Les fondamentaux de la maîtrise des risques en contexte de crise

Le contexte de crise sanitaire que les administrations de l'État ont connu en 2020 a été riche en questionnements et enseignements en lien avec le contrôle interne (CI) :

- ❑ comment adapter le dispositif de CI pré-existant en contexte contraint ?
- ❑ sur quelles priorités concentrer les efforts ?
- ❑ quels outils peuvent être mobilisés pour assurer la continuité de service ?
- ❑ comment garantir le maintien des exigences minimales en matière de maîtrise des risques lorsque prévalent les procédures dérogatoires ?
- ❑ sur le plus long terme, quel rôle le dispositif de CI peut-il jouer pour contribuer à l'amélioration de la résilience des organisations face aux crises ?
- ❑ etc.

La présente fiche a vocation à proposer quelques axes de réflexion et bonnes pratiques en matière de maîtrise des risques dans un contexte de crise. **Le contrôle interne peut, en effet, être un levier pour mieux anticiper, gérer et se remettre d'une crise.**

I/ La priorité donnée à la continuité de service

L'accomplissement par les administrations de l'ensemble de leurs missions sans interruption constitue un aspect fondamental de la continuité de l'État. Parmi ces missions, certaines sont indispensables à la vie de la Nation et ne peuvent être repoussées. En contexte contraint, le maintien de ces activités devient la priorité. Une réflexion sur la définition des missions « prioritaires » a été menée ou, à défaut, doit nécessairement être menée au sein des ministères.

La couverture des risques liés à la continuité de service peut être anticipée au moyen de différents outils, à déployer en amont.

Tout d'abord, l'organisation d'un dispositif de veille et d'alerte sur les facteurs de risques pouvant déclencher une interruption de service (pandémie comme dans le cas présent, mais également catastrophes naturelles ou d'origine humaine, dysfonctionnements informatiques d'ampleur, cyberattaque, évènements empêchant l'accès aux bâtiments, problèmes politiques ou économiques graves, défaillance du système bancaire, vols de matériels ou de données, actes de malveillance, terrorisme, *etc.)* est un moyen de mieux prévenir leurs impacts et d'avoir plus de marges de manœuvre pour adapter la stratégie de maîtrise en conséquence.

Il est bien sûr difficile d'envisager tous les évènements pouvant aboutir à une interruption de service. Si les facteurs de risques sont multiples et doivent faire l'objet du dispositif de veille précité pour les identifier le plus en amont possible, les risques de continuité qu'ils sont susceptibles d'engendrer peuvent être regroupés en quelques catégories majeures (indisponibilité des agents, matériel / réseau informatique hors service, locaux ou infrastructures inaccessibles, rupture de la chaîne de décision, difficulté d'approvisionnement, insuffisance de trésorerie, *etc.*).

En fonction de ces différents scénarios, une stratégie de continuité de service doit être formalisée dans un « plan de continuité de l'activité » (PCA). Le PCA identifie les activités essentielles de la structure, par ordre de priorité, ainsi que les ressources et procédures permettant de les maintenir en contexte contraint (canaux alternatifs pouvant être activés pour répondre aux demandes urgentes, critères objectifs de priorisation des dépenses, redéploiement des moyens affectés aux activités pouvant être momentanément suspendues, *etc.*). Le PCA est nécessairement un document élaboré de manière collégiale, et évolutif.

La priorité donnée à la continuité de service peut se traduire par un affaiblissement du contrôle interne, avec, par exemple, la mise en place de procédures dérogatoires ou l'allègement des circuits de visa pour aller plus vite et / ou éviter la constitution de stocks d'opérations en attente. Les pratiques de contournement du principe de séparation des tâches sont également plus probables. Elles peuvent parfois découler du développement du télétravail ou des difficultés d'interface entre certaines applications.

Plusieurs préconisations peuvent être formulées à cet égard :

- la mise en place d'une équipe dédiée à la gestion de crise (idéalement pré-identifiée avant le déclenchement de cette dernière), chargée d'organiser les nouvelles activités nées du contexte de crise (ex : achat urgent, versement de subventions), ainsi que d'autoriser les exceptions ou dérogations aux procédures classiques ;

Au sein de cet espace d'échanges et d'arbitrage, le référent CIF peut donner son avis sur la sécurisation, suffisante ou non, des procédures dérogatoires, sur leur proportionnalité au regard de leur nécessité. Son rôle est de veiller à ce que les fondamentaux en matière de CI soient bien présents.

- l'importance de communiquer aux agents des directives claires sur les cas (limitatifs et justifiés) dans lesquels les dérogations s'appliquent ;

En complément, il peut être utile de prévoir un dispositif de remontées des agents sur la mise en œuvre de ces directives, pour prendre en compte le retour des services (éventuelles difficultés rencontrées, questions subsidiaires non tranchées, *etc.*) et ainsi rester en capacité d'adapter le dispositif en tant que de besoin (conformément à la logique de la boucle de rétro-action du CI).

Une fois la reprise d'activité assurée, le respect de ces directives peut être vérifié dans le cadre de contrôles de supervision *a posteriori*, par sondage (vérification du caractère justifié du recours à la procédure dérogatoire pour les opérations de l'échantillon, et de l'absence d'anomalies dans ces opérations).

II/ L'adaptation de la méthodologie du contrôle interne

Les modalités de maîtrise des risques en contexte contraint ne peuvent être les mêmes qu'en temps normal. La méthodologie du CI doit être adaptée et de nouveaux moyens d'intervention doivent être trouvés, afin de maintenir la vigilance sur les risques, sans alourdir les procédures. Une approche « agile », pragmatique est à privilégier pour assurer la continuité de la maîtrise des risques.

Dans un tel contexte, la dimension pédagogique de la fonction de référent CIF se révèle d'autant plus fondamentale, pour accompagner les services opérationnels dans la prise en compte des risques nouveaux / accrus du fait de la crise. Il s'agit de faire comprendre aux acteurs que l'intégration des exigences fondamentales de maîtrise des risques aux activités de gestion de crise ne constitue en rien une contrainte, mais bien au contraire un moyen de garantir leur bon déroulé.

Le rôle du référent CIF sera d'abord d'identifier les risques nouveaux nés de la crise, en lien avec les services métiers pour être le plus opérationnel possible. Il devra également analyser ses conséquences sur les risques majeurs pré-existants (augmentation de leur probabilité de survenance et / ou de leur impact), notamment au regard des allégements métiers et outils consentis durant la période de crise. Cette analyse préalable lui permettra d'orienter au mieux l'accompagnement prodigué aux services opérationnels, en fonction des points de vigilance les plus saillants à surveiller en priorité (*cf.* notamment rôle cité *supra* du référent CIF dans le cadre de l'équipe dédiée à la gestion de crise).

Cette vision actualisée des risques permettra également le recalibrage des plans de contrôle préalablement déployés : détermination des contrôles à maintenir et des contrôles pouvant devenir facultatifs ou être repoussés, adaptation des modalités de contrôle (échantillon réduit par exemple). Ce travail, consistant en un arbitrage entre les priorités en matière de maîtrise des risques et les moyens disponibles, est à réaliser nécessairement en concertation avec les services opérationnels, pour assurer la correcte prise en compte de leurs contraintes et possibilités.

Lorsque les contrôles pré-existants sont allégés, il importe de sensibiliser largement les services à l'importance de la traçabilité. La formalisation des opérations réalisées dans le cadre des procédures dérogatoires est une condition indispensable pour permettre la réalisation de contrôles *a posteriori*.

Enfin, le référent CIF pourra promouvoir auprès des services opérationnels le recours à certains outils d'auto-évaluation de leur maîtrise des risques, leur permettant de poser eux-mêmes, de manière souple et rapide, un diagnostic sur l'organisation de leur service et de leurs procédures (outils type « échelle de maturité de la gestion des risques » (EMR), organigramme fonctionnel nominatif (OFN), contrôle non prévu dans le plan de contrôle lancé à l'initiative du responsable de service, *etc.*). Ce recours pourra constituer un palliatif face à l'affaiblissement des autres formes d'évaluation du CI, plus poussées mais aussi plus lourdes, rendues plus difficiles à mener du fait du contexte de crise (exécution du plan de contrôle, missions d'audit interne ou externe).

III/ La focalisation sur les processus à enjeux et les risques majeurs

Le besoin, en contexte de crise, de concentrer les efforts et les moyens disponibles pour le CI sur les processus portant le plus d'enjeux et les risques considérés comme majeurs, renforce la nécessité de construire en amont des cartographies des processus et des risques valorisées et hiérarchisées, faisant clairement apparaître la priorisation arrêtée par l'instance de gouvernance ministérielle en matière d'enjeux et de risques.

Au titre des risques transversaux à l'échelle de l'État et en complément des risques propres à chaque ministère, les processus « Rémunérations », « Commande publique » et « Interventions » sont le plus souvent cités comme portant le plus d'enjeux.

En ce qui concerne l'identification des risques majeurs, les ministères peuvent, entre autres, se référer aux supports documentaires de CIF mis à leur disposition par la Direction du Budget et la DGFiP (notamment sur le serveur de la qualité comptable), qui le plus souvent distinguent les risques majeurs des autres risques.

IV/ Le renforcement de la vigilance en matière de fraude et de sécurité informatique

Le contexte de crise accroît les risques liés aux fraudes internes et externes et à la cybercriminalité. La concentration sur les processus à enjeux et sur les risques majeurs doit s'accompagner d'une attention renforcée à apporter à ces trois thématiques.

- En matière de fraude interne :

L'allègement des circuits de visa et la mise à mal du principe de séparation des tâches peuvent se traduire par une augmentation des permissivités en matière de fraude interne.

Il convient alors de veiller au caractère justifié des nouveaux cumuls de tâches[1] instaurés durant la crise (absence de solutions alternatives) et, lorsqu'ils se justifient, de veiller à prévoir les mesures de maîtrise des risques compensatoires (contrôle de supervision *a posteriori* notamment). En matière de lutte contre la fraude interne, le maintien des exigences de traçabilité se révèle là aussi fondamental, pour permettre la réalisation de contrôles *a posteriori*.

- En matière de fraude externe :

Les périodes particulières (congés, pics d'activité par exemple en fin de gestion) sont propices à la recrudescence des tentatives de fraude externe (fraude aux faux ordres de virement (FOVI), arnaque à la fausse prestation informatique…). Cela se révèle d'autant plus vrai dans un contexte de crise.

Le référent CIF devra veiller à la sensibilisation large et régulière des équipes. En matière de traitement des demandes de changement de coordonnées bancaires émanant des fournisseurs notamment, la pratique du contre-appel est à maintenir systématiquement.

- En matière de sécurité informatique :

Les contextes contraints fragilisent les dispositifs de sécurité informatique des entités publiques comme privées, avec des risques accrus à la fois d'origine interne (recours à des outils insuffisamment sécurisés, ouverture d'accès larges à des applications sensibles…) et externe (attaques informatiques type virus, rançongiciel…). En particulier, l'accroissement massif du télétravail implique de repenser la sécurité des accès à distance au réseau et aux applications informatiques de l'administration.

Là encore, le maintien de la vigilance passe par une sensibilisation accrue des agents : les impératifs en matière de sécurité informatique[2] doivent être largement diffusés et connus de tous. Des directives claires doivent être communiquées en matière de doctrine d'emploi des différents outils informatiques mobilisables (incluant l'interdiction du recours à certaines applications commerciales, non adaptées aux exigences de sécurité propres à l'administration). L'inscription systématique des télétravailleurs à des e-formations relatives à la sécurité informatique constitue à cet égard une bonne pratique.

1 Lorsque ces cumuls de tâches se traduisent par l'attribution de nouveaux rôles Chorus formulaires ou Chorus aux agents, il est possible de se référer à la « matrice des associations de rôles Chorus pour les gestionnaires », qui détermine le niveau de risques associé aux différentes associations de formulaires et rôles Chorus, et permet ainsi d'aiguiller le calibrage des mesures compensatoires à mettre en place.

2 Cf. notamment le « Recueil de recommandations relatives au système d'information financière de l'État » diffusé par la DGFiP à la communauté interministérielle en novembre 2020.

En complément de ces actions de sensibilisation, les contrôles de sécurité informatique feront partie des contrôles à maintenir en priorité (contrôle des accès aux applications sensibles via une revue périodique des habilitations et un contrôle de la qualité des mots de passe, contrôle de concordance ou d'interface entre applications, contrôle des écritures modificatives, *etc.*).

V/ Le repositionnement de l'audit interne en période de crise

Comme le CI, l'audit interne doit adapter ses modalités d'intervention et faire preuve d'agilité pour maintenir sa plus-value en matière de maîtrise des risques malgré un contexte contraint, pouvant rendre difficile la réalisation de missions d'audit « classiques ». Au même titre que le référent CIF, l'auditeur interne a un rôle d'accompagnateur des services opérationnels à jouer, afin d'assurer la sécurisation de la gestion de crise.

Quelques bonnes pratiques ont pu être identifiées en la matière :

- la mobilisation des forces d'audit en support pour la réalisation des missions identifiées comme prioritaires dans le PCA ;
- l'adaptation des modalités d'audit pour permettre leur réalisation à distance, lorsque les enjeux et les risques justifiaient leur maintien ;
- la mise en place d'audits de conseil, express et ciblés, consistant à réaliser une évaluation rapide de l'environnement de contrôle découlant du contexte de crise, afin d'identifier les vulnérabilités inhérentes aux procédures dérogatoires et de formuler des recommandations pour les couvrir.

VI/ Axes à approfondir pour améliorer la résilience des organisations face aux crises

Les crises éprouvent les capacités d'adaptation des administrations. Certains réflexes de maîtrise des risques ou outils du CI peuvent être mobilisés pour les renforcer.

- Repenser les organisations pour plus de flexibilité et plus de polyvalence

Exemples : généralisation des supports de sauvegarde partagés, documentation complète des procédures (pour permettre la reprise des tâches en cas d'absence), adaptation des besoins en formation, formation de binômes pour la polyvalence, intégration dans les OFN des possibilités de travail à distance de chaque agent (équipements, accès aux applications, *etc.*).

- Analyser les possibilités d'automatiser les contrôles les plus structurants

L'automatisation des contrôles les plus structurants permet le maintien d'un filet de sécurité même lorsque les ressources humaines manquent pour les contrôles intellectuels. De même, le portage du contrôle interne par une application dédiée contribue à accroître les capacités de pilotage du dispositif, en mettant à la disposition des acteurs un outil de reporting permettant le suivi des risques majeurs (les résultats des contrôles menés donnant une indication sur une éventuelle dégradation de la maîtrise des risques).

- Examiner la pérennisation de certains allègements introduits durant la crise

La crise peut constituer une opportunité pour optimiser les procédures, rationaliser les contrôles clés. Des procédures plus simples et plus souples seront en effet gages d'une plus grande résilience.

L'opportunité de la pérennisation de ces allégements devra nécessairement être appréciée au regard des résultats du contrôle interne, qui constituent un indicateur du degré de sécurisation des procédures concernées.