RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

GUIDE MÉTHODOLOGIQUE RELATIF AU CONTRÔLE INTERNE DES SYSTÈMES D'INFORMATION DES COLLECTIVITÉS LOCALES

Version Décembre 2020 / Mai 2022 (mises à jour de forme)

Sommaire

INTRODUCTION

OBJECTIFS DU GUIDE

Soucieuse de renforcer son partenariat avec les collectivités locales, la DGFiP entend développer son offre de conseil, au plus près de leurs attentes, et les soutenir dans la démarche de fiabilisation des comptes locaux.

Ainsi, la DGFiP s'attache à accompagner les collectivités locales en mettant à leur disposition des outils pour leur permettre, quelle que soit leur organisation :

- de procéder à un diagnostic de la situation existante ;
- de valoriser les actions déjà entreprises pour renforcer le dispositif de contrôle interne ;
- d'adapter les bonnes pratiques et contrôles proposés au regard de leur situation et de leurs moyens.

A ce titre, la DGFiP a rédigé un Guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales.

Ce guide s'adresse à l'ensemble des collectivités, et en particulier à celles engagées dans la démarche de fiabilisation et de certification des comptes locaux.

Il a pour périmètre le système d'information de la collectivité : les autres systèmes d'information concourant à la production des états financiers (Hélios par exemple) ne sont pas traités dans ce document.

Ce guide n'a pas vocation à prévaloir sur la réglementation en vigueur ou à venir, ni sur les normes ou pratiques qui seront adoptées par les certificateurs, mais vise essentiellement à apporter aux collectivités un éclairage sur les travaux à engager sur le volet système d'information du projet de fiabilisation et de certification des comptes. Il permet d'accompagner et de guider les collectivités qui souhaitent s'engager dans une démarche de maîtrise du risque numérique.

COMPOSITION DU GUIDE

Le présent guide est composé de deux parties :

- Partie 1 : présentation de la démarche contrôle interne des systèmes d'information ;
- Partie 2 : renforcement du contrôle interne des systèmes d'information

Des fiches synthétiques dédiées à la mise en œuvre d'un dispositif de contrôle interne des SI figurent en annexe à la fin de ce guide. Elles sont également mises à disposition des collectivités au format tableur afin de leur offrir un outil adaptable et simple d'exploitation.

PARTIE 1. PRÉSENTATION DE LA DÉMARCHE DE CONTRÔLE INTERNE DES SYSTÈMES D'INFORMATION

Un système d'information, généralement abrégé « SI », est un ensemble organisé de ressources permettant de collecter, regrouper, classifier, traiter et diffuser de l'information dans un environnement donné. Ces ressources peuvent être de plusieurs types : matériel, logiciel, personnel, données et procédures. Ces ressources sont par ailleurs inter-reliées. La notion de SI est donc plus vaste que le domaine des logiciels informatiques. En effet, les logiciels et outils informatiques ne sont qu'une des composantes des systèmes d'information.

Le système d'information occupe aujourd'hui une place stratégique et est au cœur du fonctionnement de toute collectivité. La qualité et à l'intégrité du système d'information conditionne aujourd'hui l'efficacité de l'administration.

1.1. L'IMPACT DU RISQUE NUMÉRIQUE SUR LA QUALITÉ DES COMPTES LOCAUX

1.1.1. Le risque numérique et ses facteurs déclenchants

La gestion du risque requiert d'opérer une distinction entre :

- les facteurs déclenchants ;
- leurs conséquences : la gravité et les impacts du risque en lui-même.

Ainsi, le risque résulte d'un ou plusieurs facteurs déclenchants.

La notion de risque numérique

Le risque numérique désigne une catégorie de risques variés tels que :

- l'inadéquation du SI avec la stratégie de l'entité et les besoins des utilisateurs ;
- le manque de résilience et notamment l'incapacité de la collectivité à redémarrer les systèmes informatiques en cas d'arrêt ou de destruction ;
- une sécurité du SI inadaptée avec la présence de vulnérabilités non connues ou couvertes ;
- une insuffisante protection des accès aux données et aux applications avec la possibilité de consultation, modification ou corruption de données par des attaquants ;
- un accès à des données confidentielles par des personnes non autorisées au sein de la collectivité ;
- des vulnérabilités applicatives provenant des d'applications informatiques non fiables, c'est-à-dire non protégées contre certaines attaques informatiques ;
- un manque de fiabilité du système informatique qui présente certaines indisponibilités récurrentes sur des applications essentielles aux services métiers ;
- une possibilité de détournement des applications qui peut reposer sur une mauvaise utilisation (intentionnelle ou non) du SI par les utilisateurs ;
- un SI non conforme avec la législation numérique notamment en ce qui concerne les règles de confidentialité du Règlement Général de Protection des Données (RGPD) ;
- une obsolescence applicative, logicielle et technique du SI qui nuit à la pérennité du SI et crée des vulnérabilités ;
- etc.

Ces risques sont liés à l'utilisation, la conception, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit. Compte tenu de l'engagement des collectivités dans

une transformation numérique profonde, le risque numérique pèse de plus en plus fortement sur l'activité des collectivités territoriales. Il ne doit donc pas être circonscrit au seul périmètre des systèmes d'information mais intégré à la démarche globale de maîtrise des risques de la collectivité.

Ses facteurs déclenchants

Pour apprécier le risque numérique de manière globale, il convient de prendre en compte tous ses facteurs sous-jacents, qu'ils soient internes ou externes à la collectivité :

- **le facteur humain ;**

Il recouvre à la fois les utilisateurs et les administrateurs. Souvent minimisé, le facteur humain est le plus important et les collaborateurs doivent être pleinement intégrés à la stratégie de sécurité numérique.

Le facteur humain doit en outre être apprécié au regard du développement croissant de nouveaux modes d'organisation du travail : travail à distance (télétravail, nomadisme), espaces de co-travail (ou co-working). Cette mobilité professionnelle croissante permet à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants. Elle génère donc de nouveaux risques que les collectivités locales doivent prendre en compte.

- **le facteur technique ;**

Le facteur technique inclut les incidents liés au matériel (processeur, composants électroniques, etc.), aux logiciels et interfaces applicatives. Les changements informatiques importants et non maîtrisés sont donc un facteur de risque. A contrario, une évolution trop lente du SI, en raison des vulnérabilités qu'elle engendre, peut également constituer un facteur de risque. Par ailleurs, l'utilisation des hébergements sur des technologies de type « Cloud » peut engendrer un risque en matière de sécurité des données.

- **le facteur environnemental ;**

La maîtrise du risque numérique nécessite de porter une attention particulière à la gestion de l'environnement matériel du SI et des locaux (énergie, climatisation, etc.) et de mettre en place une politique de sécurité adéquate. Il est en outre indispensable de prévoir les moyens d'alerte et de protection contre les incidents environnementaux (incendie, inondation, etc.). Ceux-ci doivent être adaptés à la criticité de l'application considérée, c'est-à-dire à l'importance de l'application pour la sphère métier, son rôle au sein du SI, son impact économique et fonctionnel, ses interactions et dépendances avec l'écosystème informatique ainsi que le degré de risque encouru en cas de dysfonctionnement.

- **le facteur juridique.**

Sécuriser un SI, c'est également garantir sa sécurité juridique. La mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire[1] destiné notamment à **sécuriser les échanges électroniques** entre les usagers et les administrations, et entre les administrations elles-mêmes[2] (certificat, signature et envoi recommandé électroniques, etc.), à **protéger les données personnelles**[3] et à **garantir le respect du droit d'auteur**[4]. La collectivité doit également respecter les obligations relatives à l'ouverture des codes sources et des données publiques telles que précisées par la loi pour une République numérique[5].

Certaines collectivités sont en outre désignées « opérateurs d'importance vitale (OIV) »[6] ou « opérateur de services essentiels (OSE) »[7]. A ce titre, elles doivent respecter un cadre législatif et réglementaire plus contraint.

1. *« Sécurité numérique des collectivités territoriales - l'essentiel de la reglementation » élaboré par l'ANSSI.*
2. *Référentiel Général de Sécurité (RGS) et règlement no 910/2014 du 23 juillet 2014 2, dit règlement « eIDAS ».*
3. *Article 32 du « Règlement Général sur la Protection des Donnees (RGPD) » et article 226-17 du Code pénal.*
4. *Code de la propriété intellectuelle.*
5. *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.*
6. *Les OIV sont des organisations qui, si elles venaient à subir un incident grave, pourraient porter gravement atteinte au potentiel de guerre ou économique, a la sécurité ou a la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population (articles L. 1332-6-1 et suivants du code de la défense).*
7. *Les OSE sont des organisations qui supportent des services dits essentiels au fonctionnement de la société ou de l'économie (alimentation, sanitaire, etc.) et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires a la fourniture desdits services (directive UE n°2016/1148 « Network and Information Systems (NIS) »).*

Face à l'interconnexion des systèmes d'information, au développement des services en ligne pour les usagers et du travail à distance, le facteur de risque de non-conformité du SI ne doit pas être négligé.

L'ensemble des facteurs de risque évoqués supra doivent donc être pris en compte dans tout nouveau projet informatique et toute maintenance des applications existantes.

1.1.2. L'impact du risque numérique sur la qualité des comptes locaux

Le risque numérique est susceptible d'avoir des impacts variés :

- impact en matière de sécurité des biens et des personnes (ex : incendie, mise en danger des personnels) ;
- impact budgétaire (ex : coût lié à la détérioration du matériel, fraude) ;
- impact organisationnel (ex : lenteur, surcharge ou indisponibilité totale ou partielle du réseau) ;
- impact juridique (ex : engagement de la responsabilité de la collectivité en raison du non-respect de la protection des données personnelles).

Le SI traduit en outre des évènements de gestion en comptabilité. De fait, le risque numérique a également une incidence sur la production des informations financières et comptables et doit donc être considéré comme une composante de la fonction comptable.

De part la qualité de l'information qu'il restitue, **le système d'information doit donc contribuer à assurer la régularité et la sincérité des comptes**[8]. Il doit également garantir l'image fidèle du résultat de la gestion, du patrimoine et de la situation financière des collectivités locales et de leurs établissements publics.

Par ailleurs, le développement du numérique impacte de plus en plus les processus de gestion dans les collectivités. La compréhension de ces processus automatisés et de leur niveau de maîtrise et de contrôle par les collectivités, devient aujourd'hui incontournable dans le contexte de fiabilisation des comptes publics locaux.

Les collectivités locales et les établissements publics locaux doivent ainsi se préparer à répondre aux exigences de contrôle interne des systèmes d'information dans le cadre de la fiabilisation et de la certification des comptes locaux[9].

Afin de certifier les états financiers d'une entité, le certificateur s'appuie notamment sur la qualité du contrôle interne des systèmes d'information concourant à l'élaboration de l'information comptable et financière des collectivités territoriales. Dans ce cadre, il peut être amené à examiner :

- les éléments d'organisation et de contrôle sur lesquels s'appuie le système d'information de l'entité ;
- la fiabilité des applications informatiques utilisées.

Ainsi, le certificateur ne s'intéresse pas seulement aux comptes, mais procède également à une revue et à une évaluation du système d'information de la collectivité, support de la comptabilité.

1.2. COMMENT MAÎTRISER LE RISQUE NUMÉRIQUE ?

La gestion du risque numérique, compte tenu de son caractère transversal, ne peut plus être restreinte à la seule sécurité des systèmes d'information, ni aux seules activités transverses ou de support. Elle doit être intégrée dans le cadre plus général de la gestion des risques à l'échelle de l'organisation.

1.2.1. Élaborer une cartographie des risques

L'intégralité des risques portés par une collectivité ne peut être couverte. La démarche de maîtrise des risques se veut donc globale et pragmatique. La collectivité doit cibler ses actions en fonction des zones de risques à fiabiliser en priorité.

8. *Article 47-2 de la Constitution et article 27 de la loi organique n°2001-692 du 1er août 2001 relative aux lois de finances (LOLF).*

9. *Article 110 de la loi du 7 août 2015 portant nouvelle organisation territoriale de la République.*

Pour être en capacité de couvrir les risques majeurs pouvant survenir dans l'exercice de ses missions, la collectivité doit donc identifier et hiérarchiser les risques propres à chaque activité ou « processus ».

La démarche, pour identifier et hiérarchiser les risques, se déroule à travers **trois étapes**[10] **:**

1. **recenser les risques relatifs à chaque procédure** ;
2. pour chacun des risques recensés, évaluer la probabilité de survenance du risque, et la gravité des impacts en cas de réalisation afin d'**évaluer le risque inhérent à l'activité** ;
3. **analyser les effets du dispositif de contrôle interne pour évaluer le risque résiduel** ;

Cette dernière étape vise à nuancer l'analyse des risques afin d'apprécier le **risque résiduel**, c'est-à-dire le risque réel qui subsiste après la prise en compte des mesures de contrôle interne pré-existantes.

Cette méthode permet de conduire à une classification des processus ou procédures en quatre niveaux de sensibilité : risque résiduel faible, modéré, significatif ou critique.

Cette hiérarchisation des risques ainsi obtenue pourra être formalisée par la collectivité dans une **cartographie des risques**, recensant l'ensemble des risques majeurs de la collectivité et notamment ceux liés au système d'information financière.

Ce document est essentiel dans le cadre du pilotage de la démarche de maîtrise des risques. Il doit tenir compte des spécificités et des problématiques propres à chaque collectivité (particularités géographiques, moyens humains, compétences techniques, etc.). Par ailleurs, en vue d'avoir une évaluation précise des risques, il est nécessaire d'identifier toutes les parties qui prennent part ou qui sont incluses dans le dispositif et d'impliquer le personnel encadrant mais aussi les collaborateurs des services opérationnels. La collaboration de l'ordonnateur et du comptable est également fortement préconisée.

1.2.2. Renforcer le dispositif de contrôle interne des SI

Afin de couvrir les risques identifiés dans la cartographie, il convient de définir les mesures destinées à renforcer le dispositif de contrôle interne existant.

Ces mesures devront consolider **les trois leviers du contrôle interne** que sont :

- la documentation :

Le levier « documentation » vise principalement à documenter l'organisation, les procédures, les contrôles et les risques.

Exemple de mesures : élaboration et diffusion d'un organigramme fonctionnel nominatif, d'une cartographie des processus et d'une cartographie des risques, d'une fiche de procédure et des contrôles associés, etc.

- l'organisation :

Le levier « organisation » correspond à la définition et l'organisation des tâches, des acteurs et des contrôles.

Il vise à garantir le principe de continuité par une attribution claire des tâches de chaque acteur (titulaire/suppléant, séparation des tâches) et une gestion suivie des délégations. Les habilitations informatiques doivent en outre être conformes aux attributions de chacun.

Enfin, le levier « organisation » consiste à s'assurer que les contrôles sont correctement menés et ce sur l'ensemble du processus, depuis le service responsable de l'acte initial (ou du fait générateur) jusqu'au comptable. Ces contrôles sont dits :

- « *intellectuels* » lorsqu'ils sont réalisés par les opérationnels ;
- « *applicatifs* » lorsqu'ils sont intégrés au SI.

10. *Ces étapes correspondent à la démarche classique d'identification des risques en matière de contrôle interne. Afin d'identifier les risques propres au SI, les collectivités pourront également s'appuyer sur la méthode EBIOS Risk Manager.*

Tableau récapitulatif des contrôles intellectuels et les contrôles applicatifs

Contrôles « intellectuels »	**auto-contrôles**	Contrôles exercés par un agent sur ses propres opérations.
	contrôles mutuels	Contrôles exercés par un agent sur les opérations effectuées en amont par un autre agent (principe de séparation des tâches).
Contrôles « applicatifs » *	**contrôles manuels**	Processus de validation par un responsable approprié (ex : validation dans l'application d'un formulaire de demande)
	Contrôles semi-automatisés ou automatisés	Vérification que l'enregistrement sollicité est conforme aux prescriptions définies dans les paramètres du SI

Les contrôles applicatifs semi-automatisés ou automatisés doivent être privilégiés cas ils permettent de générer une alerte ayant pour objectif d'informer l'utilisateur du résultat du contrôle ou être bloquants, empêchant ainsi l'utilisateur d'aller plus loin si le résultat du contrôle est négatif.

- La traçabilité :

Le levier « traçabilité » a pour objectif de permettre à tout moment de justifier une opération, en remontant de l'enregistrement en comptabilité jusqu'au fait générateur de l'opération et inversement.

Exemple : modification du système d'information afin de tracer l'intervention des acteurs, mise en place d'interface entre des applications informatiques pour éviter les ruptures applicatives, gestion des habilitations informatiques et des mots de passe, archivage des pièces justificatives, etc.

En pratique, la traçabilité des acteurs et des opérations comptables est de plus en plus fréquemment portée par les systèmes d'information (sous réserve du respect du dispositif d'habilitations, du caractère individuel des identifiants et du secret des mots de passe).

1.2.3. Évaluer le dispositif de contrôle interne des SI

Une fois le dispositif de contrôle interne défini, il est indispensable d'en **évaluer périodiquement l'effectivité et l'efficacité**. Cette évaluation peut être réalisée en interne ou par des auditeurs externes, comme dans le cadre de la certification des comptes.

- En interne

La collectivité doit périodiquement auto-évaluer les mesures de contrôle interne. Cette évaluation peut notamment être faite au moyen de :

- **contrôles de supervision :**

Contemporains ou a posteriori[11], ces contrôles permettent à l'encadrement de s'assurer de l'effectivité des auto-contrôles et contrôles mutuels réalisés par les opérationnels. Ils ciblent en priorité les processus et opérations à enjeux et/ou à risques. En cas d'anomalie, l'encadrement doit analyser la pertinence de dispositif de contrôle interne et, le cas échéant, mettre en œuvre des actions destinées à le renforcer en agissant sur l'un des trois leviers (organisation, documentation, traçabilité).

- **l'audit interne :**

11. *Les contrôles de supervision contemporains sont réalisés lors du déroulement d'une procédure (ex : étape de validation par le chef de service). Les contrôles de supervision a posteriori interviennent après le dénouement de la procédure.*

Les auditeurs peuvent être amenés à procéder à une analyse du système d'information dans le cadre d'une mission généraliste (audit d'organisation, audit de processus, audit de régularité, etc.) ou principale, l'analyse du SI constituant alors l'objet principal de la mission de contrôle. Dans ce second cas, l'audit doit être indépendant des acteurs du système d'information et répondre aux normes professionnelles communément admises dans le secteur de l'audit des systèmes d'information. Les auditeurs doivent mobiliser des compétences informatiques spécifiques afin de s'assurer de la fiabilité des données, des applications et de l'infrastructure du SI audité.

- Dans le cadre de la certification des comptes

Le champ d'action du certificateur couvre tout ou partie des applications intervenant dans la saisie et le traitement des informations, depuis la survenance du fait générateur jusqu'à la production des états financiers. Le périmètre inclut donc :

- les applications supportant les cinq principaux processus comptables : recettes, personnel, immobilisations, achats, endettement long terme et trésorerie court terme.
- les progiciels[12], les applications spécifiques développées en interne par les collectivités ainsi que les outils bureautiques de type tableur ou bases de données ;
- le système comptable Hélios ainsi que les interfaces mises en place avec le système d'information de la collectivité.

La revue du système d'information dans le cadre de la certification des comptes comporte plusieurs étapes :

1. **prise de connaissance du système d'information** : le certificateur analyse l'incidence de l'environnement informatique sur la production des informations financières et comptables (applications clés et infrastructure les supportant, contrôles applicatifs, interfaces, référentiels de données de bases) ;

2. **revue des contrôles généraux informatiques** : le certificateur appréhende l'environnement de contrôle interne relatif aux applications supportant les processus métiers et l'information comptable et financière. Cette revue peut permettre :

- d'identifier les axes d'amélioration de l'organisation informatique par rapport aux référentiels de bonnes pratiques parmi lesquelles figure la mise en œuvre d'une interopérabilité entre les différentes briques du SI ;
- d'évaluer le niveau de sécurité et de séparation des tâches au sein des applications et de l'organisation ;
- d'appréhender les mécanismes en place concourant à assurer la continuité d'activité et la reprise en cas d'incident ;
- d'analyser l'homogénéité des procédures de contrôle entre les différents environnements techniques et applicatifs audités ;
- d'apprécier la permanence et la régularité des contrôles d'une année sur l'autre.

3. **revue ciblée de processus et tests des contrôles** : le certificateur met en exergue les forces et faiblesses des processus métiers et teste l'efficacité opérationnelle des contrôles embarqués dans les applications supportant les processus métiers.

1.2.4. Faire évoluer la cartographie des risques

L'évaluation du dispositif de contrôle interne des SI permet de mettre en exergue les points forts et faiblesses dans le déroulé des procédures de la collectivité. Au regard de ces constats et dans une **démarche d'amélioration continue**, il est recommandé que l'analyse des risques et la cartographie qui en découle soient mis à jour a minima annuellement. Au regard de cette nouvelle cartographie, les mesures de contrôle interne induites devront être revues afin de renforcer ou alléger les contrôles en fonction du degré de maîtrise des risques par les opérationnels.

12. *Applications standardisées ou adaptées acquises auprès d'éditeurs ou intégrateurs*

PARTIE 2. RENFORCEMENT DU CONTRÔLE INTERNE DES SI

Cette partie liste des bonnes pratiques en matière de contrôle interne des SI.

Pour chacune des thématiques abordées, des fiches synthétiques sont disponibles en annexe, situées à la fin du présent guide.

Il conviendra, pour la collectivité inscrite dans une démarche de fiabilisation de comptes, de collecter et recenser la documentation disponible et d'évaluer le respect des bonnes pratiques dans la mise en œuvre de ses processus internes.

2.1. ORGANISATION DE LA FONCTION SI

La fonction SI fait intervenir plusieurs acteurs, et notamment :

- La Direction des Systèmes d'Information

La Direction des Systèmes d'Information (DSI) est chargée de la gouvernance des systèmes d'information au sein de la collectivité.

Ses domaines de compétence sont divers et ne doivent pas se limiter à la simple gestion du système d'information. Elle doit permettre de contrôler et de faire évoluer les SI dans le cadre d'une démarche stratégique définie par la collectivité.

- Le Responsable de la Sécurité des Systèmes d'Information

Un Responsable de la Sécurité des Systèmes d'Information (RSSI) est nommé dans la collectivité.

Compte tenu de la complexité des risques encourus et des problématiques suscitées, il est recommandé que les RSSI ne soient pas rattachés à la direction des systèmes d'information (DSI) mais directement à la Direction générale.

Ses fonctions sont définies dans la collectivité de manière indépendante aux missions de la DSI. Il est notamment chargé :

- d'organiser et mettre en œuvre la sécurité des SI de la collectivité ;
- de garantir l'intégrité, l'accessibilité et la disponibilité des SI ;
- de sensibiliser les agents, les prestataires et les utilisateurs aux enjeux de sécurité.

- Les Directions « métiers »

Les Directions « métiers » et la DSI doivent collaborer afin de définir ensemble de nouveaux modèles d'organisation et de gouvernance.

A ce titre, un comité de pilotage[13], associant la direction générale, la DSI, le RSSI ainsi que les directions « métier », peut être mis en œuvre au sein des collectivités afin d'actualiser les projets en fonction des avancements et des innovations. Chaque rencontre du comité de pilotage doit donner lieu à rédaction d'un compte-rendu porté à la connaissance de l'ensemble des participants ainsi qu'à la direction générale.

2.1.1. Mettre en place une gouvernance du SI au moyen d'un schéma directeur

Le terme « gouvernance des SI » fait référence aux moyens de gestion et de régulation des SI mis en place dans une collectivité pour atteindre ses objectifs stratégiques.

Il est recommandé de matérialiser la stratégie informatique de la collectivité dans un schéma directeur pluriannuel dont le but est de définir, de manière globale, la politique d'organisation et d'automatisation du SI en accord avec les capacités organisationnelles et les ressources de l'entité.

13. *Voir partie 2.3.1 « Piloter les évolutions du SI ».*

L'élaboration d'un schéma directeur se déroule en plusieurs étapes :

- définition du processus d'élaboration et de validation (note de cadrage, calendrier, etc.)
- diagnostic de l'existant et définition des besoins et des enjeux en prenant en compte les problématiques organisationnelles, fonctionnelles, applicatives, techniques, réglementaires ;
- détermination des orientations et identification des différents scenarii, et évaluation des risques et de leurs impacts ;
- définition du schéma directeur et de son plan d'action.

Afin de garantir que les besoins utilisateurs sont pris en compte dans les différents projets, le processus d'élaboration du schéma directeur doit associer les acteurs métiers. L'approbation du schéma directeur doit relever de la direction générale afin de s'assurer qu'il décline les grandes orientations stratégiques de la collectivité au niveau du SI.

Une fois établi, le schéma directeur fournit à la DSI une démarche méthodologique fiable et performante sur laquelle s'appuyer pour piloter le système d'information et contrôler les projets stratégiques.

Il doit être mis à jour régulièrement et a minima une fois par an. Le schéma directeur et ses révisions doivent être conservés et archivés par la collectivité. La transparence du schéma directeur pour l'ensemble des agents de la collectivité est un atout de mobilisation collective.

En complément, la collectivité doit être en capacité de fournir une liste des projets en cours ou à venir. Cette liste doit permettre d'identifier les différentes typologies de projets menés (ex : acquisition d'une nouvelle solution, évolution du SI /migration) et les principes définis en matière de gestion de projet.

2.1.2. Élaborer un organigramme fonctionnel nominatif de la fonction SI

Au même titre que les directions « métiers » avec lesquelles elle collabore, l'organisation de la DSI doit être formalisée au sein d'un organigramme fonctionnel nominatif (OFN), précisant, pour chaque processus dont elle est en charge, la répartition des tâches existante.

Tableau représentant un exemple d'organigramme fonctionnel nominatif
Collectivité X - Processus « Gérer les serveurs locaux »

Date :		COLLECTIVITÉ X							
PROCESSUS : GÉRER LES SERVEURS LOCAUX									
PROCÉDURES	TÂCHES	TITULAIRE			SUPPLÉANT			SUPERVISION	
		NOM	DÉLÉGATION DE SIGNATURE	APPLICATION / HABILITATION INFORMATIQUE	NOM	DÉLÉGATION DE SIGNATURE	APPLICATION / HABILITATION INFORMATIQUE	RESPONSABLE DE LA SUPERVISION	NATURE DE LA SUPERVISION
Exploitation	Expertise des besoins utilisateurs								
	Installations								
	Configurations								
	Suivi - mise à jour								

Les organigrammes des directions « métiers » et de la DSI doivent être régulièrement mis à jour (et a minima annuellement) au regard des mouvements de personnel et des changements d'affectation au sein de l'entité. Les OFN et leurs révisions doivent être conservés et archivés par la collectivité.

Lorsque les projets reposent sur une organisation agile[14], une maquette d'organigramme adaptée pourra être envisagée. Cette maquette devra permettre d'identifier, en fonction du rôle joué par l'agent, les tâches réalisées.

14. *Cf. § 2.3. Gestion des évolutions du SI.*

Diffusés à l'ensemble des agents de la DSI ainsi qu'aux autres services de la collectivité, ils contribuent à favoriser le bon déroulement des procédures et le décloisonnement entre les services en permettant à tous d'identifier le champ de responsabilité de chacun des services et collaborateurs.

L'OFN est la traduction pratique du levier « organisation » du dispositif de contrôle interne. Il permet à la collectivité de porter un regard critique sur l'organisation au sein de la DSI :

- l'intégralité des tâches relevant de la DSI sont-elles effectivement prises en compte ?
- les rôles et les responsabilités de chaque intervenant figurant sur l'organigramme sont-ils clairement définis et délimités ?
- existe-t-il des tâches redondantes perturbant la fluidité des processus ?
- existe-t-il des tâches à faible valeur ajoutée pouvant être automatisées ?
- la répartition des tâches au sein du service permet-elle de garantir la continuité de service ? Des suppléants sont-ils désignés pour assurer la mise en œuvre des opérations clés en l'absence des titulaires ?
- les tâches incompatibles sont-elles séparées ? Cette séparation des tâches est-elle effective lors de la rotation des équipes, des vacances et du départ d'un personnel ?
- le recensement des habilitations informatiques est-il exhaustif ? Les habilitations informatiques sont-elles conformes aux attributions et délégations de chacun (saisie, validation, paramétrage, etc.) ?
- l'organisation comporte-t-elle des opérations de sécurisation : contrôles mutuels, contrôles de supervision, etc.) ? Les modalités de réalisation des contrôles sont-elles documentées ?
- les effectifs sont-ils en adéquation aux besoins et aux enjeux ?

En cas de défaillance dans l'organisation, il convient de prendre les mesures correctrices nécessaires.

2.1.3. Séparer les fonctions et les accès au SI

L'élaboration d'une « matrice des incompatibilités » (ou d'un « référentiel de séparation des tâches ») permet d'identifier si les tâches réalisées par une même personne sont incompatibles entre elles.

À ce titre, les incompatibilités doivent être analysées au sein des directions « métiers » de la collectivité, ainsi qu'au sein de la DSI.

Exemple : les tâches de développement d'une application, de test, puis de mise en production doivent autant que possible être séparées.

Pour être efficace, la séparation des tâches doit être déclinée et paramétrée dans le SI. Ainsi, les droits d'accès au SI doivent refléter les règles de séparation des tâches telles que définies dans l'organisation et être conformes aux délégations de pouvoir accordées au sein de la collectivité.

Exemple : les développeurs ne doivent pas avoir accès à l'environnement de production. Les environnements d'études et de production doivent en effet être séparés.

A titre très exceptionnel, il peut être dérogé à la matrice des incompatibilités. Dans cette hypothèse, des contrôles doivent être impérativement mis en œuvre pour pallier les cumuls de fonctions ou de rôles incompatibles.

2.1.4. Cartographier le SI

Cartographier un système d'information consiste à recenser et classer tout élément constituant le SI dans un seul référentiel pour en avoir une vision globale.

De manière générale, une cartographie du SI est composée de plusieurs vues :

Vue	Objet	Acteur concerné

Vue	Objet	Acteur concerné
Vue « applicative »	Cette vue présente l'architecture du SI en termes d'éléments applicatifs (description et rôle) ainsi que les flux échangés entre eux. Elle présente également les outils transverses (messagerie, bases de données, etc.).	Maîtrise d'œuvre
Vue « infrastructure »	Cette vue présente l'architecture matérielle et réseau du SI, en décrivant toute l'infrastructure qui supporte et héberge le système d'information.	Production

Les états financiers de la collectivité sont le résultat de la traduction des informations transmises par les applications financières et « métiers » de la collectivité, et par Hélios utilisé par le comptable public. L'élaboration d'une telle cartographie est une condition préalable de la fiabilité de l'information financière.

La cartographie du SI est en outre un outil :

- **décisionnel :** elle permet de réaliser l'inventaire des composants du SI et leur description détaillée, d'identifier les redondances dans le SI pour optimiser les coûts. Elle facilite l'identification des applications obsolètes qui ne sont plus adaptées aux besoins de la collectivité.
- **de pilotage** afin de comprendre les interactions entre les différents acteurs, utilisateurs et fonctions et de définir les règles de gouvernance.
- **de maîtrise des risques :** elle facilite l'identification des applications les plus exposées aux menaces afin de mettre en œuvre les mesures adéquates de protection. Elle permet en outre de qualifier les impacts « métiers » et de prévoir les conséquences d'incident ou d'une attaque numérique.
- **de gestion de crise :** elle est primordiale dans le cadre de la définition des activités prioritaires de la collectivité et de la définition d'un plan de continuité d'activité.

Il est préconisé que les collectivités se dotent a minima d'une cartographie applicative représentant sous forme graphique les principales applications du système d'information (fonctionnalités, système d'exploitation, base de données…) ainsi que les flux de données (type de données, format, fréquence du flux…).

Cette cartographie doit être régulièrement mise à jour en cas d'évolution du SI. La cartographie et ses révisions doivent être conservées et archivées. Elle doit être partagée avec l'ensemble des agents de la collectivité afin de faciliter la compréhension de l'environnement numérique par tous les agents de la collectivité.

2.1.5. Recenser les applications, les interfaces, les contrats et les effectifs

Afin de disposer d'une connaissance fine du SI, il est préconisé de tenir à jour une synthèse des effectifs internes et externes agissant pour le compte de la DSI ainsi qu'une liste :

- des principales applications financières et métiers ;
- des principales interfaces internes et externes ;
- des contrats internes et externes passés par la DSI de l'établissement ou ayant un impact sur la disponibilité du SI (contrat de maintenance, de service, etc.) ;
- des données issues de chaque SI.

Ces listes pourront être établies dans des tableaux de synthèse joints en annexe de la cartographie du SI qui aura été élaborée. Les informations suivantes devront être détaillées :

Principales	• Nom de l'application

applications financières et métiers	• Interlocuteurs (maître d'ouvrage « MOA »/ maître d'œuvre « MOE ») • Fonctionnalités • Type d'hébergement (local, externalisé) • Lieu d'hébergement ou nom du tiers (si externalisé) • Type d'application (développement interne ou par un tiers, progiciel, fichier bureautique) • Date de mise en place • Support éditeur • Prestataire pour la maintenance • Date de fin d'utilisation prévue (le cas échéant) • Système d'exploitation (OS) du serveur hébergeant l'application • Système de gestion de base de données • Projets d'évolution (ou montées de version) • Virtualisation[15] ? (Oui/Non) • Criticité (1 à 5)

Interfaces	• Identifiant d'interface (ID) • Application source du flux • Application destinataire du flux • Type de flux (automatique, semi-automatique, manuel) • Nature des flux et des données échangées • Périodicité (quotidienne, hebdomadaire, mensuelle, etc.) • Déclenchement du flux • Contrôles informatiques existants nécessaires à la sécurisation des flux de données entre les systèmes.

L'établissement d'une liste des interfaces vise à recenser les principaux liens qui existent entre les différentes applications. Elle permet en outre de s'assurer du respect des préconisations. En matière d'interface, il est recommandé :

- d'utiliser une application unique pour l'ensemble d'un processus afin d'**éviter les ruptures applicatives** ;
- de **limiter les interfaces manuelles** entre les applications « métier » et l'application comptable et financière de la collectivité. En effet, l'interfaçage automatisé des applications doit être recherché afin d'éviter la ressaisie des informations et les risques d'erreurs ou de détournements.
- de mettre en place des **contrôles** afin de s'assurer de l'exhaustivité des flux, leur intégrité et la réalité des écritures comptables associées.

Contrats[16]	• Partenaire • Objet du contrat

15. *Une application virtualisée n'est pas installée sur un poste de travail physique. Lorsqu'une application est virtualisée, les administrateurs informatiques peuvent configurer des applications à distance sur un serveur. Les utilisateurs peuvent accéder et utiliser l'application à partir d'un ordinateur différent de celui sur lequel l'application est installée.*

16. *Tout contrat d'externalisation doit contenir a minima le périmètre du contrat (applications, infrastructure, services…), la responsabilité des deux parties, les clauses de résiliation, les niveaux de services attendus et leurs modes de revue, les actions à mettre en œuvre en cas de niveaux de service d'insuffisants, les modalités de fin des prestations, les modalités d'échanges avec le prestataire, notamment en matière de délai, d'états souhaités, de documentation des systèmes, les modalités d'audit du prestataire.*

	• Date d'engagement • Date de fin d'engagement • Indicateurs de niveau de service

Ce recensement doit notamment couvrir les contrats de service (Service Level Agreements - SLA) ainsi que les engagements de prestations en interne (Operational Level Agreements - OLA).

Il permet d'apprécier le niveau d'externalisation du SI et de dépendance vis-à-vis des prestataires.

L'externalisation consiste à faire appel à un fournisseur de services externes pour gérer une partie des services informatiques. Afin de maîtriser les risques liés à cette externalisation, les collectivités et leur(s) prestataire(s) doivent mettre en place et gérer des règles et des mesures de contrôle qui couvrent les rôles et responsabilités de chaque partie, les prestations et le niveau de service attendus. En cas de défaillance du (ou des) prestataire(s) dans ses contrôles, la collectivité doit veiller à mettre en œuvre des contrôles et planifier les corrections appropriées.

Effectifs	• Synthèse des effectifs internes et externes agissant pour le compte de la DSI

2.1.6. Définir des doctrines d'emploi et élaborer des guides utilisateurs

Outre les documents d'architecture technique[17], chaque application du SI doit faire l'objet d'une doctrine d'emploi précisant l'objectif et les cas de recours à l'application.

La doctrine d'emploi fixe les situations ouvrant un droit à une application informatique. Elle doit s'attacher à limiter l'accès aux acteurs devant intervenir dans le SI pour réaliser leur mission.

Les administrateurs d'habilitation et les responsables de service s'appuieront ensuite sur cette doctrine d'emploi pour attribuer les droits aux intervenants sous leur autorité.

La doctrine d'emploi doit être diffusée largement afin que chaque agent connaisse la finalité attachée à chaque application et puisse identifier le processus dans le cadre duquel il est autorisé à utiliser telle ou telle application. Si plusieurs applications sont déployées sur tout ou partie d'un processus, chaque application doit faire l'objet d'une doctrine d'emploi qui lui est propre.

Un guide utilisateur détaillant comment utiliser l'application complète la doctrine d'emploi. Il doit être exhaustif, actualisé à chaque modification de l'application, et facilement accessible pour les utilisateurs. Les guides doivent autant que possible être mis à disposition de manière numérique avec un système de navigation simple et ergonomique.

2.1.7. Établir une liste des comptes existants

Une liste des utilisateurs des applications, bases de données et systèmes d'exploitation clés est établie. Cette liste des comptes existants est classée selon les principes « utilisateurs nommés, administrateurs, comptes génériques ».

Ce document est indispensable pour la réalisation des revues, a minima annuelle, des comptes afin de s'assurer qu'ils sont justifiés.

17. *Cf. § 2.3.2. Élaborer les documents de cadrage du projet / Approbation du projet.*

2.2. POLITIQUE DE SÉCURITÉ DES SI

La Politique de Sécurité des Systèmes d'information (PSSI) définit les objectifs à atteindre (ex : assurer la continuité des activités régaliennes, prévenir des fuites d'informations sensibles, renforcer la confiance des usagers, etc.) et les moyens accordés pour y parvenir.

C'est le document de référence en matière de sécurité des systèmes d'information de la collectivité. Elle présente, de manière ordonnée, les règles de sécurité à appliquer et à respecter. Après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires…). Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir.

La PSSI doit évoluer au gré des transformations du contexte de la collectivité (changement d'organisation, de missions…) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux).

L'objectif de cette partie n'est pas de revenir sur l'analyse des risques et des facteurs déclenchants qui guident les choix de la collectivité en matière de sécurité des systèmes d'information. Il est de mettre en exergue les éléments permettant à la collectivité de justifier qu'une politique de sécurité des SI est définie et mise en œuvre.

2.2.1. Sécuriser les sites d'hébergement informatique

L'hébergement informatique est la fourniture de l'environnement et des services associés, conformément aux besoins exprimés de sécurité (accessibilité, disponibilité, confidentialité…), nécessaires à la production d'un système d'information constitué de matériels informatiques, réseaux et télécommunications.

La sécurité de ces sites, ainsi que la gestion des installations, la gestion des incidents, la gestion de proximité des salles d'hébergement et le respect des bonnes pratiques documentaires constituent une priorité compte tenu de la nécessité de la continuité de fonctionnement des services.

Les collectivités s'assurent du respect des bonnes pratiques techniques propres au métier d'hébergeur et de la mise à jour de la documentation. A ce titre, un guide des bonnes pratiques de l'hébergement peut être élaboré et diffusé. Les collectivités veillent à ce que les infrastructures, les installations ainsi que les dispositifs de sécurité soient régulièrement passés en revue. Il est souligné la nécessite de vérifier que les hébergeurs se conforment aux obligations du RGPD.

Gestion des infrastructures et des installations

L'hébergeur doit tenir à jour les contrats de maintenance des infrastructures transverses du site.

Le planning de maintenance doit permettre d'identifier les logiciels ou matériels obsolètes, ainsi que les actions de résorption de cette « dette » technique.

Il contribue aussi à s'assurer que le site informatique possède des infrastructures transverses sous contrat de maintenance : ce planning doit être affiché, communiqué aux intervenants, avec suivi et comptes rendus archivés.

La connaissance de la disponibilité électrique par salle permet en outre d'anticiper les limites des salles informatiques.

L'hébergeur vérifie annuellement les installations afin de s'assurer de leur bon fonctionnement et de la conformité à la législation. Il veille en outre à ce que l'organisation soit conforme aux besoins.

Lorsqu'un plan de reprise ou de continuité d'activité est nécessaire, celui-ci nécessite le déploiement d'applications sur deux sites distants sécurisés et interconnectés.

Gestion de la sécurité

La sécurisation de la salle d'hébergement correspond à un ensemble de normes à respecter afin que sa validation soit obtenue. Elle regroupe tout ce qui est obligatoire en matière de sécurité : contrôle de l'accès physique au local, respect des mesures anti-incendies, suivi des préconisations en climatisation, ventilation du local, maîtrise des gestes de proximité, etc.

Un contrôle de supervision portant sur la gestion de la sécurité est mis en œuvre. Il vise à s'assurer que les éléments de sécurité (détection incendie, climatisation) sont opérationnels et que la documentation est à jour.

Restriction des accès physiques

L'accès aux infrastructures et installations informatiques participe à la sécurité du lieu. Des modalités spécifiques devront être mises en œuvre en cas de besoin d'une zone à haute sécurité.

Des dispositifs de contrôle d'accès (système de badgeage, registre des entrées et sorties) sont utilisés pour restreindre l'accès physique aux installations hébergeant les applications clés.

Il est préconisé d'utiliser des registres dématérialisés facilitant l'utilisation, le contrôle et l'exercice des droits d'accès et de rectification. En effet, le système de badgeage doit conserver les logs d'accès afin de pouvoir procéder à une extraction des entrées et sorties. Le système doit également disposer d'une copie / sauvegarde non raccordée au réseau afin de se prémunir contre des attaques. Dans le cas contraire, un formulaire d'accès ou un registre papier des entrées et sorties est à jour et consultable.

Les formulaires de demandes d'attribution d'accès (y compris pour les prestataires) sont soumis par les responsables informatiques à la DSI. Celle-ci valide la liste des personnes autorisées à accéder aux infrastructures et installations informatiques, ainsi que les droits différenciés (par exemple en cas de zone de haute sécurité). Ces formulaires doivent, autant que possible, être dématérialisés.

Une revue des accès aux infrastructures et installations informatiques doit être mise en œuvre chaque année. Elle vise à contrôler que :

- les droits d'accès correspondent aux responsabilités assignées ;
- les personnes ayant eu effectivement accès aux infrastructures et installations informatiques disposent bien d'une autorisation d'accès validée par la DSI ;
- les personnes disposant d'un accès permanent ont signé les consignes de sécurité ;
- les personnes (y compris prestataires sous contrat) disposant d'un accès font toujours partie du personnel.

En cas d'anomalie, les corrections nécessaires (ex : modification/suppression des droits) sont effectuées dans des délais raisonnables et immédiatement lorsqu'elles concernent la zone de hauté sécurité.

Les comptes-rendus des revues périodiques des droits d'accès sont archivés dans une zone sécurisée.

2.2.2. Définir des paramètres généraux de sécurité

Mécanismes d'authentification

L'authentification de l'intervenant permet de confirmer son identité. Cette authentification est matérialisée par la saisie d'un mot de passe ou via un support matériel privatif (ex : carte à puce, clé USB). Les options de connexion anonyme au SI doivent être désactivées et la déconnexion du SI doit être automatique en cas d'inactivité prolongée.

- Gestion des mots de passe :

Pour la première connexion, un mot de passe temporaire doit être systématiquement envoyé avec obligation d'en changer.

Des règles de syntaxe des mots de passe doivent être imposées : longueur minimale (8 caractères recommandés), obligation de recourir à des caractères alphanumériques et/ou caractères spéciaux.

Une modification régulière du mot de passe doit être imposée (durée de vie maximale de 90 jours recommandée). En cas de compromission (divulgation à tort), le mot de passe doit pouvoir être modifié à l'initiative de l'utilisateur.

Afin que l'utilisateur ne puisse pas reprendre un mot de passe déjà utilisé, une historisation des derniers mots de passe est mise en œuvre dans le SI (historisation des 12 derniers mots de passe recommandée).

Le SI doit prévoir un nombre maximal de tentatives infructueuses de connexion avant blocage du compte (3 tentatives maximum recommandées). La réouverture de l'accès ne peut être réalisée que par l'administrateur.

Dans la mesure du possible, les logs de connexions infructueuses sont contrôlés et des actions sont prises afin d'en détecter les origines.

- Gestion des supports matériels privatifs (ex : carte à puce, clé USB) :

Le support (carte à puce, clé USB, etc.) est délivré nominativement à l'utilisateur, valant identifiant. La délivrance de ce support est faite par l'administrateur en contrepartie d'un reçu signé par le réceptionnaire de la carte. L'administrateur conserve la liste des titulaires de supports et les reçus. L'utilisation de ce support est personnelle. La perte (ou le vol) du support doit entraîner immédiatement une déclaration de perte à l'administrateur. Ce support peut être couplé avec un mot de passe respectant des règles de composition particulières.

Sécurité du poste de travail

Il est fondamental de mettre en place un **niveau de sécurité minimal** sur l'ensemble du parc informatique de l'entité (postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc.) :

- limitation des applications installées et modules optionnels des navigateurs web aux seuls nécessaires ;
- pare-feu local et anti-virus (ceux-ci sont parfois inclus dans le système d'exploitation) ;
- chiffrement des partitions où sont stockées les données des utilisateurs ;
- désactivation des exécutions automatiques.

Les supports amovibles peuvent être utilisés afin de propager des virus, voler des informations sensibles et stratégiques ou encore compromettre le réseau de l'entité. La politique de sécurité doit donc définir également des règles sur l'utilisation des supports physiques par les utilisateurs du SI pour échanger les données (disques externes, clés USB, graveur). L'utilisation de supports amovibles doit être limitée au strict nécessaire. Il est recommandé d'utiliser ces supports en lecture seule et de recourir à des solutions de dépollution.

Enfin, les terminaux nomades (ordinateurs portables, tablettes, etc.) sont, par nature, exposés à la perte et au vol. Ils peuvent contenir localement des informations sensibles pour l'entité et constituer un point d'entrée vers de plus amples ressources du système d'information. Des mesures spécifiques de sécurisation de ces équipements sont donc à prévoir. Il est préconisé de procéder au cryptage exhaustif des disques durs et de bloquer l'accès aux portails captifs publics depuis des équipements d'accès nomades sensibles. Toute perte ou vol de matérielle doit immédiatement être déclarée auprès des équipes de sécurité.

Charte d'utilisation du SI

Les collectivités sont invitées à élaborer une charte d'utilisation du SI, validée par la direction générale et déclinant aux utilisateurs la politique de sécurité du SI. L'adhésion à la charte est obligatoire et doit être renouvelée tous les 5 ans maximum ou en cas d'évolution substantielle de celle-ci.

Selon cette charte, les utilisateurs s'engagent à :

- ne pas divulguer leur mot de passe ;
- ne pas utiliser un mot de passe trop simple ;
- ne pas stocker leur mot de passe sur un support physique (mémo, post-it) ou numérique (fichiers de mots de passe, envoi par mail à soi-même, recours aux boutons « Se souvenir du mot de passe »). ;
- changer leur mot de passe dès qu'ils le soupçonnent d'être compromis.

Elle préconise en outre l'utilisation d'un coffre-fort numérique et le recours à des mécanismes de chiffrement. En effet, la complexité, la diversité ou encore l'utilisation peu fréquente de certains mots de passe, peuvent encourager leur stockage sur un support physique (mémo, post-it) ou numérique (fichiers de mots de passe, envoi par mail à soi-même, recours aux boutons « Se souvenir du mot de passe ») afin de pallier tout oubli ou perte.

Or, les mots de passe sont une cible privilégiée par les attaquants désireux d'accéder au système. Ils doivent donc impérativement être protégés au moyen de solutions sécurisées, au premier rang desquelles figure l'utilisation d'un coffre-fort numérique et le recours à des mécanismes de chiffrement. Dès lors, le choix d'un mot de passe pour ce coffre-fort numérique doit respecter les règles énoncées précédemment et être mémorisé par l'utilisateur, qui n'a plus que celui-ci à retenir.

La charte comprend en outre une description de la traçabilité des actions sur le SI à laquelle chaque utilisateur est assujetti.

Enfin, elle précise les sanctions applicables en cas de non-respect des règles décrites.

En complément, la collectivité met en œuvre des actions de sensibilisation relatives :

- à la gestion des mots de passe ;
- à la sécurité pour le personnel doté d'ordinateurs portables (confidentialité du travail dans les lieux publics ou moyens de transport, surveillance du matériel contre le vol, etc.) ;
- aux pratiques relatives à l'utilisation de la messagerie et d'internet.

En effet, la messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou d'un clic malencontreux sur un lien redirigeant vers un site lui-même malveillant. Les utilisateurs doivent donc être particulièrement sensibilisés à ce sujet.

Gestion des fichiers bureautiques

Les fichiers critiques pour l'établissement des résultats financiers doivent être recensés par la direction et/ou la DSI. Ces outils doivent être maîtrisés par plusieurs collaborateurs de sorte à limiter la dépendance à une seule et même personne.

Ils ne doivent pouvoir être utilisés et modifiés que par le personnel approprié. En cas de modification de fichiers bureautiques utilisés dans le cadre de l'établissement des résultats financiers, une méthodologie doit être mise en place afin de pouvoir identifier les différentes versions des documents.

Les fichiers bureautiques doivent être placés sur des serveurs afin de garantir une restriction des accès et une sauvegarde régulière.

2.2.3. Garantir la traçabilité des acteurs

Encadrée par la PSSI, la procédure de gestion des accès est formalisée et précise les modalités de création-modification-suppression des habilitations, les personnes chargées de la validation et de l'approbation de la demande, ainsi que la procédure de revue périodique des comptes.

Comptes génériques

Lorsque les habilitations ne sont pas attribuées nominativement à l'utilisateur, on parle de profil ou de compte « générique ». Dans ce cas les droits ne sont pas personnalisés et plusieurs utilisateurs partagent le même compte (ex : identifiant « admin », « user »).

Afin d'identifier les utilisateurs de manière nominative et garantir ainsi la traçabilité des acteurs, la PSSI doit limiter le recours à des comptes génériques tant dans leur nombre que dans leur diffusion.

Une revue périodique (a minima annuelle) des comptes génériques est réalisée pour s'assurer qu'ils sont limités et justifiés.

Les responsables de service doivent en outre s'assurer que les mots de passe des comptes génériques gérés par leurs services sont changés régulièrement, et à chaque mouvement de mutation, selon la fréquence et le format préconisés par la politique de sécurité. Dans le cas contraire, ils procèdent à la modification du mot de passe, le communiquent de manière sécurisée aux utilisateurs habilités à utiliser le compte générique et rappellent les impératifs de sécurité à tous les agents.

Comptes nominatifs

Parmi les comptes nominatifs, on distingue les habilitations « Administrateurs » et les habilitations « Utilisateurs ».

- Habilitations « Administrateurs » :

Seuls les administrateurs chargés de l'administration des postes doivent disposer de ces droits lors de leurs interventions.

Si une délégation de privilèges sur un poste de travail est réellement nécessaire pour répondre à un besoin ponctuel de l'utilisateur, celle-ci doit être tracée, limitée dans le temps et retirée à échéance.

Chaque administrateur doit disposer d'un compte d'administration nominatif, distinct du compte « utilisateur ». Les identifiants et secrets d'authentification doivent être différents (ex : pmartin comme identifiant « utilisateur », adm-pmartin comme identifiant « administrateur »).

Ce compte d'administration, disposant de plus de privilèges, doit être dédié exclusivement aux actions d'administration. De plus, il doit être utilisé sur des environnements dédiés à l'administration afin de ne pas laisser de traces de connexion ou de mot de passe sur un environnement plus exposé.

- Habilitations « Utilisateurs » :

Les habilitations doivent correspondre aux missions exercées par les utilisateurs et aux délégations qu'ils ont reçues.

Une revue périodique (a minima annuelle) des comptes nominatifs doit être réalisée. Un agent en charge des aspects de sécurité au sein de la DSI initie cette revue en procédant à une extraction des identifiants et de leurs droits d'accès. Le responsable de service procède à la revue et s'assure notamment :

- du respect de la procédure de validation et approbation de la demande d'habilitation ;
- de la présence effective des agents pour lesquels des comptes sont actifs : le responsable de service compare la liste des agents qui ont quitté le service avec la liste des comptes qui ont été fermés/supprimés en provenance du système. Il vérifie également le délai entre la date de départ et la fermeture des comptes.
- de l'exactitude des différentes informations liées au détenteur du compte (adresse mail, nom, prénom) ;
- de la pertinence des habilitations en fonction des missions exercées par les agents et des délégations qu'ils ont reçues ;
- du respect de la matrice des incompatibilités entre les rôles détenus par un même acteur.

Les responsables de service matérialisent leurs contrôles sur les listes transmises par la DSI en identifiant les comptes et droits d'accès injustifiés. Les responsables applicatifs effectuent dans le système les corrections nécessaires sur les droits d'accès conformément aux commentaires des responsables de service.

En cas de dérogation exceptionnelle à la matrice des incompatibilités pour nécessité de service, des contrôles doivent être mis en œuvre pour pallier les cumuls de rôles incompatibles.

Exemple : un agent est doté de rôles dans le système d'information financière de la collectivité qui sont considérés incompatibles. Le responsable de service contrôle les opérations saisies par cet agent afin de réduire les risques d'erreurs, d'irrégularités ou de fraude.

Afin d'en garantir l'indépendance, la revue périodique des comptes des agents en charge de la sécurité peut être effectuée par une entité externe.

En cas d'externalisation, la collectivité fait appel à un fournisseur de services externes pour gérer une partie des services informatiques. Les salariés en poste chez le prestataire ont accès au SI de la collectivité. En complément des vérifications qui incombent aux équipes de sécurité du prestataire, la collectivité doit donc également procéder à une revue périodique des comptes applicatifs, de base de données et d'administration du domaine détenus par le prestataire de sorte à s'assurer que :

- les comptes nominatifs correspondent à des salariés toujours en poste chez le prestataire ;
- les comptes génériques sont restreints à des exigences techniques.

Cette revue ne peut pas être déléguée au prestataire qui intervient dans le cadre de l'externalisation.

2.2.4. Garantir la traçabilité des opérations

La traçabilité des opérations peut être obtenue grâce à la mise en œuvre d'une piste d'audit qui permet de partir de l'écriture en comptabilité générale et d'arriver jusqu'à la pièce justificative du fait générateur (ex :

facture) et inversement. Elle permet de voir toutes les opérations liées à ce document présentes dans le système (ex : un bon de livraison, un bon de commande, une demande d'achat), en identifiant, tout au long du processus, l'ensemble des acteurs et des opérations intervenues.

La piste d'audit (ou chemin de révision) permet donc de :

- reconstituer dans un ordre chronologique les opérations ;
- justifier toute opération par une pièce d'origine à partir de laquelle il doit être possible de remonter par un cheminement ininterrompu au document de synthèse et réciproquement ;
- expliquer l'évolution des résultats comptables et financiers.
- garantir la disponibilité des pièces comptables et des pièces justificatives avec si nécessaire la mise en place de mesures de sauvegardes dans des zones sécurisées.

Si ces fonctionnalités présentent un intérêt évident pour les utilisateurs, elles peuvent également être mises à profit par le certificateur afin d'analyser un compte.

En effet, pour pouvoir exprimer une opinion motivée sur la fiabilité des comptes de l'entité, le certificateur collecte les éléments probants nécessaires et suffisants à cette fin. Il évalue ainsi le risque d'erreurs significatives dans les comptes.

L'absence de traçabilité des opérations et de piste d'audit est donc susceptible d'entraîner une limite générale dans l'étendue des vérifications du certificateur et une incertitude sur la fiabilité des comptes. Dès lors, toutes les opérations effectuées sur des données sensibles doivent faire l'objet d'une piste d'audit suffisante.

Lorsque les applications ne communiquent pas entre elles de façon automatique à l'aide d'interfaces :

L'action humaine est nécessaire pour la ressaisie des opérations d'une application à l'autre, créant ainsi une rupture de la piste d'audit. Les ressaisies manuelles, par nature source d'erreurs, doivent être limitées.

Pour prévenir leur survenance, des contrôles automatisés doivent être mis en place au sein du système de manière à alerter l'utilisateur et, dans certains cas, à bloquer la saisie d'écritures erronées à chaque fois que le risque le justifie.

En l'absence de contrôle automatisé dans le SI, un contrôle de supervision doit être réalisé afin de limiter le risque d'erreur. Le système d'information doit donc permettre de disposer d'états de restitution de toutes les écritures d'origine manuelle.

Lorsque le SI est intégré :

Lorsque le SI est intégré, toutes les applications communiquent entre elles de façon automatique par le biais d'interfaces. Les informations ne sont saisies qu'une seule fois dans les systèmes et les échanges de données font l'objet de contrôles d'intégrité automatiques. La piste d'audit peut donc être entièrement informatisée.

Une réconciliation des flux tels qu'ils ressortent des applications remettantes avec ceux qui figurent dans les applications destinataires doit être réalisée afin de s'assurer de l'exhaustivité et l'exactitude des informations transmises.

Cette réconciliation peut être un contrôle « intellectuel » réalisé par un opérationnel. Dans ce cas, le système doit prévoir de conserver toutes les données rejetées dans un fichier d'anomalies protégé. Les données rejetées sont éditées, analysées et corrigées (ex : recyclage du flux) dans des délais raisonnables et compatibles avec les délais de validation des traitements.

Lorsque la réconciliation est faite par le biais d'un contrôle automatisé dans le SI, un fichier retour doit être prévu de l'application destinataire vers l'application remettante. Il doit être conservé.

Enfin, un contrôle régulier de la piste d'audit doit être mis en œuvre afin d'évaluer la qualité des pistes (couverture, exploitabilité…), la sécurité des pistes et de ses constituants, les procédures de contrôle et d'archivage. Les résultats de ces contrôles doivent être notifiés et retracés.

2.3. GESTION DES ÉVOLUTIONS DU SI

Des évolutions du SI peuvent s'avérer nécessaires pour des raisons diverses : dysfonctionnement du système existant, insatisfaction des utilisateurs, montée de version de certains composants (logiciel, application, etc.), évolution réglementaire, corrections d'anomalies, etc.

La gestion des évolutions du SI constitue donc un processus central qui permet d'évaluer la façon dont les changements sont opérés, tracés et historisés.

Les évolutions peuvent être mineures et avoir un impact négligeable sur le SI. Dans cette hypothèse, la gestion peut être déléguée au support informatique (exemple : changement d'un mot de passe).

Les évolutions significatives impactent quant à elles de façon plus importante le SI et impliquent un cycle de décision spécifique et encadré avec information des directions métiers. Lorsque, de surcroît, celles-ci s'avèrent urgentes, la collectivité peut adapter sa gestion des changements afin de permettre une mise en production accélérée et contrôlée.

Les collectivités peuvent notamment mettre en œuvre deux méthodes de gestion de projet :

- la **méthode en « cascade »** ;

Cette méthode consiste à découper le projet en différentes phases et procéder étape par étape (cadrage du projet, conception générale, conception détaillée, production, tests et corrections, mise en production). Elle permet d'éviter les allers-retours, puisque chaque étape fait l'objet d'une validation avant de pouvoir passer à la suivante. Elle offre en outre une bonne visibilité sur la gestion des délais et la suite du projet.

- la **méthode « agile ».**

Cette méthode permet de mettre en œuvre une gestion de projet basée sur :

  - un fonctionnement par itérations, c'est-à-dire des cycles courts (ou très courts) durant chacun desquels une partie de l'application est développée ;
  - un processus incrémental qui permet d'enrichir l'application en lui ajoutant des nouvelles fonctionnalités à l'issu de chaque itération ;
  - une organisation collaborative : les notions de rôles et de hiérarchie sont réduites à leur strict minimum et la notions d'équipe est favorisé. Ainsi si les notions de maîtrise d'ouvrage et maîtrise d'œuvre, d'utilisateur et d'équipe chargée du développement existent toujours, ces personnes travaillent ensemble et de préférence sur un même site.

Cette méthode offre l'avantage d'une plus grande flexibilité face aux imprévus. Les livrables applicatifs issus de chaque itération devant être validés, le contrôle « qualité » est également accru. Cette méthode permet ainsi d'éviter l'accumulation des erreurs tout au long du projet.

Les éléments de contrôle interne présentés ci-après se basent sur la méthode en « cascade ». Cependant, qu'elle que soit la méthode choisie, il est rappelé que la mise en production des changements (qu'ils touchent les applications, leur paramétrage ou les éléments de l'infrastructure) doit impérativement faire l'objet d'une validation formelle avant mise en production.

2.3.1. Piloter les évolutions du SI

La procédure de gestion des changements doit être formalisée et décrit a minima :

- le dispositif de contrôle interne (couvrant les trois leviers : documentation, organisation, traçabilité) à mettre en œuvre dans le cadre de chacune des phases du cycle de changement ;
- les validations formelles intervenant dans le processus de gestion du changement.

Pour chaque projet majeur (ex : acquisition d'une nouvelle solution, évolution du SI nécessitant la migration d'une application à une autre), la collectivité définit des principes de gestion.

Ainsi, différentes instances de pilotage sont mises en place pour accompagner un projet. Elles sont généralement au nombre de trois :

- le **comité de pilotage** qui est l'instance de décision et de pilotage stratégique du projet (lancement, suivi du développement de la solution, conduite du changement et mise en œuvre, management du projet, arbitrage, allocation de ressources…) ;
- le **comité de projet** qui assure le pilotage opérationnel du projet agissant pour le compte du comité de pilotage, comprenant des représentants de la maîtrise d'œuvre (y compris prestataires) ;
- le **comité des utilisateurs**, chargé de l'expression détaillée des besoins et des règles de gestion, de la validation des dossiers de conception présentés par l'équipe projet, de la participation aux tests du système, à l'élaboration de la documentation « utilisateurs » et aux actions de formation ; de la réception définitive du logiciel.

Des réunions périodiques des instances de pilotage sont organisées afin de suivre l'avancement du projet. Elles donnent lieu à des comptes-rendus écrits, partagés avec l'ensemble des participants ainsi que la hiérarchie. Chaque instance fait l'objet d'une planification, d'un ordre du jour et d'un compte-rendu transmis aux participants. La transmission du compte-rendu doit être faite dans un délai court (inférieur à 1 semaine dans la mesure du possible).

Un outil est dédié à la traçabilité des modifications impactant le SI. Il permet de tracer les opérations effectuées, de l'initiation à la mise en production ainsi que les contrôles réalisés.

Les projets majeurs donnent lieu à un reporting (tableau de bord par exemple permettant de suivre l'évolution du périmètre, des coûts, des délais et des indicateurs).

2.3.2. Élaborer les documents de cadrage du projet

La phase préparatoire comporte différentes étapes destinées à cadrer le projet d'évolution du SI. Ces étapes permettent d'aboutir à la mise au point de documents contractuels d'engageant la maîtrise d'œuvre et la maîtrise d'ouvrage dans le lancement du projet.

Il est indispensable que les besoins en matière de contrôles automatisés dans le SI soient pris en compte à chaque étape.

Initiation de la demande de changement

La demande d'évolution du SI doit être formalisée. La collectivité est invitée à mettre en place un outil dédié à la traçabilité des modifications impactant le SI permettant :

- d'identifier les différentes demandes et assurer leur traçabilité ;
- de prioriser les demandes (ex : demande d'évolution indispensable, importante ou souhaitée, etc.) ;
- d'assurer le suivi et la communication de l'avancement aux utilisateurs.

Expression des besoins

Tout projet informatique existe pour répondre à un besoin. Il faut donc s'assurer, au-delà du respect de la méthodologie de conduite du projet, que le besoin existe, qu'il a été convenablement recueilli et exprimé, et qu'il n'est pas perdu de vue.

L'expression détaillée des besoins est formalisée dans un cahier des charges. Il préconise une solution fonctionnellement et techniquement pertinente au regard des besoins exprimés. Il prend en compte et priorise les exigences des utilisateurs, les populations ciblées, les options et principes de gestion retenus.

Étude d'opportunité

Le choix de faire évoluer le SI de manière significative doit être fait après vérification que l'optimisation des processus concernés ne suffit pas à apporter par elle-même les gains de performance attendus.

La collectivité doit donc veiller à réaliser une étude d'opportunité, formalisée dans un document comprenant :

- les objectifs du projet ;
- l'analyse des déficiences des systèmes existants ;
- les enjeux et la faisabilité du projet ;

- la compatibilité du projet avec le SI existant (intégration technique et fonctionnelle, unicité des référentiels (ex : clients, fournisseurs, etc.) de l'organisation) ;
- les bénéfices attendus et la rentabilité économique du projet ;
- les contraintes du projet.
- la liste des acteurs concernés.

Cette étude d'opportunité est revue par les directions métier et la DSI. Elle conduit à la rédaction d'une « note de cadrage », validée par le Comité de Pilotage du projet (et éventuellement les instances décisionnelles selon l'enjeu du projet). Cette note officialise l'intention de mettre en œuvre le projet ou le rejet du projet.

Étude de faisabilité du projet

L'étude de faisabilité permet d'envisager les scenarii possibles avec les bilans prévisionnels correspondants (coûts et avantages). Tous les scenarii sont envisagés, même celui de ne pas faire évoluer le SI.

Un dossier de faisabilité (ou dossier de conception générale informatique) est établi et comprend, pour chaque scenario, une description générale de la solution et une analyse :

- des différentes contraintes (besoins en matériels, en formation, en RH, contraintes juridiques, faisabilité opérationnelle, etc.) ;
- de l'impact économique (bénéfices attendus, coûts de développement, de formation, de maintenance, etc.) ;
- des risques.

Chaque scenario doit prendre en compte les besoins en matière de contrôles automatisés dans le SI.

Le dossier de faisabilité est remis au comité de pilotage afin que chaque scénario soit étudié. Ainsi, le choix de la solution est fait en toute objectivité et se fonde sur des critères d'évaluation pertinents. Le choix de la solution et la poursuite du projet sont approuvés par écrit par la personne compétente.

Étude détaillée du projet

L'étude détaillée est une analyse plus approfondie des besoins qui vise à formaliser un document contractuel entre le maître d'œuvre et le maître d'ouvrage. Elle donne lieu à la rédaction d'un cahier des charges fonctionnel (ou dossier de conception détaillée informatique) qui spécifie de façon détaillée les composants logiciels à mettre en œuvre ainsi que les interfaces. Le cahier des charges fonctionnel permet donc à la maîtrise d'ouvrage de clarifier les contraintes imposées à la maîtrise d'œuvre.

A ce stade, il convient de s'assurer qu'il existe des contrôles adaptés à chaque point critique du système (préventifs et correctifs), ainsi que des pistes d'audit permettant de suivre la totalité des transactions.

Par ailleurs, tous les acteurs concernés doivent être impliqués dans le projet (utilisateurs, administrateurs de données, responsable sécurité, etc.).

L'étude détaillée est présentée au comité de projet. La poursuite du projet est approuvée par écrit par une personne compétente.

Étude technique

L'étude technique est la phase d'adaptation de la conception à l'architecture technique retenue, tout en décrivant et documentant le fonctionnement de chaque unité du logiciel.

Le livrable de l'étude technique est le Cahier des Clauses Techniques Particulières (CCTP). L'étude détaillée peut éventuellement s'accompagner de la création d'une maquette, ou prototype, permettant aux représentants des utilisateurs de vérifier que la solution retenue répond bien à leurs attentes.

Approbation du projet

Tout projet doit donner lieu à l'élaboration d'un document d'architecture technique (DAT). Ce document définit et justifie les choix structurants du projet. Il s'articule autour de plusieurs volets :

- la présentation du projet : son calendrier, ses enjeux, ses exigences et le planning ;
- la représentation opérationnelle du projet au regard des processus métiers ;
- l'architecture fonctionnelle qui décline les besoins métiers et décrit les concepts techniques sur lesquels s'appuie l'application pour fonctionner ;
- l'architecture applicative qui décrit les éléments applicatifs, leurs fonctionnalités, ainsi que les flux échangés entre eux ;
- l'architecture technique qui correspond à l'infrastructure et l'ensemble des moyens techniques constituant le socle informatique nécessaire au support physique des applications ;
- l'analyse des risques :
- l'exploitation et sa préparation : la mise en production, le déploiement, la formation, le support et l'exploitation proprement dite.

Le DAT est présenté aux comités adéquats et validé par ceux-ci. La direction générale valide, in fine, les projets.

2.3.2. Gérer les développements, assurer la pertinence des tests et mettre en production

Les trois phases de développement, de tests, et de mise en production font l'objet d'une séparation des tâches et des fonctions. Les équipes dédiées à ces trois phases sont distinctes et les environnements correspondants sont impérativement séparés.

Développement

La phase de développement consiste à produire :

- un ensemble de codes exécutables (programmes) structuré et documenté correspondant aux spécifications et respectant les dispositions du plan d'assurance qualité ;
- les interfaces internes et externes.

Un protocole de test doit être élaboré et faire l'objet d'une mise à jour continue.

Les développements ou solutions progicielles mises en œuvre font l'objet d'une documentation qui sera tenue à jour lors des évolutions futures de l'organisation ou des solutions.

Tests

Toute application informatique doit être testée, selon un protocole formalisé, avant de passer en production. Les tests sont dans un premier temps réalisés par la maîtrise d'œuvre, puis par la maîtrise d'ouvrage.

La maîtrise d'œuvre s'assure que chacun des composants de l'application fonctionne conformément au dossier de spécifications et réalise des tests unitaires sur l'ensemble des composants de l'application et des tests d'intégration sur les interfaces de l'application dans le SI.

Les développements font ensuite l'objet d'un test par les acteurs métiers (comité utilisateurs). Cette phase de test, également appelée « phase de recette », vise à vérifier que les développements réalisés par le service « Études » sont conformes aux attentes des utilisateurs. Une validation par la maîtrise d'œuvre et la maîtrise d'ouvrage est nécessaire pour valider la recette.

Les outils de tests automatisés doivent être privilégiés afin de permettre une intégration continue.

Les anomalies bloquantes détectées à l'issue des tests doivent donner lieu aux corrections appropriées et la phase de test doit être validée par les responsables appropriés avant la mise en production.

Les services métiers assument la responsabilité de l'acceptation temporaire ou non des anomalies non bloquantes.

Homologation et mise en production

La mise en production consiste à installer et déployer la solution recettée. Chaque mise en production fait l'objet :

- d'une demande préalable de mise en production formalisée ;
- d'un compte rendu d'intervention ;
- d'un plan de retour arrière en cas d'anomalie majeure lors de la mise en production.

Ces documents doivent être archivés afin d'assurer la traçabilité des évolutions apportées au SI.

Une validation par la maîtrise d'œuvre et la maîtrise d'ouvrage est nécessaire pour confirmer la mise en production.

Il est en outre préconisé, voire obligatoire[18], de mettre en œuvre une procédure d'homologation[19] avant la mise en production de l'application. Cette décision constitue un acte formel par lequel le responsable de l'organisation :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- accepte les risques qui demeurent, appelés « risques résiduels ».

Accompagnement du changement

La politique de changement, notamment lorsqu'elle s'attache à l'évolution des solutions existantes (ex : nouvelles fonctionnalités…), précise les actions de communication à destination des utilisateurs ainsi que les actions de formation entreprises.

Ainsi, il convient de s'assurer que les doctrines d'emploi et les guides utilisateurs sont mis à jour et diffusés. Les formations dispensées doivent être en adéquation avec les évolutions ayant impacté le SI.

Suivi et maintien des conditions de sécurité

À la suite de la mise en production, il est indispensable de veiller au maintien du niveau de sécurité du système. Les anomalies rencontrées par les utilisateurs après la mise en production doivent être prises en compte et traitées.

L'homologation doit faire l'objet d'une révision périodique afin de s'assurer que les conditions de l'homologation sont respectées dans le temps. À ce titre, une veille technologique doit permettre d'identifier les vulnérabilités du système et de s'assurer qu'elles sont corrigées. Lorsqu'une vulnérabilité sérieuse est détectée, il est préconisé de relancer le processus d'homologation sans attendre l'issue de la durée d'homologation en cours.

2.3.3. Gérer les opérations de migration

L'acquisition ou le changement d'un logiciel ou d'une application peut nécessiter une migration des données avant la mise en production afin de transférer les données de l'ancien système, dit « source », vers le nouveau système, dit « cible ».

Quelle que soit la méthodologie de reprise des données retenue, un certain nombre de bonnes pratiques doit être respecté :

- **analyser les données sources et cibles** ;

Le diagnostic des données sources consiste à analyser l'homogénéité et la qualité des données et leur valeur dans l'organisation (s'agit-il de données stratégiques ?)

Il s'agit ensuite de comprendre le fonctionnement et l'organisation des données dans le système cible, pour ensuite identifier dans la source les données qui permettront de les alimenter.

18. *La réglementation rend obligatoire l'homologation pour les systèmes d'information traitant d'informations classifiées de défense (IGI 1300) et ceux permettant des échanges entre une autorité administrative et les usagers, ou entre autorités administratives (RGS).*

19. *« L'homologation de sécurité en neuf étapes simples », préconisée par l'ANSSI.*

- **définir une stratégie de migration et une méthodologie de reprise des données** ;

La stratégie de reprise vise à faire un arbitrage entre les données du système source qui devront être migrées, celles qui devront être corrigées avant la migration et celles qui seront ignorées et non reprises dans le système cible (de qualité insuffisante, par exemple). La migration peut également concerner les algorithmes, les scripts et les outils. Une démarche spécifique de gestion du changement doit être prévue pour ces éléments.

Cette stratégie de reprise permet de se prémunir des risques de dysfonctionnement, de retard, de dépassement de budget, voire d'échec du projet. Elle doit être documentée et adaptée aux besoins et exigences de la collectivité.

La méthodologie de reprise vise quant à elle à détailler les modalités de reprise des données. Pour des applications complexes, il est recommandé d'opter pour une migration par lots.

- **nettoyer les données existantes** ;

Cette étape est indispensable pour fiabiliser les données existantes dans le système source avant leur reprise dans le système cible. Ces opérations de fiabilisation devront être documentées et tracées.

- **sauvegarder les données sources** ;

La sauvegarde des données de l'ancien système est indispensable pour conserver un historique des données intact. Cette sauvegarde doit être sécurisée sur un site distant et doit pouvoir être réutilisée dans l'ancien système. La conservation de données brutes sous format standard (exemple csv ou xml) peut également permettre une reprise sur un autre système si nécessaire.

- **établir les règles de transcodification des données** ;

Ces règles permettent de connaître la valeur d'une donnée dans le système source, et sa valeur correspondante dans le système cible. Il s'agit plus communément d'établir une table de correspondances entre le système source et le système cible et les règles de transformation des données, indispensables pour la migration.

- **procéder à des tests pré-migration** ;

Un plan de test pré-migration doit être mis en œuvre. Il prévoit les tests à blanc qui seront réalisés avant la migration afin de se prémunir contre le risque d'échec de la migration des données.

Ces tests sont réalisés sur un échantillon de données représentatif. Les tests simulent des choix et permettent d'analyser les conséquences sur les données. Ces tests doivent être tracés et validés.

- **suivre et corriger les anomalies rencontrées** ;

Les tests peuvent révéler certaines anomalies qui nécessiteront des traitements automatisés pour convertir, corriger les données identifiées comme problématiques.

Exemple : suppression des valeurs anormales (données obsolètes, inutilisées et des doublons), correction de format (date…), passage d'une information d'un champ à un autre, fusion de champs, intervention sur erreurs répétées de saisie, etc.

Tous ces traitements doivent être documentés et vérifiés. Si les méthodes évoluent, la documentation relative à la méthodologie de reprise des données devra être mise à jour.

- **reprendre les données** ;

Les migrations (applicatives et systèmes) font l'objet d'une demande formelle de mise en production validée par la DSI ainsi que par les directions métiers afin de valider les résultats de la migration et tenir compte des impacts potentiels en cas d'indisponibilité ou de corruption de données.

Une fois la reprise achevée, la DSI procède à des contrôles afin de s'assurer de l'intégrité et de l'exhaustivité des données reprises. Des contrôles détaillés doivent également être réalisés par les acteurs métiers suite à la reprise des données. Ces contrôles doivent être traçables.

Les opérations de bascule et de reprise des données donnent lieu à une validation formelle par la DSI et les directions métiers. En cas de difficultés majeures lors de la reprise, le plan de retour arrière doit être mis en œuvre.

2.4. GESTION DE L'EXPLOITATION DU SI

2.4.1. Mettre en œuvre des procédures appropriées de sauvegarde et de restauration

La sauvegarde des données informatiques a pour objectif de les sécuriser et d'en permettre la restauration en cas de détérioration.

La politique de sauvegarde et de restauration des données doit être formalisée afin de s'assurer que les données, les programmes et les environnements qui sont nécessaires à la constitution de l'information financière peuvent être récupérés. Elle est validée par la DSI et les directions métiers.

La politique de sauvegarde doit être adaptée à la sensibilité des données.

Le système d'information comprend deux types de données :

1. les données structurées ;

   Dans le cas d'une sauvegarde portant sur des données structurées (ex : base de données d'une application), les informations sauvegardées sont organisées et formatées. La pérennité des sauvegardes inclut cependant la nécessité de pouvoir lire leurs supports. Une version appropriée de l'application, sur un support adapté, doit donc être conservée afin de permettre cette lecture.

2. les données non structurées.

   Les données non structurées sont une désignation générique qui regroupe les serveurs de fichiers, les fichiers bureautiques, les images, les fichiers audio, la messagerie, etc.

   Dans le cas d'une sauvegarde portant sur ce type de données la structure des fichiers sauvegardés n'est ni organisée, ni formatée. La structure des fichiers sauvegardés doit donc être décrite afin de permettre, le cas échéant, de restaurer, individuellement ou en groupe, les fichiers voulus.

Un contrôle de supervision portant sur la procédure de sauvegarde est mis en œuvre afin de veiller au respect :

- de la **fréquence de réalisation des sauvegardes** ;

Les rotations et fréquences de sauvegardes dépendent des risques identifiés par la DSI et de l'analyse d'impact d'une perte des données. Elles doivent cependant être réalisées a minima quotidiennement.

- du **correct recensement des supports de sauvegarde ;**

Les sauvegardes de données sont faites sur des supports comme des bandes magnétiques de sauvegarde, ou des disques durs. Un listing des supports doit être tenu à jour afin d'en connaître le contenu.

- de la **rotation des supports de sauvegarde** ;

Les supports sont distincts pour chaque jour de la semaine et doivent être régulièrement prélevés afin de permettre une rétention des données en phase avec les besoins métiers.

- des **modalités de stockage des supports de sauvegarde** ;

Le stockage doit être fait dans des conditions permettant de prévenir les dommages physiques des supports.

Les supports doivent être entreposés dans un endroit différent du bâtiment où sont situées les installations informatiques. Cet endroit doit répondre aux mêmes critères de protection et contraintes de sécurité que le site de production. En effet, le niveau de protection des sauvegardes doit être au moins identique à celui des éléments sauvegardés. L'accès aux supports de sauvegarde doit être sécurisé afin de garantir la sécurité de l'information financière.

- du **contenu des sauvegardes** ;

Les sauvegardes doivent contenir l'intégralité des données. Périodiquement ou a minima à chaque modification, les fichiers systèmes et les systèmes d'exploitation doivent également être sauvegardés.

- du **remplacement des bandes**.

En cas de stockage des sauvegardes sur des bandes magnétiques, le remplacement des bandes doit être fait conformément aux recommandations du constructeur (basé sur la moyenne des temps entre 2 pannes) et a minima tous les ans.

- des **modalités d'externalisation** ;

Selon une périodicité à définir par la collectivité, les supports de sauvegarde peuvent être externalisés. L'externalisation des sauvegardes auprès d'un tiers peut également être envisagée.

Dans ces hypothèses, il convient de s'assurer que les dispositifs de continuité et de sécurité mis en œuvre par le prestataire, sont conformes aux attentes de la collectivité, aux bonnes pratiques et au droit (ex : RGPD).

Enfin, des **tests des procédures de restauration** sont mis en œuvre périodiquement, et a minima annuellement, afin d'identifier l'ensemble des anomalies de restauration de sauvegardes. Ils sont validés par des représentants « Métiers » afin de s'assurer de l'efficacité du processus de restauration et de la qualité des supports de sauvegarde.

2.4.2. Contrôler les traitements automatisés

Ce contrôle consiste à s'assurer de l'exactitude, l'exhaustivité et la rapidité des traitements automatisés (batch, interface…) qui concourent à la constitution de l'information financière.

Les traitements automatisés couvrent notamment :

- les batchs informatiques : séquence de traitement automatique, également appelée « traitement par lots », généralement réalisée en temps différé ;
- les traitements transactionnels qui visent à réaliser des tâches informatisées de manière unitaire.

Au regard des nombreux batchs et traitements unitaires qui peuvent composer le SI d'une collectivité, ce point de contrôle constitue un enjeu majeur. Il est donc indispensable que des contrôles quotidiens soient prévus, réalisés et tracés.

2.4.3. Traiter les incidents

Procédure de gestion des incidents

La procédure de gestion des incidents doit être formalisée. Elle définit :

- **les acteurs** :

Tout incident de sécurité doit être signalé. Le service en charge de l'exploitation centralise et traite les incidents constatés ou remontés par les utilisateurs (ou provenant d'autres sources comme les prestataires, les partenaires).

Pour ce faire, le RSSI doit sensibiliser les utilisateurs et plus généralement l'ensemble des personnes intervenant sur le SI de la structure à la détection des incidents liés au SI. Cette sensibilisation peut être effectuée de manière présentielle mais également via des solutions dématérialisées (masterclass, support de présentation, FAQ, tutoriel, etc.).

- **les outils** ;

Il est préconisé d'utiliser un outil dédié à la gestion des incidents. Cet outil permet aux utilisateurs de faire remonter les incidents qu'ils rencontrent par le biais d'un « ticket d'incident ».

Pour chaque incident, une fiche de suivi doit systématiquement être ouverte. Elle comporte a minima les éléments suivants : la date de survenance, la date de réparation, la dénomination des intervenants, le type de procédure d'alerte, la description de la solution, le statut de la fiche (diagnostic en cours, réparation en cours, pièce en commande, clos…), les conséquences.

- **les indices de criticité** ;

Les incidents touchant le SI peuvent être classés en fonction d'indices de criticité basés sur la probabilité de survenance de l'incident et ses impacts (ressources impactées, étendue du périmètre, durée estimée de

l'incident). Ces indices permettent de déterminer si un incident est considéré comme mineur, moyen ou majeur.

Tout incident de sécurité détecté doit faire l'objet d'une analyse et d'une qualification en terme de criticité par le RSSI.

- **les modalités de traitement des incidents** ;

Dans le cadre du traitement des incidents de sécurité, doivent être identifiées :

- les mesures conservatoires permettant d'isoler la menace, de réduire le périmètre de l'incident, de conserver des preuves (copies des serveurs, conservation des journaux et logs) ;
- les mesures correctives permettant d'éradiquer la menace ;
- ayant des impacts significatifs sur les processus métiers de la collectivité ;
- les mesures curatives permettant le retour à la normale pour les SI endommagés suite à un incident.

Quelle que soit la nature de l'incident, il convient de détailler toutes les actions entreprises pour tenter de le résoudre (documents, copies écran, etc.). Cette documentation de l'incident permet, en cas de transfert du cas, de ne pas répéter des actions déjà entreprises et donc de ne pas perdre de temps dans la résolution du problème.

- **les dispositifs d'escalade** ;

En fonction de la complexité ou de l'impact de l'incident une escalade doit être envisagée.

Le dispositif d'escalade peut être :

- fonctionnel : ce dispositif est prévu dans le processus de gestion des incidents et consiste en un transfert de l'incident au niveau supérieur (en raison du manque d'expertise du niveau en cours, par exemple) ;
- hiérarchique : à n'importe quel moment dans le cycle de gestion de l'incident afin d'alerter la hiérarchie et transférer la responsabilité des décisions.

De manière générale, il est préconisé d'informer, dans les plus brefs délais, le RSSI de tout incident de sécurité :

- ayant une origine malveillante ;
- ayant des impacts significatifs sur les processus métiers de la collectivité ;
- générant un risque financier, juridique ou médiatique important ;
- sans impact significatif, mais récurrent.

Le RSSI informe sans délai la direction de tout incident grave de sécurité qui jugera de la nécessité d'engager des poursuites judiciaires (dépôt de plainte).

- **les modalités de signalement des incidents graves.**

Les vulnérabilités ou failles de sécurité d'un système d'information peuvent être signalés à l'Autorité Nationale de Sécurité des Systèmes d'Information (ANSSI)[20].

En cas de cybermalveillance, les collectivités victimes peuvent s'appuyer sur la plateforme[21] développée par le Groupement d'Intérêt Public « Action contre la Cybermalveillance » (GIP ACYMA), qui leur propose un accompagnement : établissement d'un diagnostic de la situation, diffusion de conseils pratiques et mise en relation avec des spécialistes et organismes compétents.

Les collectivités territoriales sont en outre tenues de notifier les incidents portant sur des traitements de données à caractère personnel à la Commission Nationale de l'Informatique (CNIL)[22]. Ce signalement doit être fait dans les meilleurs délais et, si possible, 72 h au plus tard après en avoir pris connaissance.

Externalisation de la gestion des incidents

La collectivité peut avoir recours à la tierce maintenance applicative (TMA) : la collectivité confie la gestion du système d'information à un prestataire informatique tiers dans le cadre d'un contrat pluriannuel.

20. *Article L2321-4 du Code de la Défense*.
21. *Assistance de la plateforme Cybermalveillance.gouv.fr*.
22. *Notifier une violation de données personnelles à la CNIL*.

La mission du prestataire en charge de la TMA est de s'assurer du bon fonctionnement du logiciel, notamment de la correction des erreurs remontées par les utilisateurs, mais aussi des mises à jour nécessaires à l'optimisation d'utilisation du logiciel.

Pour chaque activité externalisée, la collectivité conclut avec le prestataire un contrat. La traçabilité des opérations réalisées par le prestataire est assurée par l'utilisation de comptes nominatifs.

Les prestataires doivent s'engager à respecter les obligations de confidentialité qui incombent à l'ensemble des acteurs de la sphère publique.

La collectivité doit vérifier le niveau de service délivré par le prestataire au regard des conditions contractuelles.

Revue de la gestion des incidents

Des contrôles de supervision doivent être réalisés régulièrement et formalisés par la DSI.

Il s'agit de s'assurer que la procédure de gestion des incidents est respectée. Sur la base d'un échantillon d'incidents clos, il convient de vérifier que :

- l'incident a fait l'objet d'une fiche de suivi dûment renseignée dans l'outil dédié ;
- l'incident a fait l'objet d'un diagnostic pour identifier les failles du système ayant permis l'incident ;
- le cas échéant, les mesures d'isolement du ou des ordinateurs incidentés ont été prises ;
- l'incident est documenté de toutes les actions entreprises pour le résoudre ;
- les délais de résolution de l'incident sont raisonnables ;
- des rappels de bonnes pratiques ont été faits ou des nouvelles consignes ont été données aux utilisateurs à l'issue de la crise.

La DSI réalise également une revue régulière (a minima 1 fois par an) des incidents au statut « non résolu » et prend les mesures nécessaires pour solutionner les points de blocage.

2.5. PLANS DE CONTINUITÉ ET DE REPRISE D'ACTIVITÉ

Les plans de continuité et de reprise d'activité dépassent le champ des systèmes d'information. Ils sont un dispositif clé qui conditionne la capacité de la collectivité à agir en situation de crise interne ou externe.

Un **Plan de Continuité d'Activité (PCA)** comprend un ensemble de mesures et des moyens humains, techniques et logistiques qui permettraient à une organisation de poursuivre son activité **pendant un sinistre**. Ainsi, l'activité de la collectivité ne cesse pas. Une priorisation des activités est appliquée afin d'identifier celles indispensables à la continuité du fonctionnement de la collectivité. D'autres peuvent en revanche être interrompues temporairement, pour des mesures sanitaires et/ou de protection individuelle.

Un **Plan de Reprise d'Activité** (PRA) regroupe quant à lui un ensemble de mesures qui permet à une organisation de reprendre son activité **après un sinistre**.

Sur le volet SI et en amont de l'élaboration de ces deux plans, un travail de fond est à réaliser avec les services concernés et la DSI au cours duquel seront déterminées :

- la durée maximale d'interruption admissible[23] : il s'agit d'évaluer à partir de combien de temps l'interruption du système informatique serait problématique pour l'activité de la collectivité. Cette durée d'interruption peut être distincte suivant les différentes applications pour distinguer celles qui sont utiles, nécessaires et critiques.
- la perte de données maximale admissible[24] : il s'agit d'évaluer la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne.

23. *Traduction de « RTO » ou « Recovery Time Objective ».*

24. *Traduction de « RPO » ou « Recovery Point Objective ».*

Les PCA et PRA auront ensuite pour but de prévoir les systèmes de sécurité et les processus d'intervention précis ayant vocation à maintenir les éventuelles interruptions d'activité en dessous de cette durée et à permettre de conserver et restituer les données au redémarrage de la solution de secours.

En cas de survenance d'un sinistre, l'efficacité et la rapidité de réaction des équipes d'intervention et le retour à une situation d'équilibre dépendent de la qualité des plans de continuité et de reprise d'activité. Ceux-ci doivent être :

- opérationnels en détaillant les procédures adaptées au type de sinistre ;
- exhaustifs en recensant et organisant toutes les actions à entreprendre ;
- applicables et évolutifs : les PCA et PRA doivent être tenus à jour et font l'objet d'une mise à jour formelle 1 fois par an. Ils sont validés par des tests qui, seuls, permettent de mesurer en grandeur réelle la pérennité de l'adéquation de la solution de secours aux objectifs de continuité et de reprise d'activité. Ces tests font systématiquement l'objet d'un retour d'expérience en présence des DSI et des directions métiers. Les actions à mettre en œuvre, identifiées à l'issue des tests, sont recensées dans un plan d'amélioration. Leur réalisation est tracée et archivée.

ANNEXES : FICHES RELATIVES AU CONTRÔLE INTERNE DES SI

FICHE 1 : DOCUMENTATION GÉNÉRALE DU SI

FICHE 2 : SÉCURITÉ PHYSIQUE DU SI

FICHE 3 : RESTRICTION DES ACCÈS PHYSIQUES

FICHE 4 : MÉCANISMES D'AUTHENTIFICATION

FICHE 5 : SÉCURISATION DU POSTE DE TRAVAIL

FICHE 6 : GESTION DES FICHIERS BUREAUTIQUES

FICHE 7 : GESTION DES HABILITATIONS

FICHE 8 : REVUE DES HABILITATIONS

FICHE 9 : TRAÇABILITÉ DES OPÉRATIONS

FICHE 10 : GESTION DES PROJETS

FICHE 11 : DÉVELOPPEMENTS, TESTS ET PRODUCTION

FICHE 12 : OPÉRATIONS DE MIGRATION

FICHE 13 : REVUE DES TRAITEMENTS AUTOMATISÉS

FICHE 14 : PROCÉDURES DE SAUVEGARDE ET DE RESTAURATION

FICHE 15 : GESTION DES INCIDENTS

FICHE 16 : PLAN DE REPRISE D'ACTIVITÉ