projet "SAFE4Whistleblowers", financé par l'Union européenne. Les points de vue et les opinions exprimés sont toutefois ceux des auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'autorité qui l'a financée ne peuvent en être tenues pour responsables.

TABLE DES MATIERES

REMERCIEMENTS

Transparency International tient à remercier les personnes et les organisations suivantes qui ont fourni des informations et une expertise qui ont grandement contribué à l'élaboration de cette grille d'auto-évaluation.

Alessia Rizzo, Transparency International Italia

Céline Pinzio, Transparency International

David Martinez, Transparency International España

Giorgio Fraschini, Transparency International Italia

Giovanni Pellerano, Whistleblowing Solutions

Ida Nowers, Transparency International Irlande

Irina Lonean, Transparency International Roumanie

Isabel Buechner, Transparency International

Jan Dupák, Transparency International Tchèque

Judit Zeisler, Transparency International Hongrie

John Devitt, Transparency International Irlande

Kremena Chobanova, Transparency International Bulgarie

Krista Asmusa, Transparency International Lettonie (DELNA)

Kristina Marova, Transparency International Slovaquie

Laurence Fabre, Transparency International France

Lousewies Van Der Laan, Transparency International Pays-Bas

Lotta Rydstrom, Transparency International Suède

Lotte Rooijendijk, Transparency International Pays-Bas

Martim Agarez, Transparency International Portugal

Miklos Ligeti, Transparency International Hongrie

Susanna Ferro, Whistleblowing Solutions

Zuzana Grochalová, Transparency International Slovaquie

Protect, the UK's whistleblowing charity

GLOSSAIRE

Système d'alerte interne : objectifs, politiques, procédures, processus, lignes directrices et outils d'une organisation en matière d'alerte.

Responsable ou bureau d'alerte : personne ou service responsable du fonctionnement du système d'alerte interne.

Signalement : communication d'informations sur des actes répréhensibles présumés (voir ci-dessous) à des personnes ou à des entités dont on pense qu'elles sont en mesure d'agir.

Acte répréhensible : un acte ou une omission qui est illégal, abusif ou qui peut causer un préjudice.

Lanceur d'alerte : toute personne qui rapporte ou divulgue des informations sur des actes répréhensibles présumés, acquises dans le cadre de ses activités professionnelles, en étant raisonnablement convaincue que les informations rapportées étaient vraies au moment où elles ont été rapportées.

Rapport interne : rapport de signalement effectué au sein d'une organisation publique ou privée (c'est-à-dire sur le lieu de travail).

Rapport externe : rapport de signalement adressé à une autorité compétente.

Divulgation publique : rendre des informations sur des actes répréhensibles disponibles dans le domaine public, soit en les publiant - par exemple, sur des plateformes en ligne ou des réseaux sociaux - soit en les signalant à des parties prenantes telles que les médias, les élus, les organisations de la société civile, les syndicats ou les organisations commerciales/professionnelles.

Comportement préjudiciable : toute menace, recommandation ou action ou omission réelle, directe ou indirecte, qui cause ou peut causer un préjudice, et qui est liée à un signalement réel ou présumé ou qui en résulte.

Personne concernée : une personne physique ou morale mentionnée dans le rapport ou la plainte d'un lanceur d'alerte comme étant responsable de l'acte répréhensible ou du comportement préjudiciable suspecté, ou associée à cette personne.

Tiers protégés : personnes autres que le lanceur d'alerte qui risquent d'être victimes d'un comportement préjudiciable lié à l'alerte.

Personnel : les administrateurs, les dirigeants, les employés, le personnel temporaire ou les travailleurs, les stagiaires et les internes d'une organisation.

Représentants du personnel : personnes reconnues comme telles par la législation ou la pratique nationale, qu'il s'agisse de représentants syndicaux ou de représentants élus (par exemple, les comités d'entreprise).

Top management : personne ou groupe de personnes qui dirigent et contrôlent une organisation au plus haut niveau (c'est-à-dire les dirigeants).[1]

Organe directeur : personne ou groupe de personnes qui a la responsabilité ultime de l'ensemble d'une organisation.[2]

[1] ISO 37002:2021, Systèmes de gestion des alertes - Lignes directrices.
[2] ISO 37002:2021, Systèmes de gestion des alertes - Lignes directrices.

ACRONYMES

DEI : Diversité, équité et inclusion

DPA : Accord sur la protection des données (data processing agreement)

ESG : Environnement, social et gouvernance

GESI : Genre, égalité et inclusion sociale

ISO : Organisation internationale de normalisation

OSC : Organisation de la société civile

RH : Ressources humaines

RSE : Responsabilité sociale des entreprises

SAI : Système d'alerte interne (*Internal whistleblowing system*)

SRI : Indicateur synthétique de risque (*Synthetic risk indicator*)

UE : Union européenne

INTRODUCTION

Le signalement par les lanceurs d'alerte est l'un des moyens les plus efficaces de mettre au jour la corruption, la fraude, la mauvaise gestion et d'autres actes répréhensibles qui menacent la santé et la sécurité publiques, l'intégrité financière, les droits de l'homme et l'environnement.

Le signalement, ou alerte, est la divulgation d'informations sur des actes répréhensibles présumés à des personnes ou à des entités dont on pense qu'elles sont en capacité de prendre des mesures. Les organisations elles-mêmes sont souvent les mieux placées pour traiter les actes répréhensibles commis dans le cadre de leurs attributions et, dans la pratique, la plupart des lanceurs d'alertes signalent d'abord les actes répréhensibles présumés au sein de leur organisation. Il est donc essentiel que les organisations, qu'il s'agisse d'entreprises privées ou d'institutions publiques, mettent en place des mécanismes sûrs et efficaces pour recevoir et traiter ces rapports, ainsi qu'une protection solide pour les lanceurs d'alerte.

Par conséquent, un nombre croissant de législations nationales exigent des organisations qu'elles mettent en place un système d'alerte interne (SAI), également connu sous le nom de "speak up" ou de systèmes de signalement interne. C'est le cas, par exemple, dans les pays de l'Union européenne (UE), en vertu de la directive européenne de 2019 sur la protection des lanceurs d'alerte.

Les organisations doivent considérer un système d'alerte interne comme étant plus qu'une simple obligation légale. Un système d'alerte interne efficace permet non seulement de préserver l'intérêt public, mais aussi de protéger les organisations contre les répercussions d'une mauvaise conduite, telles que les responsabilités juridiques, les atteintes à la réputation et les pertes financières importantes. À ce titre, un système d'alerte interne est considéré comme essentiel dans le contexte des pratiques environnementales, sociales et de gouvernance (ESG).[3]

En permettant au personnel et aux autres parties prenantes concernées de dénoncer les comportements illégaux ou contraires à l'éthique, les systèmes d'alerte interne favorisent une culture organisationnelle de confiance, de transparence et de responsabilité. Ces systèmes apportent donc de réels avantages à la culture, à la marque, à la création de valeur et à la croissance d'une organisation.[4]

Transparency International a développé cette grille d'auto-évaluation pour aider les organisations à établir, mettre en œuvre et réviser leurs systèmes internes de signalement, afin qu'ils soient efficaces et conformes aux meilleures pratiques et aux normes internationales, aux *meilleures pratiques SAI* de Transparency International *pour les organisations publiques et privées* et aux lignes directrices ISO pour les systèmes de gestion des alertes. Bien qu'il s'agisse d'une grille d'"auto-évaluation", cet outil peut également être utilisé par des organisations tierces, telles que des OSC, des autorités et des cabinets de conseil, pour réaliser une évaluation approfondie des systèmes

[3] Par exemple, l'existence d'un système d'alerte interne est l'un des principaux critères de notation ESG de Morgan Stanley Capital International (MSCI) et des normes européennes d'information sur le développement durable (European Sustainability Reporting Standards).

[4] Voir,par exemple, Stephen Stubben et Kyle Welch (2020), Evidence on the Use and Efficacy of Internal Whistleblowing Systems ; Bussmann, K-D. & Niemeczek, A. (2019), Compliance through company culture and values : Une étude internationale basée sur l'exemple de la prévention de la corruption. *Journal of Business Ethics*, 157(3), 797-811 ; Kaptein, M. (2011), De l'inaction à l'alerte externe : The influence of the ethical culture of organizations on employee responses to observed wrongdoing, *Journal of Business Ethics*, 98, 513-530 ; Mayer, D.M., Nurmohamed, S., Klebe Treviño, L., Shapiro, D.L. & Schminke, M. (2013), Encouraging Employees to Report Unethical Conduct Internally : It Takes a Village. *Organizational Behavior and Human Decision Processes*, 121, 89-103 ; Seifert, D.L., Sweeney, J.T., Joireman, J. & Thornton, J.M. (2010). The influence of organizational justice on accountant whistleblowing. *Accounting, Organizations and Society*, 35(7), 707-717.

d'alerte interne d'une organisation, soit en collaboration avec cette dernière, soit sur la base de données publiquement disponibles.[5]

La grille d'auto-évaluation s'adresse aux organisations de tous les secteurs - public, privé et "troisième" secteur - et de toutes les juridictions, y compris les organisations internationales telles que les Nations unies. Il vise également à aider les organisations opérant au sein de l'UE à respecter leurs obligations au titre de la directive européenne sur la protection des lanceurs d'alerte.

Les organisations devraient utiliser la grille d'auto-évaluation en même temps que les principes et lignes directrices susmentionnés.

QUI DOIT METTRE EN PLACE DES SYSTEMES D'ALERTE INTERNE ?

Toutes les organisations publiques et la plupart des organisations privées devraient disposer d'un système d'alerte interne.

Toutes les organisations publiques

Toutes les entités publiques, au niveau local, régional, national ou international, sans exception et quelle que soit leur taille, doivent mettre en œuvre un système d'alerte interne. Cela inclut celles qui sont détenues ou contrôlées par l'État, telles que les entreprises publiques.[6] Les entités doivent établir et mettre en œuvre un indicateur synthétique de risque (SRI) selon des modalités adaptées à leur taille et à leur exposition aux risques. Les petites autorités locales, telles que les municipalités, pourraient partager les ressources - par exemple, au niveau local supérieur - pour la réception des rapports et les enquêtes qui s'ensuivent. Toutefois, la responsabilité de préserver la confidentialité, de fournir un retour d'information au lanceur d'alerte et de traiter l'acte répréhensible signalé incombe à chaque organisation concernée.[7]

La plupart des organisations privées[8]

- Toutes les moyennes et grandes entités privées employant 50 personnes ou plus doivent mettre en œuvre un système d'alerte interne, de même que toutes les entités du secteur des services financiers, quelle que soit leur taille.[9] Il s'agit aussi bien d'entreprises que d'organisations à but non lucratif.
- Il est vivement conseillé aux petites entités privées comptant moins de 50 employés de mettre en œuvre un système d'alerte interne, en particulier lorsque la nature de leurs activités les expose à des risques de corruption ou présente d'autres risques pour l'intérêt public - par exemple, pour les droits de l'homme,

[5] Les évaluateurs tiers doivent reconnaître les limites inhérentes à une évaluation basée uniquement sur des données accessibles au public.
[6] La directive européenne permet aux États membres de l'UE d'exempter les municipalités de moins de 10 000 habitants ou de moins de 50 travailleurs, ainsi que les autres entités publiques de moins de 50 travailleurs, de l'obligation de mettre en œuvre un système d'alerte interne. La règle varie donc d'un pays de l'UE à l'autre.
[7] Même les petites municipalités prennent régulièrement des décisions dans des domaines à haut risque, tels que les marchés publics, la protection de l'environnement et la santé publique, ce qui rend la présence d'un système d'alerte interne essentielle. La directive européenne permet aux municipalités de disposer de canaux de signalement communs ou partagés, mais elles doivent toujours mettre en œuvre leurs propres procédures pour tous les autres aspects d'un système d'alerte interne.
[8] Les organisations privées comprennent les organisations du troisième secteur, c'est-à-dire les organisations à but non lucratif telles que les organisations de la société civile, les associations caritatives et les organisations non gouvernementales.
[9] Cela s'explique par les risques particuliers de blanchiment d'argent et de financement du terrorisme. La plupart des entités privées qui fournissent des services, des produits et des marchés financiers dans l'UE sont tenues de mettre en œuvre les systèmes d'alerte interne en vertu de diverses directives européennes.

l'environnement ou la santé publique. Les entreprises qui font partie d'un groupe doivent disposer d'un système d'alerte interne, quelle que soit leur taille.[10]

- Les petites et moyennes entités privées comptant moins de 250 employés pourraient choisir de partager les ressources pour la réception des rapports et toute enquête ultérieure. Toutefois, comme dans le secteur public, la responsabilité de préserver la confidentialité, de fournir un retour d'information au lanceur d'alerte et de traiter l'acte répréhensible signalé incombe à chaque organisation concernée.

Protection universelle des lanceurs d'alerte

Toutes les entités, qu'elles aient ou non mis en place un SAI formel, doivent adopter une approche de tolérance zéro à l'égard des comportements préjudiciables aux lanceurs d'alerte. Elles doivent également faciliter les signalements d'actes répréhensibles et donner suite aux préoccupations lorsque cela est possible.

LA DIRECTIVE EUROPÉENNE SUR LA PROTECTION DES LANCEURS D'ALERTE

En 2019, l'Union européenne a adopté la "Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 relative à la protection des personnes qui signalent des violations du droit de l'Union" (directive sur la protection des lanceurs d'alerte). Les 27 États membres de l'UE avaient deux ans, jusqu'en décembre 2021, pour se conformer à la directive, bien que la plupart d'entre eux n'aient pas respecté le délai.[11]

La directive prévoit des normes minimales communes strictes pour la protection des lanceurs d'alerte en Europe. Les États membres sont tenus de transposer ces dispositions conformément à l'esprit de la directive, qui est d'offrir un niveau élevé de protection aux lanceurs d'alerte.

Principales dispositions de la directive européenne sur les lanceurs d'alerte :

- La directive couvre à la fois le secteur public et le secteur privé.
- Elle couvre un large éventail de lanceurs d'alerte potentiels, y compris les personnes qui ne sont pas dans la relation traditionnelle employé-employeur, comme les consultants, les contractants et les bénévoles ; les personnes appartenant à l'organe d'administration, de gestion ou de surveillance ; les anciens travailleurs et les candidats à l'emploi (article 4).
- Elle protège également les personnes qui aident les lanceurs d'alerte, ainsi que les personnes physiques et morales liées aux lanceurs d'alerte (article 4.4).
- Les infractions au droit sont définies comme des actes ou des omissions qui sont soit illégaux, soit contraires à l'objet ou au but des règles (article 5.1).
- En accordant la protection, la directive ne prend en aucun cas en compte le motif du lanceur d'alerte.

[10] Étant donné que les petites entités du groupe peuvent facilement partager les ressources pour la réception des rapports et toute enquête à mener - par exemple, par l'intermédiaire du SAI au niveau du groupe - la charge administrative et financière potentielle de la mise en œuvre d'un SAI est faible et largement compensée par ses avantages pour les organisations et l'intérêt public.

[11] Le EU Whistleblowing Monitor permet de suivre l'évolution de la transposition de la directive européenne sur les lanceurs d'alerte dans les 27 États membres de l'UE, www.whistleblowingmonitor.eu/.

- Elle protège l'identité des lanceurs d'alerte dans la plupart des circonstances, avec des exceptions claires et limitées à la confidentialité, et une notification préalable au lanceur d'alerte lorsque son identité doit être divulguée (article 16).
- Elle accorde une protection aux lanceurs d'alerte qui ont signalé ou divulgué des informations de manière anonyme et qui ont ensuite été identifiés (article 6.3).
- Elle oblige un large éventail d'entités publiques et privées à mettre en place des systèmes d'alerte interne (article 8).
- Les entités publiques et privées et les autorités compétentes sont tenues de donner suite aux signalements reçus et de tenir le lanceur d'alerte informé dans un délai raisonnable (articles 9 et 11.2).
- La directive permet aux lanceurs d'alerte de signaler les violations de la loi en interne ou directement aux autorités compétentes (article 10).
- Elle autorise la divulgation publique dans certaines circonstances (article 15).
- Elle interdit "toute forme de représailles", y compris les menaces de représailles et les tentatives de représailles, et fournit une liste d'exemples longue, diverse et non exhaustive (article 19).
- Les États membres de l'UE sont tenus de veiller à ce que des conseils facilement accessibles et gratuits, complets et indépendants soient fournis au public (article 20.1(a)).
- La directive prévoit une assistance juridique et financière pour les lanceurs d'alerte, qui sont des éléments essentiels d'une protection efficace des lanceurs d'alerte (article 20, paragraphe 2).
- Elle crée une présomption de représailles lorsqu'un lanceur d'alerte subit un préjudice (article 21.5).
- Elle prévoit des mesures provisoires qui permettent au lanceur d'alerte de conserver son statut professionnel et financier jusqu'à la fin de la procédure judiciaire (article 21.6).
- La directive prévoit des sanctions à l'encontre des personnes qui entravent ou tentent d'entraver le signalement, qui exercent des représailles à l'encontre des lanceurs d'alerte (y compris en engageant une procédure vexatoire) ou qui ne respectent pas l'obligation de préserver la confidentialité de l'identité du lanceur d'alerte (article 23).
- Elle prévoit que les lanceurs d'alerte ne peuvent être tenus pour responsables de la violation de restrictions à l'acquisition ou à la divulgation d'informations, y compris de la violation de secrets commerciaux ou autres (article 21, paragraphes 2, 3 et 7). Elle exclut également la possibilité de renoncer au droit de dénoncer, par exemple par le biais de clauses de loyauté ou d'accords de confidentialité ou de non-divulgation (article 24).

REALISER L'AUTO-EVALUATION

La grille d'auto-évaluation doit être utilisée comme une étape cruciale dans la conception ou la révision du système d'alerte interne (SAI) d'une organisation. Son utilisation est essentielle pour plusieurs raisons :

- **Identifier les forces et les faiblesses** : La grille aide les organisations à évaluer l'efficacité de leurs SAI. En identifiant les forces et les faiblesses de leurs SAI, les organisations peuvent renforcer leurs bonnes pratiques et en combler les lacunes, afin d'en améliorer l'efficacité globale.
- **Garantir les meilleures pratiques** : Les conclusions de l'auto-évaluation permettent de s'assurer qu'une organisation adhère aux meilleures pratiques en matière de protection des lanceurs d'alerte. Cela est essentiel pour maintenir la confiance du personnel et des parties prenantes, et pour favoriser un environnement qui encourage les alertes éthiques.
- **Promouvoir une culture de la transparence et de la responsabilité** : Le processus encourage une culture dans laquelle le personnel se sent en sécurité pour signaler des actes répréhensibles sans crainte de représailles. Il démontre l'engagement d'une organisation en faveur de la transparence, de l'intégrité et d'un comportement éthique, ce qui favorise la confiance entre les membres du personnel.
- **Orienter les améliorations et les réformes** : Les enseignements tirés de l'auto-évaluation peuvent guider des réformes et des améliorations ciblées des procédures d'alerte. Il peut s'agir de mettre à jour les politiques, d'améliorer les stratégies de communication ou de renforcer les programmes de formation afin de mieux soutenir les lanceurs d'alerte potentiels.
- **Faciliter la communication et la collaboration internes** : L'implication de différents services, tels que les ressources humaines et la conformité, dans l'auto-évaluation favorise la communication et la collaboration internes. Cela permet de mieux comprendre le processus d'alerte et d'intégrer le retour d'information provenant de différents points de vue au sein de l'organisation.
- **Renforcer l'apprentissage organisationnel** : Une auto-évaluation régulière offre des possibilités d'apprentissage et de développement continus. Elle aide votre organisation à se tenir au courant des meilleures pratiques, à s'adapter aux nouvelles attentes et à répondre efficacement aux défis émergents en matière de protection des lanceurs d'alerte.
- **Instaurer la confiance avec les parties prenantes externes** : En démontrant son engagement à s'auto-évaluer et à s'améliorer, votre organisation renforce la confiance des parties prenantes externes, y compris les régulateurs, les partenaires et le public. Cette confiance est essentielle pour maintenir une réputation positive et assurer la durabilité à long terme.

Dans l'ensemble, l'utilisation de la grille d'auto-évaluation est une mesure proactive visant à renforcer l'efficacité du système d'alerte d'une organisation, à protéger les lanceurs d'alerte et à faire respecter les normes éthiques.

ROLES ET RESPONSABILITES DANS LA CONDUITE DE L'EVALUATION

L'agent ou le bureau chargé de l'alerte est responsable de la réalisation de l'auto-évaluation. Pour maximiser son efficacité, il doit collaborer avec d'autres services ou fonctions, tels que les ressources humaines (RH), la conformité, l'éthique, le service juridique, la responsabilité sociale des entreprises (RSE) et la diversité, l'équité et l'inclusion (DEI), ainsi qu'avec les organes concernés, y compris l'organe directeur et les représentants du personnel. Ces

GRILLE D'EVALUATION : DIMENSIONS ET QUESTIONS

Le cœur de l'évaluation est structuré autour d'un ensemble de 130 questions regroupées sous huit dimensions et divisées en 20 sous-catégories, comme décrit dans le tableau ci-dessous :

Dimensions	**Sous-catégories**
Principaux éléments à prendre en compte lors de la mise en place d'un SAI	*Genre, égalité et inclusion sociale dans les systèmes d'alerte interne*
Champ d'application	Quels types d'actes répréhensibles doivent être couverts par les systèmes d'alerte interne ? Qui devrait être en mesure d'effectuer des signalements par le biais de systèmes d'alerte interne ? Qui doit être protégé ?
Rôles et responsabilités	Leadership de haut niveau L'agent ou le bureau chargé de l'alerte Responsables hiérarchiques
Information et communication	Fourniture d'informations à toutes les parties prenantes concernées Informations à fournir Favoriser une culture de la parole et de l'écoute
Procédures	Multiples canaux d'alerte En cas d'externalisation vers des prestataires de services externes Donner suite aux alertes Archivage et protection des données
Soutien et protection des lanceurs d'alerte	Protection de l'identité des lanceurs d'alerte et des autres personnes protégées Protection contre les comportements préjudiciables et les ingérences Traiter les cas de conduite préjudiciable, d'ingérence et de violation de la confidentialité Soutenir les lanceurs d'alerte
Protection des personnes concernées	Protection des personnes concernées
Contrôle et révision continus	Collecte de données Révision et modifications Responsabilité à l'égard des parties prenantes

La structure de la grille reflète largement la structure des *meilleures pratiques SAI* de Transparency International *pour les organisations publiques et privées,* afin de faciliter la référence.

INSTRUCTIONS POUR REMPLIR LA GRILLE

On peut répondre à chaque question par "oui", "non" ou "partiellement". Certaines questions sont composées de plusieurs éléments, y compris des questions de suivi ou des questions détaillées, tandis que d'autres peuvent comporter des sous-questions. Les utilisateurs ne doivent répondre par "oui" ou "non" que si cette réponse s'applique à tous les éléments de la question. Si certains éléments de la question exigent un "oui" et d'autres un "non", la réponse doit être "partiellement".

Exemple de question à laquelle une réponse "partielle" pourrait être apportée

10. Outre les salariés, toute personne ayant une relation professionnelle avec votre organisation peut-elle signaler un acte répréhensible couvert par le SAI de l'organisation (ci-après "acte répréhensible pertinent") ? Il s'agit au moins des catégories de personnes suivantes, que leur relation avec votre organisation soit en cours ou qu'elle ait pris fin :
    - les travailleurs (à temps plein ou à temps partiel, à durée déterminée ou temporaire), y compris les fonctionnaires
    - les travailleurs indépendants
    - les actionnaires et les personnes appartenant à l'organe d'administration, de direction ou de surveillance
    - les bénévoles et les stagiaires rémunérés ou non
    - les personnes travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseurs
    - les personnes telles que les candidats à un emploi ou les soumissionnaires qui ont obtenu des informations au cours du processus de recrutement ou d'autres négociations précontractuelles.

Il convient de répondre "partiellement" à cette question si une ou plusieurs des catégories de personnes énumérées ne peuvent pas signaler des actes répréhensibles par l'intermédiaire du système d'alerte interne de votre organisation - par exemple, si les bénévoles ne peuvent pas signaler des actes répréhensibles par l'intermédiaire du système d'alerte interne.

Les utilisateurs doivent également répondre "partiellement" lorsqu'il n'existe qu'une pratique informelle et qu'elle n'est pas formellement établie par une politique, une procédure, un processus ou une ligne directrice officielle.

Pour les organisations qui ont déjà mis en œuvre un SAI depuis un certain temps, les utilisateurs sont invités à fonder leurs réponses sur les résultats réels et l'efficacité du système, le cas échéant, plutôt que sur l'existence ou non de mesures spécifiques.

En cas de réponse négative ou partielle à une question, les utilisateurs doivent en indiquer les raisons dans la section des commentaires. Cette section devrait également être utilisée pour proposer des moyens potentiels de combler les lacunes identifiées.

Sources de données

Pour compléter la grille, les utilisateurs devront se référer à plusieurs sources de données, notamment

- la politique de l'alerte de l'organisation
- les procédures de traitement des alertes
- les données sur les cas d'alerte et de représailles
- les registres des risques et les évaluations des risques de non-conformité

- les résultats des audits ou d'autres évaluations relatives à la gouvernance, à la conformité et à la culture organisationnelle
- d'autres politiques pertinentes, telles que celles relatives au harcèlement sexuel et aux brimades, aux griefs et à la protection des données, ainsi que le code de conduite de l'organisation
- les ordres du jour permanents des organes de direction et autres organes de surveillance, en vérifiant spécifiquement si le SAI ou les rapports connexes y figurent
- enquêtes sur le personnel
- les programmes de formation
- des données sur tous les actes répréhensibles, qu'ils aient été signalés par un lanceur d'alerte ou détectés par d'autres moyens (par exemple, un audit)
- des dépliants, des bulletins d'information internes et des sections pertinentes de l'intranet et du site web de l'organisation
- des modèles de contrats de travail et de contrats de fournisseurs.

ANALYSER LES REPONSES ET DEFINIR LES ACTIONS DE SUIVI

Après avoir répondu à toutes les questions et identifié les forces et les faiblesses du système d'alerte interne et les avoir documentées dans la section des commentaires, l'étape suivante consiste à élaborer des recommandations spécifiques en vue d'améliorer le système d'alerte interne. Il est conseillé de formuler des recommandations pour chaque lacune ou faiblesse identifiée avant de décider d'un ordre de priorité.

Lors de la formulation de recommandations visant à améliorer les domaines ayant reçu une réponse négative ou partielle, nous encourageons les utilisateurs à consulter les *principes de bonnes pratiques en matière de SAI* de Transparency International *pour les organisations publiques et privées*. Cette grille d'auto-évaluation a été conçue comme un outil complémentaire aux principes de bonnes pratiques des SAI et suit la même structure, ce qui permet aux utilisateurs de trouver plus facilement les principes et conseils pertinents lorsqu'ils cherchent à améliorer des aspects spécifiques de leurs SAI.

La grille d'auto-évaluation n'attribue pas de score ou de poids à des questions, sous-sections ou dimensions spécifiques. Par conséquent, les utilisateurs ne doivent pas supposer qu'une sous-section ou une dimension est "suffisamment forte" et ne nécessite pas d'amélioration supplémentaire simplement parce qu'ils ont répondu "oui" à la plupart des questions qu'elle contient.

Le responsable ou le bureau chargé des alertes devrait inviter les départements et organes concernés, tels que les RH, la conformité, l'éthique, le service juridique et le service de diversité, équité et inclusion (DEI), ainsi que l'organe directeur et les représentants du personnel, à contribuer à l'analyse des réponses, à l'élaboration de recommandations et aux discussions sur les prochaines étapes.

Les actions de suivi pourraient inclure la révision des politiques, procédures et processus pertinents, la mise à jour du contenu de la formation et des informations fournies au personnel, le lancement d'une campagne de sensibilisation interne et la modification des modèles de contrats d'emploi et de services externes.

PRINCIPAUX ELEMENTS A PRENDRE EN COMPTE LORS DE LA MISE EN PLACE D'UN SYSTEME D'ALERTE INTERNE

Questions		Y	N	P*
1	Votre organisation a-t-elle procédé à une évaluation complète des risques et des besoins afin d'éclairer la conception de son SAI ?			
2	Le SAI a-t-il été conçu après consultation des parties prenantes concernées, y compris le personnel, les comités d'entreprise, les syndicats ou d'autres représentants du personnel, et - le cas échéant - en accord avec eux ?			
3	Votre organisation a-t-elle veillé à la conformité de son système d'alerte interne avec les exigences légales nationales, dans le cadre de la législation sur la protection des lanceurs d'alerte et d'autres législations, telles que les lois sur la protection des données, le travail, la lutte contre le blanchiment d'argent et la corruption ?			
4	Le SAI fait-il partie du cadre de gouvernance de l'organisation et est-il lié aux programmes d'intégrité et de conformité ?			
5	Votre organisation a-t-elle pris des mesures pour rendre sa politique d'alerte juridiquement contraignante pour l'organisation et ses employés, en garantissant la protection des lanceurs d'alerte telle qu'elle est décrite dans la politique, en particulier lorsque cette protection dépasse les garanties prévues par le droit national ? ***Remarque :*** les exigences légales nationales applicables à un SAI ne respectent souvent pas les meilleures pratiques dans un ou plusieurs domaines, tels que le champ d'application matériel et personnel, le signalement anonyme, les mesures de protection et de soutien, et les			

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
	actions de réparation. Une organisation doit toujours fournir des informations claires sur le droit applicable, notamment sur les personnes protégées par la législation nationale relative à la protection des lanceurs d'alerte, sur les raisons de cette protection et sur les modalités de cette protection. Si le SAI de votre organisation va au-delà des exigences légales dans un ou plusieurs domaines, l'organisation doit souligner les différences entre le SAI et la loi, afin que les lanceurs d'alerte potentiels comprennent ce qui constitue leur protection légale et ce qui relève d'un engagement volontaire plus élevé de la part de l'organisation. En outre, votre organisation doit souligner que si elle peut offrir une protection complète contre les comportements préjudiciables à l'encontre du lanceur d'alerte sur le lieu de travail, sa capacité à protéger les lanceurs d'alerte en dehors du lieu de travail est limitée.			
6	Votre organisation sait-elle clairement comment elle distinguera les alertes internes des autres types de retours d'information et de plaintes, tels que les griefs ?			
7	Le SAI a-t-il été conçu après consultation des parties prenantes concernées, y compris le personnel, les comités d'entreprise, les syndicats ou d'autres représentants du personnel, et - le cas échéant - en accord avec eux ?			
8	Votre organisation a-t-elle tenu compte de l'accessibilité, de la sensibilité au genre et de l'inclusivité lors de la conception de son SAI ?			
9	Si votre organisation fait partie d'un groupe, d'un réseau ou d'un partenariat, avez-vous envisagé d'aligner votre SRI sur celui des autres organisations membres, en particulier sur celui du siège ou de l'entité équivalente, ainsi que sur la manière dont le SRI de votre organisation s'intègre à ces systèmes ? Cela s'applique, par exemple, aux entreprises au sein d'un groupe, aux OSC faisant partie d'un réseau formel ou aux membres d'une organisation partenaire.			
10	Si votre organisation est le siège ou l'entité équivalente d'un groupe, d'un réseau ou d'un partenariat, prend-elle des mesures pour aider les organisations membres à mettre en œuvre un SRI efficace et pour faciliter l'alignement de ces systèmes sur le SRI de votre organisation - par exemple, en fournissant des lignes directrices, une formation ou une plateforme ?			
Commentaires et recommandations :				

LE GENRE, L'ÉGALITÉ ET L'INCLUSION SOCIALE DANS UN SAI

Un SAI sensible aux questions de genre, d'égalité et d'inclusion sociale (GESI) vise à créer un environnement inclusif et accessible pour tous les lanceurs d'alerte potentiels, en promouvant une culture où chacun se sent en confiance pour signaler des actes répréhensibles sans crainte de représailles ou de discrimination. Pour élaborer et mettre en œuvre efficacement un SAI sensible au GESI, les organisations doivent tenir compte des éléments suivants

- **Politique d'alerte** : La politique d'alerte de votre organisation mentionne-t-elle explicitement les principes d'égalité des sexes et d'inclusion sociale ?
- **Champ d'application du SAI** : Le SAI couvre-t-il la violence, le harcèlement, la discrimination et les brimades fondés sur le sexe, ainsi que d'autres formes d'inconduite sur le lieu de travail qui affectent de manière disproportionnée les groupes marginalisés ?
- **Canaux de signalement** : Les différents canaux de signalement confidentiels et anonymes sont-ils accessibles à tous les lanceurs d'alerte potentiels et prennent-ils en considération des facteurs tels que les barrières linguistiques, le sexe, l'analphabétisme, les handicaps, la sensibilité culturelle, l'accès limité à la technologie et la nécessité pour les personnes de pouvoir soumettre des rapports pendant et en dehors des heures de travail normales ?
- **Accessibilité des informations** : Les informations sur le SAI sont-elles disponibles dans un langage clair, facilement accessible et inclusif, ainsi que dans plusieurs langues le cas échéant ? Votre organisation a-t-elle veillé à ce que les informations relatives à son système d'alerte interne soient diffusées de manière inclusive, en tenant compte des spécificités de genre et en les rendant accessibles aux personnes handicapées ?
- **Formation** : Votre organisation propose-t-elle une formation spécifique aux cadres, aux responsables des alertes et aux enquêteurs sur le traitement sensible et impartial des alertes impliquant des groupes marginalisés ?
- **Soutien** : Votre organisation propose-t-elle des services de soutien aux lanceurs d'alerte, tels que l'accès à un soutien psychologique, à des conseils confidentiels, à une assistance juridique et à des réseaux d'entraide entre lanceurs d'alerte, en mettant l'accent sur ceux qui peuvent être confrontés à des difficultés supplémentaires en raison de leur identité sociale, comme le sexe, la race, l'appartenance ethnique, l'âge, le statut socio-économique, l'orientation sexuelle ou le handicap ?
- **Des équipes d'alerte et d'enquête diversifiées** : Les critères de désignation des personnes chargées de traiter les signalements garantissent-ils l'inclusion et la prise en compte de la dimension de genre ?
- **Collecte et analyse des données** : Votre organisation recueille-t-elle et analyse-t-elle des données anonymes et désagrégées pour identifier et traiter les modèles de signalement et les obstacles, y compris les comportements préjudiciables, en tenant compte du sexe et d'autres facteurs qui influencent les expériences individuelles, tels que la race, l'appartenance ethnique ou le handicap ?
- **Examens** : Les examens impliquent-ils les parties prenantes concernées, y compris les représentants du personnel, le bureau ou le responsable DEI, l'organe directeur et les services concernés, tels que les ressources humaines, la conformité, l'éthique et le service juridique ?
- **Engagement des parties prenantes** : Votre organisation collabore-t-elle avec des organisations de la société civile et des experts GESI afin d'améliorer continuellement le SAI et de s'assurer qu'il reste pertinent et inclusif ?

Note : ces questions sont intégrées dans les sections correspondantes de la grille d'auto-évaluation.

CHAMP D'APPLICATION

Votre organisation définit-elle clairement qui peut signaler et ce qui peut être signalé - et traité - par le biais de son système d'alerte interne, ainsi que les personnes protégées ?

	Questions	Y	N	P*
	QUELS TYPES D'ACTES REPREHENSIBLES DOIVENT ETRE COUVERTS PAR LES SYSTEMES D'ALERTE INTERNE ? (CHAMP D'APPLICATION MATERIEL)			
11	Le SAI définit-il un acte répréhensible comme toute action ou omission illégale, abusive ou susceptible de causer un préjudice ? Son champ d'application couvre-t-il toute suspicion d'acte répréhensible relevant de cette définition et qui est, a été ou est susceptible d'être commis au sein, par ou pour l'organisation ? Il convient de noter que le champ d'application du SAI va potentiellement au-delà des exigences légales minimales.	[ ]	[ ]	[ ]
12	Si ce n'est pas le cas, le SAI couvre-t-il au moins les points suivants ? • infractions pénales • les manquements aux obligations légales (nationales et internationales) • les dangers pour la santé et la sécurité publiques et professionnelles • les dangers pour l'environnement • les violations des droits humains	[ ]	[ ]	[ ]

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
	• l'exploitation ou la maltraitance des enfants • la violence, le harcèlement, les brimades et la discrimination fondés sur le sexe • la corruption sous toutes ses formes, y compris les pots-de-vin, le blanchiment d'argent, la corruption sexuelle, la malversation, le détournement de fonds, l'abus de pouvoir, l'obstruction à la justice et l'enrichissement illicite • d'autres violations des normes ESG • les délits d'initiés, l'évasion fiscale ou les infractions à la règlementation en matière de concurrence et aux sanctions commerciales internationales • les conflits d'intérêts • les déclarations financières frauduleuses • un gaspillage ou une mauvaise gestion flagrants • un comportement préjudiciable à l'égard des lanceurs d'alerte et d'autres parties protégées • un comportement qui comporte un risque significatif pour votre organisation parce qu'il porte atteinte à ses intérêts, à sa réputation, à ses activités, à sa santé financière ou à sa gouvernance, ainsi que toute autre violation des codes de conduite ou d'éthique de votre organisation et des politiques pertinentes • la dissimulation d'actes répréhensibles et les tentatives de dissimulation de tels actes, y compris l'ingérence ou la tentative d'ingérence dans le signalement d'actes répréhensibles ?			
13	Le champ d'application du SAI couvre-t-il les actes répréhensibles présumés qui sont, ont été ou sont susceptibles d'être commis dans, par ou pour l'organisation ? Il s'agit des actes répréhensibles commis par le personnel, mais aussi par toute personne travaillant directement ou indirectement pour l'organisation, y compris le personnel actuel et ancien, les personnes appartenant à l'organe d'administration, de gestion ou de surveillance, les bénévoles, les contractants ou sous-traitants, et les fournisseurs ou consultants, dans le cadre de leur travail pour l'organisation ?			
Commentaires et recommandations :				

Questions		Y	N	P*
QUI DEVRAIT ETRE EN MESURE DE FAIRE UN RAPPORT PAR L'INTERMEDIAIRE DU SAI DE VOTRE ORGANISATION ? (CHAMP D'APPLICATION PERSONNEL)				
14	Outre les salariés, toute personne ayant une relation professionnelle avec l'organisation peut-elle signaler un acte répréhensible couvert par son SAI (ci-après "acte répréhensible pertinent") ?[12] Il s'agit au moins des catégories de personnes suivantes, que leur relation avec l'organisation soit en cours ou qu'elle ait pris fin : • les travailleurs (à temps plein ou à temps partiel, à durée déterminée ou temporaire), y compris les fonctionnaires • les travailleurs indépendants • les actionnaires et les personnes appartenant à l'organe d'administration, de direction ou de surveillance • les bénévoles et les stagiaires rémunérés ou non • les personnes travaillant sous la supervision et la direction de contractants, de sous-traitants et de fournisseurs • les personnes, telles que les candidats à l'emploi ou les soumissionnaires, qui ont obtenu des informations au cours du processus de recrutement ou d'autres négociations précontractuelles ?			
Commentaires et recommandations :				
QUI DOIT ETRE PROTEGE ?				
15	Le SAI définit-il les "lanceurs d'alerte" comme toute personne qui signale, tente de signaler, est censée être sur le point de signaler ou est censée avoir signalé des actes répréhensibles présumés en étant raisonnablement convaincue que l'information signalée était vraie au moment où elle l'a été ?			

[12] Certaines organisations ouvrent leur système d'alerte interne à toute personne susceptible d'obtenir des informations sur des actes répréhensibles, que ce soit dans le cadre de leurs activités professionnelles ou en dehors, comme les utilisateurs, les clients, les bénéficiaires ou les membres de la communauté locale. D'autres mettent en place des systèmes distincts pour recevoir et traiter les rapports émanant de "personnes extérieures".

Questions		Y	N	P*
16	Si une personne affirme que le déclarant - lanceur d'alerte présumé - savait que l'information était fausse au moment où il l'a déclarée, le SAI fait-il peser la charge de la preuve sur la personne qui fait cette affirmation ? Le SAI dispose-t-il d'une procédure pour traiter les rapports sciemment faux et pour avertir les déclarants que s'ils font un rapport sciemment faux, ils ne bénéficieront d'aucune protection et pourront faire l'objet de sanctions légales ?			
17	Le SAI évite-t-il d'utiliser des termes décrivant le motif de la personne qui fait le rapport, tels que "de bonne foi", "malveillant", "vexatoire" ou "abusif" ?			
18	Le SAI protège-t-il les lanceurs d'alerte, qu'ils aient fait un signalement interne ou externe aux autorités, ou qu'ils aient fait une divulgation publique conformément à la législation ?			
19	Le SAI protège-t-il les lanceurs d'alerte qui ont rapporté des informations sur des actes répréhensibles de manière anonyme - en interne, en externe ou par le biais d'une divulgation publique - et qui ont été identifiés par la suite ?			
20	Le SAI protège-t-il les lanceurs d'alerte, qu'ils aient utilisé les canaux internes désignés ou qu'ils se soient adressés à une autre autorité interne "naturelle", telle qu'un directeur, un responsable de la santé et de la sécurité, un responsable de la conformité, un responsable des ressources humaines, un responsable de l'intégrité, un responsable juridique ou de la protection de la vie privée, un directeur financier, un responsable de l'audit ou un membre de l'organe de direction ?			
21	Le SAI couvre-t-il les personnes qui ont l'obligation professionnelle de signaler les actes répréhensibles dans le cadre de leurs fonctions, comme les auditeurs internes ou les responsables de la santé et de la sécurité ?			
22	Votre organisation protège-t-elle les tiers qui risquent d'être victimes d'un comportement préjudiciable ? Il s'agit notamment des • personnes morales dont le lanceur d'alerte est propriétaire, pour lesquelles il travaille ou avec lesquelles il a d'autres liens • tiers liés au lanceur d'alerte, tels que les collègues et les parents • personnes physiques qui aident ou tentent d'aider un lanceur d'alerte, de manière confidentielle • personnes morales, y compris les organisations de la société civile (OSC) et les syndicats, qui aident ou tentent d'aider un lanceur d'alerte, de manière confidentielle • personnes citées dans le rapport comme témoins potentiels • personnes participant au suivi d'un rapport, y compris les témoins • personnes qui refusent de participer à des actes répréhensibles.			
Commentaires et recommandations :				

ROLES ET RESPONSABILITES

Votre organisation établit-elle et communique-t-elle clairement les rôles et responsabilités de toutes les personnes impliquées dans la mise en œuvre de son SAI ?

	Questions	Y	N	P*
LEADERSHIP DE HAUT NIVEAU				
23	Le système d'alerte interne a-t-il été approuvé par la direction générale de votre organisation et par son organe de contrôle le plus élevé (ci-après "l'organe directeur") ?			
24	Le SAI désigne-t-il l'organe directeur comme responsable de la supervision finale du système d'alerte ?			
25	La direction générale et l'organe directeur de votre organisation ont-ils veillé à ce que le SAI dispose de ressources suffisantes pour atteindre efficacement ses objectifs ?			
26	La direction générale et l'organe directeur de votre organisation sont-ils correctement formés ou, au minimum, informés de l'importance du SAI, de son fonctionnement et du rôle qu'ils ont à jouer pour le soutenir ?			
Commentaires et recommandations :				

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
L'AGENT OU LE BUREAU CHARGE DE L'ALERTE				
27	En fonction de sa taille, de son exposition aux risques et de ses besoins, votre organisation a-t-elle désigné une personne (le "responsable chargé de l'alerte") ou un service (le "bureau chargé de l'alerte") comme responsable du fonctionnement du SAI, y compris pour : • la conception, le suivi et la révision du SAI • fournir des informations sur le SAI à toute personne • recevoir, évaluer, suivre et fournir un retour d'information sur les rapports • l'évaluation et le suivi des risques de représailles à l'encontre des lanceurs d'alerte • recevoir, évaluer, suivre et fournir un retour d'information sur les plaintes pour représailles déposées par les lanceurs d'alerte • rendre compte régulièrement à la direction générale et à l'organe directeur de votre organisation de la mise en œuvre du SAI ?			
28	Le responsable des alertes ou le chef du bureau en charge du traitement des alertes a-t-il un accès direct et facile à l'organe directeur qui supervise le SAI ?			
29	Le responsable des alertes ou le chef du bureau en charge du traitement des alertes jouit-il d'une indépendance et d'une autorité suffisantes dans le cadre de la structure organisationnelle ou de gouvernance ?			
30	Le SAI prévoit-il des solutions pour les conflits d'intérêts potentiels de l'agent ou du service chargé du traitement des alertes ?			
31	Le responsable des alertes ou les membres du bureau en charge de leur traitement possèdent-ils les qualifications requises et reçoivent-ils une formation spécifique et régulière aux fins du fonctionnement du SAI, y compris pour garantir l'inclusion et la prise en compte des questions de genre dans sa mise en œuvre ?			
32	Les critères de désignation des personnes chargées de traiter les rapports garantissent-ils l'inclusion et la prise en compte de la dimension de genre ?			
Commentaires et recommandations :				

Questions		Y	N	P*
RESPONSABLES HIERARCHIQUES				
33	Le SAI protège-t-il les lanceurs d'alerte qui s'adressent à leurs supérieurs hiérarchiques ?			
34	Les supérieurs hiérarchiques sont-ils régulièrement formés - au moins une fois par an - à la réception et au traitement des rapports d'alerte, en abordant des questions telles que le champ d'application du SAI et le cadre juridique, la manière de reconnaître les rapports d'alerte, la manière de traiter les informations reçues - par exemple en orientant le lanceur d'alerte vers les canaux appropriés, en préservant la confidentialité - et la manière de traiter avec sensibilité et impartialité les situations impliquant des groupes marginalisés, la violence fondée sur le genre, le harcèlement ou la discrimination ?			
Commentaires et recommandations :				

INFORMATION ET COMMUNICATION

Votre organisation fournit-elle des informations sur son système d'alerte interne à toutes les parties prenantes concernées, afin de les sensibiliser ?

	Questions	Y	N	P*
	INFORMER LE PERSONNEL DE VOTRE ORGANISATION ET LES AUTRES PARTIES PRENANTES CONCERNEES			
35	Le système d'alerte interne est-il signalé en interne, par les canaux les plus couramment utilisés par le personnel, tels que les brochures, les affiches ou l'intranet de votre organisation, et dans des langues permettant l'accès à tous ?	☐	☐	☐
36	Votre organisation fournit-elle des informations sur le SAI sur son site web, dans une section dédiée, facilement accessible, et dans des langues permettant l'accès à tous, afin d'atteindre les parties prenantes concernées autres que le personnel ?	☐	☐	☐
37	Votre organisation propose-t-elle une formation de sensibilisation à l'ensemble du personnel, lors de l'intégration et à intervalles réguliers ?	☐	☐	☐
38	Votre organisation fait-elle régulièrement la promotion de son SAI en interne - par exemple, lors de réunions générales du personnel, dans des bulletins d'information internes ou par courrier électronique ?	☐	☐	☐
39	Les modèles de contrat de votre organisation - y compris pour l'emploi, la fourniture, le conseil et la prestation de services - exigent-ils que le signataire lise et reconnaisse le code de conduite et la politique d'alerte de l'organisation ?	☐	☐	☐
40	Votre organisation a-t-elle veillé à ce que les canaux de diffusion des informations sur ses SAI soient inclusifs, sensibles au genre et accessibles aux personnes handicapées ?	☐	☐	☐

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
41	Votre organisation offre-t-elle des moyens sûrs au personnel et aux autres parties prenantes couvertes par le SAI de recevoir des informations et des conseils complets sur son champ d'application et ses procédures, la protection contre les comportements préjudiciables, les voies de recours disponibles et les droits des personnes concernées (c'est-à-dire les personnes désignées dans le rapport d'un lanceur d'alerte comme responsables de l'acte répréhensible ou du comportement préjudiciable suspecté) ?			
Commentaires et recommandations :				

INFORMATIONS A FOURNIR

42	Votre organisation fournit-elle des informations sur : • les rôles et responsabilités liés au SAI, y compris les personnes qui en sont responsables • le champ d'application du SAI, y compris par rapport à d'autres systèmes internes de signalement ou de plainte, tels que les mécanismes de réclamation, avec des conseils sur le système de signalement ou de plainte le mieux adapté pour recevoir et traiter tel ou tel type de préoccupation • les conditions à remplir pour bénéficier de la protection du SAI, en précisant que : o les motivations d'une personne pour signaler des actes répréhensibles présumés ne sont pas pertinentes pour sa protection, tant qu'elle croit raisonnablement que l'information signalée était vraie au moment où elle l'a fait. o Les lanceurs d'alerte sont protégés, qu'une enquête ultérieure apporte ou non la preuve d'un acte répréhensible, y compris ceux qui ont communiqué des informations inexactes par erreur. • le droit applicable, y compris qui est protégé par la législation nationale sur la protection des lanceurs d'alerte et comment, en soulignant les différences potentielles entre la politique et les procédures de l'organisation en matière d'alerte et de protection des lanceurs d'alerte et le droit en vigueur, afin que les lanceurs d'alerte potentiels comprennent ce qui constitue leur protection légale et ce qui relève d'un engagement volontaire plus élevé de la part de l'organisation. • les coordonnées des canaux d'information et de signalement internes • les procédures applicables au signalement des actes répréhensibles, y compris pour : o les demandes d'éclaircissement ou de complément d'information			

Questions		Y	N	P*
	○ les accusés de réception ○ les retours d'information au lanceur d'alerte ○ la nature du suivi, y compris les principales étapes - telles que l'évaluation initiale, l'enquête, la clôture du dossier - et le calendrier correspondant • le régime de confidentialité et d'anonymat, y compris les exceptions légales et les limitations pratiques • le type de mesures de protection et de soutien que votre organisation offre aux lanceurs d'alerte, y compris les procédures et les voies de recours en cas de comportement préjudiciable • comment les données à caractère personnel seront traitées, combien de temps elles seront conservées et dans quel but • des canaux de conseil confidentiels et indépendants disponibles gratuitement en dehors de l'organisation, tels que ceux gérés par les autorités nationales, les syndicats ou les OSC • les procédures de notification externe aux autorités compétentes ?[13]			
43	Le SAI indique-t-il clairement qu'il est interdit au personnel d'adopter toute forme de comportement préjudiciable à l'égard d'un lanceur d'alerte ou d'un tiers protégé, et qu'un tel comportement fera l'objet d'une action disciplinaire ?			
44	Le SAI indique-t-il clairement que lorsqu'un rapport est reçu par des canaux internes autres que les canaux de signalement désignés, ou par un personnel autre que celui chargé de traiter les rapports, il est interdit à la personne qui reçoit le rapport de divulguer toute information susceptible d'identifier le lanceur d'alerte ou les personnes concernées, et qu'elle doit rapidement orienter le lanceur d'alerte vers le canal approprié, dans la mesure du possible ?			
45	Le SAI explique-t-il que la protection offerte par la confidentialité ou l'anonymat n'est pas absolue dans la pratique ? Par exemple, si votre organisation est très petite, si le lanceur d'alerte est le seul témoin ou s'il a fait part de ses préoccupations à des collègues avant de faire un rapport, il y a un risque que le rapport remonte jusqu'à lui.			
Commentaires et recommandations :				

[13] La directive européenne exige des SAI qu'ils fournissent des informations claires et facilement accessibles sur les procédures de notification externe aux autorités nationales compétentes et, le cas échéant, aux institutions, organes et organismes de l'UE.

	Questions	Y	N	P*
FAVORISER UNE CULTURE DE LA PAROLE ET DE L'ECOUTE				
46	Le SAI reflète-t-il et renforce-t-il les valeurs de votre organisation ?			
47	Votre organisation invite-t-elle ses parties prenantes à discuter ouvertement de situations éthiques difficiles ?			
48	Votre organisation assure-t-elle le suivi de sa culture "parler et écouter", par exemple par le biais d'enquêtes et d'autres mécanismes de retour d'information ? Les résultats des activités de suivi sont-ils utilisés pour améliorer en permanence les politiques et les pratiques ?			
49	Le leadership de votre organisation est-il perçu par les parties prenantes internes et externes comme étant éthique et favorable au SAI ? Cette perception peut être mesurée au moyen d'enquêtes sur l'engagement des parties prenantes et du retour d'information du personnel.			
50	Les dirigeants de votre organisation font-ils la promotion du SAI en tant qu'élément clé de la gouvernance et outil d'amélioration continue ? Cela implique une communication claire, cohérente et positive, par écrit et en personne, à la fois en interne avec le personnel et en externe avec les autres parties prenantes et le grand public.			
51	Tous les niveaux de direction et tous les superviseurs directs expriment-ils leur soutien au SAI - par exemple, en encourageant le personnel à suivre une formation sur le SAI ?			
52	Les supérieurs hiérarchiques sont-ils tenus responsables de la promotion et du maintien d'une culture d'intégrité et de conduite éthique, y compris de la promotion d'une culture de la prise de parole - par exemple, en incluant cet aspect dans leur évaluation des performances ?			
53	Votre organisation félicite-t-elle les lanceurs d'alerte qui se sont exprimés, notamment par une reconnaissance privée ou - avec le consentement du lanceur d'alerte - publique de la part de la direction générale ?			
54	Les personnes chargées de recevoir les rapports et de communiquer avec le lanceur d'alerte - comme le responsable du traitement des alertes, les supérieurs hiérarchiques ou un prestataire de services externe - sont-elles formées à l'écoute et à la création d'une sécurité psychologique ?			
Commentaires et recommandations :				

* Y = Oui ; N= Non ; P = Partiellement

PROCEDURES

Votre organisation a-t-elle mis en place des systèmes de réception et de suivi des alertes ?

	Questions	Y	N	P*
MULTIPLES CANAUX D'ALERTE				
55	Votre organisation dispose-t-elle de plusieurs canaux d'alerte, permettant des rapports écrits et oraux, en ligne, hors ligne et à distance, facilement accessibles au personnel et aux autres parties prenantes couvertes par le SAI de l'organisation, tels que le courrier électronique, les plateformes en ligne, le téléphone, le courrier postal, les réunions physiques et les "boîtes aux lettres" ?[14]	[ ]	[ ]	[ ]
56	Lors de la mise en place de ses canaux d'alerte, votre organisation a-t-elle pris en compte et traité des facteurs tels que les barrières linguistiques, le sexe, l'analphabétisme, les handicaps, l'accès limité à la technologie et la nécessité pour les personnes de pouvoir soumettre des rapports pendant et en dehors des heures de travail normales ?	[ ]	[ ]	[ ]
57	Les canaux d'alerte interne de votre organisation sont-ils gérés uniquement par des personnes désignées ou d'autres personnes appropriées ?[15]	[ ]	[ ]	[ ]
58	Votre organisation dispose-t-elle d'un canal d'alerte qui permet un signalement anonyme ?	[ ]	[ ]	[ ]

* Y = Oui ; N= Non ; P = Partiellement

[14] La directive européenne exige des organisations qu'elles mettent en place des canaux internes d'alerte qui permettent un signalement écrit ou oral, ou les deux. Le signalement oral doit être possible par téléphone ou par d'autres systèmes de messagerie vocale et, à la demande de l'auteur du signalement, par le biais d'une rencontre physique dans un délai raisonnable.
[15] La directive européenne exige que les canaux d'alerte interne soient mis en place et exploités de manière sécurisée afin de protéger la confidentialité de l'identité du lanceur d'alerte et de tout tiers mentionné dans le rapport, et d'empêcher l'accès à ces informations par du personnel non autorisé.

Questions		Y	N	P*
59	Votre organisation met-elle en place des canaux de communication sûrs entre le lanceur d'alerte - y compris ceux qui sont anonymes, le cas échéant - et la personne chargée de traiter leur rapport, qui permettent le transfert de documents justificatifs sous forme physique et numérique ?			
60	Votre organisation reconnaît-elle les supérieurs hiérarchiques comme des destinataires potentiels d'alerte interne ?			
Commentaires et recommandations :				
Si votre organisation externalise les canaux de notification à des prestataires de services externes				
61	Votre organisation reste-t-elle en charge du suivi du rapport, de la correction des actes répréhensibles identifiés et du retour d'information au lanceur d'alerte ?			
62	Votre organisation s'est-elle assurée que le prestataire de services externe respecte les exigences légales et les meilleures pratiques applicables à un SAI ? Les garanties d'indépendance et de confidentialité figurent-elles dans le contrat de service ?			
63	Le rôle, les tâches et les responsabilités du prestataire externe sont-ils clairement établis et communiqués au personnel et aux autres parties prenantes couvertes par le SAI de votre organisation ?			
Commentaires et recommandations :				

	Questions	Y	N	P*
	DONNER SUITE AUX ALERTES			
64	Le système d'alerte interne de votre organisation garantit-il un suivi approfondi et opportun des rapports d'alerte, y compris des rapports anonymes lorsque cela est possible ?			
65	Le suivi implique-t-il une procédure définie pour la réception des rapports et leur évaluation initiale, l'enquête et la clôture - avec des critères clairs pour la prise de décision à la fin de chaque étape ?			
66	Le suivi du rapport s'effectue-t-il selon des règles de confidentialité strictes, sur la base du besoin de savoir ?			
67	Votre organisation dispose-t-elle d'un système de gestion des dossiers pour l'enregistrement, le suivi et la surveillance des alertes et des plaintes pour représailles ?			
68	Le fait que la personne responsable n'accuse pas réception d'un rapport, ne donne pas suite à un rapport ou ne fournit pas de retour d'information à un lanceur d'alerte déclenche-t-il une enquête, assortie, le cas échéant, d'une éventuelle action disciplinaire pour faute ou manquement aux devoirs de la charge ?			
69	Le SAI offre-t-il aux lanceurs d'alerte, aux tiers protégés et aux personnes concernées un système de recours contre les décisions concernant a) la clôture du dossier ou le renvoi à une autre procédure, b) la conduite ou le résultat de toute action de suivi ou d'enquête, c) la conduite ou le résultat de toute enquête sur une plainte pour représailles, ou d) toute décision de divulguer l'identité d'un lanceur d'alerte (sauf dans des cas exceptionnels) ?			
	Commentaires et recommandations :			
	Communication avec les lanceurs d'alerte, et leur participation			
70	La communication avec les lanceurs d'alerte a-t-elle lieu régulièrement tout au long du processus de suivi, ce qui leur permet de clarifier leur rapport, de fournir des preuves supplémentaires et de partager leurs préoccupations concernant les risques de comportement préjudiciable et la protection de l'identité ? Le lanceur d'alerte peut-il refuser toute communication ultérieure ?			

* Y = Oui ; N= Non ; P = Partiellement

	Questions	Y	N	P*
Accusé de réception				
71	Un accusé de réception d'un rapport est-il fourni aux lanceurs d'alerte dans un délai court et préétabli,[16] et comprend-il les éléments suivants : • la possibilité pour le lanceur d'alerte de clarifier son rapport et de fournir des informations ou des preuves supplémentaires • le délai de prise de contact • les responsabilités du lanceur d'alerte, telles que le respect de la confidentialité et le fait de ne pas enquêter lui-même sur les actes répréhensibles présumés • les mesures de conseil et de soutien disponibles et la procédure de signalement d'un comportement préjudiciable • le contenu et les politiques pertinents du SAI ?			
Retour d'information aux lanceurs d'alerte				
72	Un retour d'information est-il fourni au lanceur d'alerte régulièrement, au moins aux moments suivants : • à l'issue de l'évaluation initiale du rapport, et au plus tard dans les trois mois suivant la réception du rapport - selon la première éventualité • aux principales étapes du processus de suivi et au moins tous les trois mois • à la fin du processus de suivi ?			
73	Le retour d'information régulier au lanceur d'alerte comprend-il des informations sur : • la question de savoir si le rapport fera l'objet d'un suivi supplémentaire et, si ce n'est pas le cas, une explication - par exemple, la mention que le rapport sort du cadre du SAI ou qu'il n'y a pas suffisamment de preuves • le calendrier prévu pour le suivi du rapport • les actions envisagées ou entreprises pour donner suite au rapport, ainsi que leurs motifs • les mesures prises pour protéger l'identité ou l'anonymat du lanceur d'alerte ; le soutien disponible et, le cas échéant, les mesures prises pour protéger le lanceur d'alerte contre tout comportement préjudiciable • à quel moment le lanceur d'alerte peut s'attendre à recevoir un retour d'information sur les suites données à son signalement ?			

[16] La directive européenne sur la protection des lanceurs d'alerte fixe le délai à sept jours.

Questions		Y	N	P*
74	Les lanceurs d'alerte sont-ils informés des conclusions et des résultats du suivi de leur rapport, y compris des informations sur : • les allégations qui ont fait l'objet d'une enquête et toute limitation importante de l'enquête • les conclusions tirées pour chaque allégation • un aperçu des mesures correctives • le cas échéant, une explication de toute limitation des informations pouvant être fournies ?			
75	Les lanceurs d'alerte ont-ils la possibilité d'examiner et de commenter ces résultats, et leurs commentaires sont-ils inclus dans le rapport de suivi ?			
Commentaires et recommandations :				
Évaluation initiale des rapports d'alerte				
76	Tous les rapports reçus sont-ils enregistrés, reconnus et évalués avec diligence, y compris avec la possibilité pour la personne chargée du suivi du rapport de demander des informations complémentaires au lanceur d'alerte ?			
77	Dès la réception du rapport, la personne qui le traite procède-t-elle à une première évaluation du risque de comportement préjudiciable à l'encontre du lanceur d'alerte ? [17]			
78	Dès la réception du rapport, la personne qui le traite évalue-t-elle les risques de préjudice pour les autres parties, pour votre organisation elle-même et pour l'intérêt public, et répète-t-elle cette évaluation régulièrement tout au long du processus de suivi ?			
79	Votre organisation peut-elle prendre des mesures de soutien et de protection pour éviter tout comportement préjudiciable et tout dommage au lanceur d'alerte, à d'autres parties, à l'organisation elle-même et à l'intérêt public, sur recommandation du responsable chargé du traitement de l'alerte ?			
80	Lorsqu'un rapport est considéré comme dépassant le cadre du SAI, le lanceur d'alerte est-il orienté vers un autre système interne de signalement ou de plainte, ou éventuellement vers un système extérieur à votre organisation, s'il en existe un ?			

[17] Les orientations statutaires irlandaises pour les organismes publics et les personnes prescrites fournissent de bons conseils sur la manière d'évaluer et de contrôler les risques d'actions préjudiciables à l'encontre des lanceurs d'alerte et des tiers protégés. Voir : Department of Public Expenditure, NDP Delivery and Reform, Protected Disclosures Act - Statutory guidance for public bodies and prescribed persons, novembre 2023, pp.68-69, https://www.gov.ie/pdf/?file=https://assets.gov.ie/277081/c8a506a6-1e4c-41de-bc7f-6cba598f7638.pdf#page=null.

	Questions	Y	N	P*
	Commentaires et recommandations :			
	Enquête sur les actes répréhensibles signalés			
81	Votre organisation dispose-t-elle de protocoles d'enquête qui garantissent une procédure régulière, y compris : • le respect de la présomption d'innocence des personnes concernées et de leurs droits à répondre et à recevoir une assistance au cours du processus de suivi • des mesures visant à garantir que la personne chargée du suivi du signalement peut mener ou superviser l'enquête avec une indépendance suffisante par rapport au lanceur d'alerte, aux personnes concernées et aux autres parties intéressées ?			
82	Pour chaque enquête, des termes de référence clairs sont-ils élaborés, lesquels définissent la portée, les méthodes, les compétences et les ressources nécessaires ?			
83	Les enquêtes respectent-elles, lorsque cela est approprié, les principes "axés sur la victime/survivante" *("victim/survivor-focused" principles*), comme dans les cas de harcèlement moral, de harcèlement sexuel, de corruption sexuelle ou d'exploitation sexuelle, et sont-elles menées de manière à éviter la retraumatisation et à donner la priorité au bien-être, aux besoins et aux souhaits des victimes ?			
84	Les risques de comportement préjudiciable à l'encontre du lanceur d'alerte et d'autres parties protégées sont-ils surveillés tout au long du processus de suivi ?			
85	Les conclusions préliminaires de l'enquête sont-elles présentées au lanceur d'alerte pour examen et commentaires éventuels, et ces commentaires sont-ils inclus dans le rapport d'enquête ?			
	Commentaires et recommandations :			
	Clôture du suivi			
86	Les SAI précisent-ils que si une enquête révèle qu'un acte répréhensible se produit, s'est produit ou est susceptible de se produire, votre organisation doit prendre les mesures nécessaires pour y remédier, y compris, le cas échéant, des mesures visant à : • faire cesser ou prévenir l'acte répréhensible et en minimiser les effets			

	Questions	Y	N	P*
	• sanctionner les auteurs de l'acte répréhensible, lorsqu'ils sont identifiés • remédier à tout dommage causé • faire part de l'acte répréhensible aux autorités compétentes ?			
87	Le SAI précise-t-il que votre organisation doit prendre les mesures appropriées pour corriger tout problème systémique identifié, tel que des faiblesses dans les politiques, les procédures ou les contrôles, que l'enquête ait ou non révélé des actes répréhensibles ?			
88	Le SAI permet-il de rouvrir des dossiers lorsque de nouvelles informations justifiant la poursuite de l'enquête sont communiquées, par exemple par le lanceur d'alerte ou un autre lanceur d'alerte ?			
89	Le responsable ou le bureau chargé du traitement de l'alerte continue-t-il à surveiller les risques de comportement préjudiciable à l'encontre du lanceur d'alerte après la clôture du suivi ?			
Commentaires et recommandations :				

	Questions	Y	N	P*
	ARCHIVAGE ET PROTECTION DES DONNEES			
90	Votre organisation documente-t-elle les rapports reçus, les mesures prises en guise de suivi, les conclusions et les résultats du suivi, ainsi que la communication avec le lanceur d'alerte et la personne concernée, d'une manière qui garantisse la confidentialité du rapport et, le cas échéant, l'anonymat du lanceur d'alerte ?			
91	Les rapports sont-ils conservés pendant une durée proportionnée et pas plus longtemps que nécessaire, notamment pour permettre un suivi diligent et pour protéger les lanceurs d'alerte contre les comportements préjudiciables, ainsi que les droits de la personne concernée ?			

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
92	Ces dossiers sont-ils conservés sous une forme accessible et vérifiable, conformément aux exigences de confidentialité et de protection des données ?			
93	Votre organisation a-t-elle veillé à ce que le SAI soit conforme aux normes de protection des données,[18] , y compris en : • identifiant clairement l'objectif du SAI • démontrant qu'elle a évalué et atténué les risques pour la vie privée aux stades de la conception et de la mise en œuvre du SAI, par exemple en procédant à une évaluation de l'impact sur la protection des données • appliquant le principe de minimisation des données pour le SAI et ne traiter que les informations personnelles adéquates, pertinentes et nécessaires au traitement d'un dossier • définissant des périodes de conservation proportionnées pour les informations à caractère personnel traitées dans le cadre du traitement d'une alerte, en fonction du résultat du suivi - par exemple, pour les alertes dont il s'avère qu'elles ne relèvent pas du champ d'application du SAI après une première évaluation, ou lorsqu'une enquête a été ouverte ? • la mise en place d'un accord de protection des données personnelles (APD) avec le prestataire de services, si votre organisation a externalisé une partie du traitement des cas d'alerte?			
Commentaires et recommandations :				

[18] Par exemple, le règlement général sur la protection des données (RGPD) de l'UE.

SOUTIEN ET PROTECTION DES LANCEURS D'ALERTE

Votre organisation a-t-elle réfléchi à la manière d'assurer la protection et le soutien de toutes les catégories de lanceurs d'alerte potentiels et de parties protégées ?

	Questions	Y	N	P*
PROTECTION DE L'IDENTITE DES LANCEURS D'ALERTE ET AUTRES PERSONNES PROTEGEES				
94	Le SAI indique-t-il clairement que, sans le consentement explicite du lanceur d'alerte, son identité et toute information permettant de l'identifier ne doivent pas être divulguées à d'autres personnes que celles qui sont compétentes pour recevoir les rapports ou en assurer le suivi ?	[ ]	[ ]	[ ]
95	Le SAI précise-t-il que lorsqu'il existe une obligation légale de divulguer des informations d'identification, le lanceur d'alerte doit en être informé au préalable avec un préavis suffisant et recevoir une explication écrite - par exemple, que le fait de ne pas divulguer ces informations compromettrait des enquêtes ou des procédures judiciaires connexes - ainsi que des mesures de protection supplémentaires, s'il y a lieu ?	[ ]	[ ]	[ ]
96	Toutes les personnes désignées pour fournir des informations et traiter les rapports des lanceurs d'alerte sont-elles tenues à un devoir de confidentialité, et votre organisation prévoit-elle des sanctions en cas de manquement à ce devoir ?	[ ]	[ ]	[ ]
97	Votre organisation prend-elle des mesures pour protéger le lanceur d'alerte et son identité au-delà de la clôture de l'affaire ?	[ ]	[ ]	[ ]

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
98	Le SAI indique-t-il clairement que les lanceurs d'alerte anonymes bénéficieront du même niveau de soutien et de protection internes si leur identité est révélée ?			
Commentaires et recommandations :				
PROTECTION CONTRE LES COMPORTEMENTS PREJUDICIABLES ET LES INGERENCES				
Interdiction des comportements préjudiciables et des ingérence				
99	Le SAI interdit-il clairement toute forme de comportement préjudiciable à l'égard des lanceurs d'alerte et des tiers protégés - y compris les menaces et les tentatives de comportement préjudiciable - et prévoit-il des sanctions pour ce type de comportement ?			
100	Le SAI définit-il les comportements préjudiciables de manière large, afin d'inclure toute menace, recommandation ou action réelle, directe ou indirecte, ou omission liée à ou résultant d'une alerte réelle ou présumée, qui cause ou peut causer un préjudice ? En ce qui concerne le personnel de votre organisation, la conduite préjudiciable inclut, mais n'est pas limitée à • la suspension, le licenciement ou des mesures équivalentes • la non-transformation d'un contrat de travail temporaire en contrat permanent[19] • la rupture anticipée ou le non-renouvellement d'un contrat de travail temporaire • le licenciement déguisé, lorsqu'une organisation rend les conditions de travail intolérables, ce qui pousse un individu à démissionner • rétrogradation ou refus de promotion • le transfert de fonctions, la réduction ou la limitation des tâches, la modification des heures de travail • une sélection déloyale pour des tâches ou la participation à des événements ; refus de formation • les restrictions ou la suppression des ressources disponibles, telles que les budgets ou les ressources humaines			

[19] C'est le cas lorsque le travailleur s'attendait légitimement à ce qu'on lui propose un emploi permanent.

Questions		Y	N	P*
	• la réduction de la rémunération ou la retenue du paiement • une évaluation négative des performances ou des références d'emploi • l'inspection ou l'enquête injustifiée des fonctions, ou la divulgation des résultats de ces inspections • l'imposition ou l'administration d'une mesure disciplinaire, d'un blâme ou d'une autre sanction • la coercition, l'intimidation, le harcèlement ou l'ostracisme • la discrimination ou le traitement désavantageux ou injuste • les préjudices physiques ou psychologiques ou la violence • les atteinte à la réputation de la personne - par exemple, la salir, la discréditer ou l'humilier en mettant en doute sa santé mentale, sa compétence professionnelle, sa fiabilité ou son honnêteté • la perte financière • la divulgation de l'identité du lanceur d'alerte • des poursuites ou des actions en justice. En ce qui concerne les lanceurs d'alerte et les tiers protégés qui ne font pas partie du personnel, la conduite préjudiciable comprend, sans s'y limiter, les éléments suivants : • la réduction de la rémunération ou la retenue du paiement • une référence négative • un audit ou une évaluation injustifiés, ou la divulgation des résultats de ces audits • la coercition, l'intimidation, le harcèlement ou l'ostracisme • la discrimination ou le traitement désavantageux ou injuste • les préjudices physiques ou psychologiques ou la violence • les atteintes à la réputation de la personne - par exemple, salir, discréditer ou humilier une personne en mettant en doute sa santé mentale, sa compétence professionnelle, sa fiabilité ou son honnêteté • la perte financière • le boycott ou l'inscription sur une liste de blocage			

Questions		Y	N	P*
	• la résiliation anticipée ou l'annulation d'un contrat de biens ou de services • la divulgation de l'identité du lanceur d'alerte • des poursuites ou des actions en justice.			
101	Le SAI interdit-il clairement toute ingérence ou tentative d'ingérence dans l'alerte et prévoit-elle des sanctions pour ce type de comportement ?			
Commentaires et recommandations :				
Prévenir les comportements préjudiciables				
102	Votre organisation s'est-elle expressément engagée à ne pas conclure d'accords susceptibles de renoncer aux droits et protections d'un lanceur d'alerte ou d'y faire obstacle, y compris des accords d'arbitrage avant litige, des clauses de loyauté dans les contrats, ou des accords de confidentialité ou de non-divulgation ?			
103	Votre organisation a-t-elle inclus dans les accords les modèles de contrat et les politiques et procédures organisationnelles des clauses reconnaissant explicitement les droits et protections des lanceurs d'alerte prévus par son SAI et stipulant qu'en cas de conflit ou de perception de conflit avec la politique d'alerte, la politique d'alerte prévaut ?			
104	Votre organisation veille-t-elle à ce que le personnel et les autres parties prenantes soient informés que son code de conduite et ses SAI interdisent tout comportement préjudiciable à l'égard des lanceurs d'alerte et des autres personnes protégées, et qu'un tel comportement entraînera des sanctions ?			
105	Votre organisation met-elle en œuvre des stratégies visant à prévenir les comportements préjudiciables à l'égard des lanceurs d'alerte tout au long du processus de suivi et après la conclusion de l'affaire, telles que des évaluations systématiques et régulières des risques et des mesures préventives ?			
106	Votre organisation prend-elle des mesures pour éviter que le lanceur d'alerte ne subisse d'autres préjudices en attendant la résolution d'une plainte interne pour comportement préjudiciable - par exemple, en suspendant toute procédure disciplinaire à l'encontre du lanceur d'alerte ou en lui accordant un congé payé ?[20]			

[20] Une fois qu'il est établi que la personne qui se plaint d'un comportement préjudiciable a fait un rapport interne ou externe, ou une divulgation publique, et qu'elle a subi un préjudice.

Questions		Y	N	P*
107	Votre organisation considère-t-elle que le fait de ne pas prendre de mesures raisonnables pour prévenir un comportement préjudiciable constitue un manquement au devoir des personnes responsables ?			
Commentaires et recommandations :				
TRAITER LES CAS DE CONDUITE PREJUDICIABLE, D'INGERENCE ET DE VIOLATION DE LA CONFIDENTIALITE				
108	Le SAI prévoit-il des mécanismes exécutoires, transparents et opportuns pour recevoir et suivre les plaintes concernant : • tout comportement préjudiciable à l'égard des lanceurs d'alerte et des tiers protégés • l'ingérence ou les tentatives d'ingérence dans les alertes • les violations de la confidentialité de l'identité du lanceur d'alerte ?			
109	Une fois qu'il est établi qu'une personne se plaignant d'un comportement préjudiciable est un lanceur d'alerte ou une autre personne protégée, et qu'elle a subi un préjudice, le SAI exige-t-il de la personne accusée du comportement préjudiciable qu'elle démontre de manière claire et convaincante que ce comportement n'est en aucune façon lié à un lanceur d'alerte réel ou présumé ?			
110	Lorsqu'une personne qui se plaint d'un comportement préjudiciable est un lanceur d'alerte ou une autre personne protégée, votre organisation lui fournit-elle des mesures de soutien, telles qu'un soutien juridique et psychologique, un congé payé ou une formation de reconversion ?			
111	Si l'existence d'un comportement préjudiciable est confirmée, le SAI indique-t-il que votre organisation doit prendre les mesures nécessaires pour mettre fin au comportement préjudiciable et protéger le bien-être physique, financier et psychologique de la personne concernée ?			
112	Si l'existence d'un comportement préjudiciable est confirmée, le système d'alerte interne prévoit-il une gamme complète d'actions réparatrices pour remédier au préjudice causé à la personne concernée ? Ces mesures comprennent, par exemple • la réintégration de la personne dans le poste qu'elle occupait avant le comportement préjudiciable ou dans un poste similaire à salaire, statut, fonctions et conditions de travail égaux • le renvoi de la personne responsable de la conduite préjudiciable, lors de la réintégration du lanceur d'alerte ou d'une autre partie protégée qui lui a fait courir le risque de nouvelles représailles • l'accès équitable à toute promotion et formation qui aurait pu être refusée			

Questions		Y	N	P*
	• le rétablissement des fonctions, si possible • la reconnaissance du temps perdu et l'impact sur les performances • le retrait d'un litige contre un lanceur d'alerte • la suppression de tout enregistrement susceptible de constituer un dossier en vue de l'établissement d'une liste noire ou de représailles ultérieures • relancer une procédure de passation de marchés • le rétablissement d'un contrat annulé • presenter des excuses pour les échecs • des félicitations pour avoir défendu la mission, les valeurs ou les intérêts de votre organisation en dénonçant des actes répréhensibles, par le biais d'une reconnaissance privée ou, avec le consentement du lanceur d'alerte, publique de la part de la direction générale - par exemple, un prix interne "Speak Up" • une compensation financière pour les pertes de revenus passées, présentes et futures • une compensation financière pour la douleur et la souffrance, y compris les frais médicaux.			
Commentaires et recommandations :				
Faire en sorte que les auteurs de comportements préjudiciables, d'interférences et de violations de la confidentialité rendent des comptes				
113	Votre organisation prévoit-elle des sanctions efficaces, proportionnées et dissuasives, à la suite de procédures disciplinaires, pour : • les comportements préjudiciables à l'égard des lanceurs d'alerte et des tiers protégés • l'ingérence ou les tentatives d'ingérence dans les alertes de mauvaises pratiques • la violation de la confidentialité de l'identité du lanceur d'alerte ?			

Questions		Y	N	P*
114	Votre organisation a-t-elle mis en place des procédures et des sanctions appropriées pour sanctionner les comportements préjudiciables de personnes autres que les salariés, qui ne sont pas soumises à des procédures disciplinaires, telles que les consultants, les fournisseurs, les personnes appartenant à l'organe d'administration, de gestion ou de surveillance, et les bénévoles ? Les sanctions peuvent inclure, par exemple, la révocation d'un poste et la résiliation ou la non-exécution d'un contrat. • De telles situations sont-elles prévues dans les accords contractuels de votre organisation avec des parties externes ?				
Commentaires et recommandations :				
SOUTENIR LES LANCEURS D'ALERTE				
115	Lorsqu'un lanceur d'alerte ou une autre personne protégée se plaint d'un comportement préjudiciable, votre organisation peut-elle prendre des mesures internes pour prévenir ou atténuer le préjudice, par exemple en proposant un autre supérieur hiérarchique ou un autre espace de travail, un congé payé ou une formation de reconversion ?			
116	Votre organisation propose-t-elle des services de soutien aux lanceurs d'alerte, tels que l'accès à un soutien psychologique, des conseils confidentiels, une assistance juridique et des réseaux de soutien par les pairs pour les lanceurs d'alerte, en mettant l'accent sur ceux qui peuvent être confrontés à des difficultés supplémentaires en raison de leur identité sociale - comme le sexe, la race, l'appartenance ethnique, l'âge, le statut socio-économique, l'orientation sexuelle ou le handicap ?			
Commentaires et recommandations :				

PROTECTION DES PERSONNES CONCERNEES

Votre organisation prévoit-elle des mesures de protection pour la personne concernée ?

Questions		Y	N	P*
117	Le SAI protège-t-il l'identité des personnes concernées ?			
118	Votre organisation protège-t-elle les droits des personnes concernées, y compris la présomption d'innocence, le droit de réponse et le droit de recevoir une assistance pendant le suivi d'un rapport d'alerte ou d'une plainte émanant d'un lanceur d'alerte ou d'un tiers protégé ?			
119	Le SAI dispose-t-il d'une procédure permettant de traiter les rapports sciemment faux et d'avertir les personnes déclarantes que si elles font un tel rapport, elles risquent de ne pas bénéficier de la protection du SAI et de se voir infliger des sanctions légales ?			
Commentaires et recommandations :				

* Y = Oui ; N= Non ; P = Partiellement

ASSURER LE SUIVI, L'EXAMEN ET LA RESPONSABILITE EN CONTINU

Votre organisation assure-t-elle un suivi continu et procède-t-elle régulièrement à l'examen et à la révision de son SAI ?

	Questions	Y	N	P*
	COLLECTE DES DONNEES			
120	Votre organisation a-t-elle développé des indicateurs pour contrôler la mise en œuvre et évaluer l'efficacité et l'adéquation du SAI, y compris : • le nombre total de signalements reçus ; le nombre de signalements considérés comme ne relevant pas du champ d'application du SAI et les raisons générales qui les ont motivés ; le nombre de signalements anonymes ; les mesures prises en réponse aux signalements et leurs résultats - y compris l'estimation des dommages financiers, des indemnisations, des recouvrements et des sanctions, le renvoi aux autorités, les procédures pénales, le temps nécessaire pour donner suite aux signalements et les types d'actes répréhensibles signalés • le nombre de plaintes pour comportement préjudiciable, les mesures prises pour y donner suite et leurs résultats, le temps nécessaire pour parvenir à une solution et les types de mesures de protection prises	[ ]	[ ]	[ ]

* Y = Oui ; N= Non ; P = Partiellement

Questions		Y	N	P*
	• le retour d'information des lanceurs d'alerte sur leur expérience du SAI, y compris les recommandations visant à améliorer le système • la connaissance et la confiance dans le SAI par le personnel et les autres parties prenantes qu'il couvre - établies, par exemple, par des enquêtes ?			
121	Votre organisation dispose-t-elle d'un système de collecte des données susmentionnées, ventilées sous une forme anonyme par sexe et - si possible - par race, ethnie et handicap ?			
Commentaires et recommandations :				
EXAMINATION ET MODIFICATIONS				
122	Votre organisation examine-t-elle la mise en œuvre, l'utilisation, l'efficacité et l'adéquation du SAI, au moins une fois par an ou plus souvent si nécessaire, sur la base des indicateurs et des données susmentionnés ?			
123	Votre organisation procède-t-elle à un examen complet et formel au moins tous les trois ans, ou plus souvent si nécessaire, de la mise en œuvre, de l'utilisation, de l'efficacité et de l'adéquation du SAI, sur la base des indicateurs et des données susmentionnés ?			
124	Les examens du SAI répondent-ils généralement aux questions suivantes ? • Un an après l'entrée en vigueur du SAI, votre organisation a-t-elle alloué des ressources humaines et financières pour permettre son fonctionnement efficace ? • Votre organisation a-t-elle créé un département spécifique pour sa politique d'éthique ou de conformité et son système d'alerte interne ? Si ce n'est pas le cas, à quel service a-t-elle rattaché le responsable ou le bureau chargé des alertes ? • Quel est le délai moyen pour fournir un retour d'information à un lanceur d'alerte ? • Votre organisation a-t-elle planifié et réalisé des révisions, internes ou externes, du SAI ? Avec quelle régularité ? Avec quels résultats ? • L'organe directeur procède-t-il à l'examen du système ? • Le SAI a-t-il été examiné par une autorité compétente, telle qu'une agence de lutte contre la corruption ou une autorité de signalement ? Dans l'affirmative, quels ont été les résultats ?			

Questions		Y	N	P*

	• Au cours de l'année écoulée, votre organisation a-t-elle
	  ○ organisé une formation ou d'autres activités de sensibilisation au SAI à l'intention de tous les lanceurs d'alerte potentiels ?
	  ○ mené une enquête pour mesurer la sensibilisation et la confiance du personnel dans le SAI ? Quels ont été les résultats ?
	  ○ reçu des rapports ? Si oui, combien ?
	  ○ reçu des plaintes pour comportement préjudiciable ? Si oui, combien ?
	  ○ donné suite à des rapports ? Si oui, combien ?
	  ○ pris des mesures disciplinaires ou engagé des poursuites à la suite d'une alerte ou d'une plainte pour comportement préjudiciable ? Si oui, combien ?
	• Votre organisation dispose-t-elle d'une procédure de suivi systématique pour s'assurer que les lanceurs d'alerte ne subissent pas de représailles au fil du temps - par exemple, après trois mois, six mois, un an et deux ans ?
	• Le responsable ou le bureau chargé des alertes produit-il un rapport annuel contenant des données anonymes ? Avec qui sont-elles partagées et comment sont-elles utilisées ?
	• Le SAI est-il inclusif et sensible au genre ? Votre organisation recueille-t-elle et analyse-t-elle des données anonymes et désagrégées afin d'identifier et de traiter les modèles de signalement et les obstacles - y compris les comportements préjudiciables - en tenant compte du sexe et d'autres facteurs qui influencent les expériences individuelles, tels que la race, l'appartenance ethnique ou le handicap ?
	• Votre organisation dispose-t-elle d'un mécanisme permettant de réviser le système d'alerte interne à la suite des audits et des rapports annuels ? Quel est le calendrier ?			

125	Le SAI fait-il l'objet d'examens indépendants périodiques - par exemple, par des OSC, une société mère, une autorité publique ou des conseillers professionnels ?	☐	☐	☐
126	Les examens impliquent-ils les parties prenantes internes concernées, y compris le personnel, les représentants du personnel, le bureau ou le responsable DEI, l'organe directeur et les départements et organes concernés, tels que les RH, la conformité, l'éthique et le service juridique ? Les examens impliquent-ils également les parties prenantes externes, le cas échéant, telles que les filiales, les fournisseurs ou les OSC ?	☐	☐	☐
127	Votre organisation révise-t-elle son SAI en fonction des résultats de l'examen, afin d'en améliorer l'efficacité et de garantir que les systèmes sont à jour et conformes à la législation et aux meilleures pratiques ?	☐	☐	☐
Commentaires et recommandations :				

Questions		Y	N	P*
RESPONSABILITE A L'EGARD DES PARTIES PRENANTES				
128	Les données ci-dessus et les résultats de l'examen sont-ils communiqués chaque année à l'organe directeur de votre organisation, à son personnel et aux autres parties prenantes concernées, y compris les actionnaires ?			
129	Ces rapports annuels sont-ils publiés sur le site web de votre organisation - par exemple, dans la section consacrée au SAI - et inclus dans des rapports pertinents tels que son rapport de responsabilité ou de gouvernance ?			
130	Les données susmentionnées et les résultats de l'examen sont-ils partagés d'une manière qui ne révèle aucune information permettant d'identifier le lanceur d'alerte et les autres parties impliquées, y compris les personnes concernées, les tiers protégés et les témoins ?			
Commentaires et recommandations :				

PRINCIPES CLES POUR LES SYSTEMES D'ALERTE INTERNE

Toutes les organisations publiques et la plupart des organisations privées devraient disposer d'un système d'alerte interne, en suivant ces principes clés :

CHAMP D'APPLICATION

1. Les systems d'alerte interne doivent inviter à signaler toute suspicion d'acte répréhensible - c'est-à-dire tout acte ou omission illégal, abusif ou susceptible de causer un préjudice - commis au sein de l'organisation, par elle ou pour son compte.

2. Les SAI doivent inviter toute personne susceptible d'obtenir, dans le cadre de ses activités professionnelles, des informations sur des actes répréhensibles commis par ou pour l'organisation ou au sein de celle-ci, à présenter un rapport.

3. Les organisations doivent protéger les lanceurs d'alerte - c'est-à-dire toute personne qui signale des actes répréhensibles présumés en étant raisonnablement convaincue que l'information communiquée était vraie au moment où elle l'a fait - ainsi que les tiers qui risquent d'être victimes d'un comportement préjudiciable.

ROLES ET RESPONSABILITES

4. Les dirigeants de l'organisation sont responsables de la mise en œuvre effective de son système d'alerte interne. Ils doivent démontrer leur engagement et donner un "ton d'en haut" clair en faveur de la prise de parole et de l'écoute en cas d'actes répréhensibles.

5. Les organisations devraient désigner une personne ou un service impartial responsable du fonctionnement du système d'alerte interne. Cette personne ou ce service devrait être exempt de tout conflit d'intérêts et disposer d'une indépendance, de pouvoirs et de ressources suffisants, ainsi que des qualifications requises.

INFORMATION ET COMMUNICATION

6. Les informations relatives au système d'alerte interne de l'organisation doivent être très visibles et accessibles, par le biais d'un large éventail de médias et de canaux. Toutes les parties prenantes concernées, y compris les lanceurs d'alerte potentiels et les personnes concernées, devraient avoir accès au système d'alerte interne et recevoir des informations pertinentes à ce sujet.

7. Les organisations devraient rendre compte publiquement chaque année de leur engagement en faveur d'une culture de l'écoute et de la parole, et de la mise en œuvre de leur système d'alerte interne.

PROCEDURES

8. Les systèmes d'alerte interne devraient comporter plusieurs canaux de signalement sûrs et facilement accessibles, et permettre les signalements par écrit et oralement. Les organisations devraient reconnaître les supérieurs hiérarchiques comme des destinataires potentiels des rapports d'alerte.

9. Les systèmes d'alerte interne devraient assurer un suivi diligent - c'est-à-dire approfondi, opportun, équitable et impartial - de tous les rapports reçus,[21] afin d'établir si des actes répréhensibles ont été commis,[22] pour traiter les actes répréhensibles confirmés et pour corriger tout problème systémique identifié.

10. En tant que parties prenantes bien informées et intéressées, les lanceurs d'alerte doivent être tenus informés tout au long du processus et avoir la possibilité d'apporter leur contribution au suivi de leur rapport.

11. Les rapports reçus, les actions de suivi, les conclusions et les résultats du suivi, ainsi que la communication avec le lanceur d'alerte et la personne concernée doivent être documentés de manière adéquate et conservés sous une forme accessible et vérifiable, conformément aux exigences en matière de confidentialité et de protection des données.

SOUTIEN ET PROTECTION DES LANCEURS D'ALERTE

12. Sans le consentement explicite du lanceur d'alerte, son identité et toute information permettant de l'identifier - c'est-à-dire toute information permettant de déduire directement ou indirectement son identité - ne devraient pas être divulguées en dehors des personnes compétentes pour recevoir les rapports ou en assurer le suivi.

13. Les organisations devraient accepter les rapports anonymes et y donner suite, et protéger les lanceurs d'alerte anonymes.

14. Les organisations devraient interdire toute forme de comportement préjudiciable - c'est-à-dire toute menace, recommandation ou action ou omission réelle, directe ou indirecte, qui cause ou peut causer un préjudice - lié aux alertes, ainsi que toute interférence avec les alertes.

15. Les organisations devraient prendre des mesures raisonnables pour prévenir les comportements préjudiciables et pour s'assurer que les personnes et les entités sous leur contrôle ou travaillant pour elles s'abstiennent de tout comportement préjudiciable.

16. Les systèmes internes d'alerte devraient prévoir des mécanismes applicables, transparents et opportuns pour (1) recevoir et suivre les plaintes pour conduite préjudiciable, ingérence et violation de la confidentialité, (2) sanctionner les auteurs et (3) garantir une réparation complète aux lanceurs d'alerte concernés et aux autres personnes protégées, par le biais de mesures correctives et d'une indemnisation.

[21] Cela inclut les rapports anonymes.

[22] Il s'agit également de savoir si un acte répréhensible a été commis ou est susceptible de l'être.

17. Les organisations doivent apporter un soutien aux lanceurs d’alerte afin d'éviter toute atteinte à leur santé ou à leur carrière.

PROTECTION DE LA PERSONNE CONCERNEE

18. Les organisations doivent protéger l'identité et les droits de la personne concernée, notamment en prévoyant des sanctions efficaces, proportionnées et dissuasives pour les personnes qui communiquent sciemment de fausses informations.

CONTROLE ET REVISION CONTINUS

19. Les systèmes d’alerte interne doivent faire l'objet d'un examen formel au moins une fois par an, et des révisions doivent être apportées en conséquence pour améliorer l'efficacité et garantir que les systèmes sont à jour et conformes à la législation et aux meilleures pratiques.

Transparency International France
14 Passage Dubail

75020 Paris

www.transparency-france.org