ANNEXES : FICHES RELATIVES AU CONTRÔLE INTERNE DES SI

Les fiches présentées dans les onglets de ce tableur constituent des annexes au guide méthodologique du contrôle interne des systèmes d'information des collectivités locales.

Les mesures de contrôle interne présentées dans ces fiches constituent une base mise à la disposition des responsables des différentes structures.
Il leur appartient, compte-tenu de la situation de chaque entité, de son organisation et de ses moyens :
- 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 la situation de l'entité et de ses moyens.

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

FICHE 1 : DOCUMENTATION GÉNÉRALE DU SI

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Inadéquation du SI avec la stratégie de la collectivité et les besoins des utilisateurs.	Absence de schéma directeur Absence de gouvernance informatique Absence de documentation Mauvais archivage de la documentation	**Budgétaire :** coûts liés aux projets informatiques en échec **Organisationnel :** désorganisation de la fonction SI, perte de productivité des utilisateurs en raison du manque de performance du SI
(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)		

OBJECTIF

S'assurer que la collectivité dispose de l'ensemble de la documentation nécessaire à la prise de connaissance du SI.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Un schéma directeur est élaboré afin de définir la stratégie du SI. Celle-ci est en conformité avec les grandes orientations stratégiques de la direction générale de la collectivité et des métiers.
Il fait l'objet d'une planification pluriannuelle, réajustée en fonction du contexte de la collectivité ou des contraintes réglementaires.

Une liste des projets en cours ou à venir est établie. La gestion des changements (évolutions fonctionnelles du SI, évolutions applicatives et logicielles, mise à jour de l'infrastructure, gestion de l'obsolescence technologique) est alignée sur le schéma directeur.

Un Organigramme fonctionnel nominatif de la DSI est élaboré et régulièrement mis à jour (a minima 1 fois par an). Il permet d'identifier les liens fonctionnels, organisationnels et hiérarchiques de la fonction informatique au sein de la collectivité. L'organigramme est adapté à la gestion de projets selon la méthode agile.

Une matrice d'incompatibilité est conçue afin de s'assurer du non cumul de fonction incompatibles. Les incompatibilités identifiées sont transposées en rôles dans le SI et paramétrées dans le SI (via un système de gestion des habilitations).

Une cartographie applicative est disponible et représente 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...).

Existence d'un tableau de synthèse à jour décrivant :
- les principales applications financières et métiers.
- les principales interfaces entre les principales applications du SI.
- les principaux contrats conclus par la DSI (niveaux SLA, OLA, ...) ou ayant un impact direct sur la disponibilité des systèmes d'informations (contrats de maintenance, contrats de service...).

Existence d'un document, à jour, synthétisant les effectifs internes et externes agissant pour le compte de la DSI.

Des documents d'architecture, doctrines d'emploi et des guides utilisateurs sont élaborés pour chaque application.

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 ». Elle est mise à jour périodiquement et a minima 1 fois par an.

PLAN D'ACTION DE LA COLLECTIVITÉ

Schéma directeur	*Insérer la référence des documents ici*
Liste des Projets en cours ou à venir	
Organigramme fonctionnel nominatif de la DSI	
Matrice d'incompatibilité	
Cartographie applicative	
Tableau de synthèse des applications dûment complété	
Tableau de synthèse des principales interfaces dûment complété	
Tableau de synthèse des principaux contrats dûment complété	
Tableau de synthèse des effectifs internes et externes	
Documents d'architecture, doctrines d'emploi et des guides utilisateurs	
Liste des comptes existants	

FICHE 2 : SÉCURITÉ PHYSIQUE DU SI

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Carence dans la mise en œuvre des dispositifs de sécurité physique du SI	Survenance d'un incident sur le site d'hébergement Méconnaissance des normes relatives à l'environnement matériel du SI (évacuation, incendie, accès, sauvegarde, etc.) Absence de contrat de maintenance des matériels informatiques.	**Sécurité des biens et des personnes :** incendie, inondation, mise en danger des personnels **Budgétaire :** coût lié à la détérioration du matériel **Organisationnel :** lenteur, surcharge ou indisponibilité totale ou partielle du réseau **Juridique :** responsabilité de la collectivité en matière de sécurité des SI et de protection des données personnelles **Comptable et financier :** altération des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que des dispositifs de sécurité adéquats sont mis en place pour les sites d'hébergement informatique.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Un guide des bonnes pratiques de l'hébergement est élaboré et diffusé.
La documentation d'installation des infrastructures du site (schéma des installations, descriptif fonctionnel des équipements, inventaire, etc.) est tenue à jour.

Levier « organisation »

Une structure dédiée à la gestion de la sécurité est mise en place : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité.

Un contrôle de supervision annuel portant sur la gestion des infrastructures transverses du site (contrats de maintenance, planning de maintenance, connaissance de la disponibilité électrique salle par salle) est mis en œuvre.

Un contrôle de supervision annuel relatif à la gestion des installations est mis en œuvre. Il vise à s'assurer du bon fonctionnement des installations et de leur conformité à la législation. Il veille en outre à ce que l'organisation soit conforme aux besoins.

Des contrôles de supervision relatifs à la gestion de la sécurité sont mis en œuvre pour s'assurer que les éléments de sécurité (détection incendie, climatisation) sont opérationnels et que la documentation est à jour.

Des audits de sécurité du SI sont réalisés à intervalles réguliers. Bien qu'ils ciblent en priorité les applications critiques du système d'information, l'ensemble des applications font l'objet d'audits réguliers en vue de leur homologation.

Levier « traçabilité »

Les listes sont tenues à jour :
- interlocuteurs internes et externes du site, afin de faciliter la recherche d'interlocuteurs en cas d'incident ;
- personnes disposant d'un accès permanent au site ;
- personnes ayant signé les consignes de sécurité, à rapprocher de la liste des personnes disposant d'un accès permanent au site.

Le planning de maintenance est affiché, communiqué aux intervenants, avec suivi et comptes rendus archivés. Il doit permettre d'identifier les logiciels ou matériels obsolètes, ainsi que les actions de résorption de cette dette technique.

L'historique des accès ponctuels de personnes est rapproché du planning annuel de maintenance et de l'historique des entrées et sorties de matériel.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 3 : RESTRICTION DES ACCÈS PHYSIQUES

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Carence dans la mise en œuvre des dispositifs de sécurité physique du SI	Accès aux infrastructures et installations informatiques par une personne non autorisée Attribution d'un accès à tort Maintien d'un droit d'accès non justifié Dysfonctionnement du dispositif de contrôle des accès	**Sécurité des biens et des personnes :** intrusion dans le réseau, perte ou vol de données **Budgétaire :** coût lié à la détérioration du matériel **Juridique :** responsabilité de la collectivité en matière de sécurité des SI et de protection des données personnelles **Comptable et financier :** altération des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que l'accès aux infrastructures et installations informatiques est limité aux personnes autorisées et que des dispositifs de sécurité adéquats sont mis en place.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La gestion des droits d'accès aux infrastructures et installations informatiques est encadrée par la Politique de Sécurité des SI (PSSI).

Les consignes de sécurité sont formalisées dans un document signé par les personnes disposant d'un droit d'accès permanent.

Levier « organisation »

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

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).

En cas de départ d'un agent, les accès sont supprimés dans les plus brefs délais.

Une revue périodique des droits d'accès aux infrastructures et installations informatiques est mise en œuvre (a minima 1 fois par an).

En cas d'anomalie constatée lors de la revue périodique des droits d'accès, les corrections nécessaires (ex : modification/suppression des droits) sont effectuées dans des délais raisonnables.

Levier « traçabilité »

Le système de badgeage conserve les logs d'accès afin de pouvoir procéder à une extraction des entrées et sorties. Dans le cas contraire, un formulaire d'accès ou un registre papier des entrées et sorties est à jour et consultable. Le système dispose d'une copie / sauvegarde non raccordée au réseau afin de se prémunir contre des attaques.

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

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 4 : MÉCANISMES D'AUTHENTIFICATION

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Accès aux données et aux applications par des personnes non autorisées	Absence de Politique de Sécurité des SI Non respect des règles de sécurisation des mots de passe. Communication par un utilisateur de son mot de passe à un tiers.	**Sécurité des biens et des personnes :** intrusion dans le réseau, perte ou vol de données **Budgétaire :** fraude **Juridique :** responsabilité de la collectivité en matière de sécurité des SI et de protection des données personnelles **Organisationnel :** lenteur, surcharge ou indisponibilité totale ou partielle du réseau **Comptable et financier :** altération des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que :
- les principales applications financières et « métiers » du SI mettent en œuvre un mécanisme d'authentification permettant de sécuriser l'accès au SI ;
- les paramètres de gestion des mots de passe applicatifs sont configurés en accord avec la politique de sécurité de l'établissement et les meilleures pratiques.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Les mécanismes d'authentification à l'ensemble des applications clés du SI, permettant l'identification de l'utilisateur, sont documentés et encadrés par la Politique de Sécurité du SI (PSSI) :
- sécurisation des mots de passe ;
- renouvellement des mots de passe ;
- etc.

Une procédure de revue de la gestion des mots de passe est documentée et testée périodiquement.

Levier « organisation »

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

Des règles de syntaxe des mots de passe (longueur minimale, caractères alphanumériques et spéciaux) et un renouvellement régulier sont imposés.

Des actions de sensibilisation ou de rappel sur la gestion des mots de passe sont mises en œuvre au sein de la collectivité.

Un contrôle de la conformité du paramétrage des mots de passe à la politique de sécurité est mis en œuvre au sein de la collectivité. Ce contrôle est documenté.

Les logs de connexions infructueuses sont contrôlés et des actions sont menées afin d'en détecter les origines.

Levier « traçabilité »

La collectivité est en capacité de faire une extraction du système du paramétrage des contraintes de mot de passe.

La revue est traçable : elle est formalisée sur une grille de contrôle, laquelle est archivée.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 5 : SÉCURISATION DU POSTE DE TRAVAIL

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Acte malveillant par intrusion sur le SI de la collectivité	Infection virale ou lancement de programmes malveillants sur le poste de travail Rançongiciel Absence de solution de cryptage pour les postes nomades	**Sécurité des biens et des personnes :** intrusion dans le réseau, perte ou vol de données **Budgétaire :** fraude **Organisationnel :** indisponibilité du SI **Juridique :** non respect de la réglementation relative à la sécurité du SI et à la protection des données **Comptable et financier :** altération des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer qu'un niveau minimal de sécurité est requis sur chaque poste de travail.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La politique de sécurité détaille les modalités et procédures mises en œuvre pour assurer un niveau de sécurité minimal sur l'ensemble du parc informatique de l'entité.

La politique de sécurité fixe les règles relatives à l'utilisation des supports physiques par les utilisateurs du SI pour échanger les données (disques externes, clés USB, graveur).

Une charte d'utilisation du SI établie par la DSI et validée par la direction générale de la collectivité, décline aux utilisateurs la politique de sécurité du SI.

Levier « organisation »

Des actions de sensibilisation aux pratiques relatives à l'utilisation de la messagerie et d'internet sont réalisées.

Des mesures spécifiques de sécurisation des équipements nomades (ordinateurs portables, tablettes, etc.) sont mises en œuvre (ex : crytage exhaustif du disque dur).

Levier « traçabilité »

La charte d'utilisation des SI est signée par les utilisateurs. Elle doit être renouvelée tous les 5 ans.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 6 : GESTION DES FICHIERS BUREAUTIQUES

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Carence dans la conservation des données informatiques	Absence de contrôle des accès aux fichiers Modification non autorisée des fichiers Perte de données suite à la défaillance des postes informatiques (données irrécupérables) Le développement et l'exploitation des fichiers bureautiques critiques sont maîtrisés par une seule personne Difficultés de maintenance et d'évolution des outils	**Organisationnel** : défaillance ou indisponibilité des outils **Comptable et financier :** défaillance ou indisponibilité des outils et/ou des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que la gestion des fichiers bureautiques garantit la disponibilité des données concourant à la production des états financiers.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La collectivité liste les fichiers bureautiques critiques impactant les états financiers.

Le développement et l'exploitation des fichiers bureautiques critiques sont documentés.

Levier « organisation »

Les fichiers bureautiques critiques sont stockés sur des serveurs afin de garantir :
- une restriction appropriée des accès ;
- une sauvegarde régulière.

Le développement et l'exploitation des fichiers bureautiques critiques sont maîtrisés par un nombre suffisant de collaborateurs (au moins deux quelque soit le fichier).

Levier « traçabilité »

Une méthodologie de gestion de versions est mise en place afin de pouvoir tracer les modifications. Celle-ci doit s'appuyer, autant que possible, sur des outils numériques de gestion documentaire.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 7 : GESTION DES HABILITATIONS

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Accès aux données et aux applications par des personnes non autorisées	Les droits sont attribués en méconnaissance des délégations de signature Un utilisateur dispose de droits étendus injustifiés au regard de ses fonctions	**Budgétaire : fraude** **Comptable et financier :** incertitudes quant à la fiabilité des données concourant à la production des états financiers
Absence de traçabilité des acteurs	Généralisation des profils génériques.	**Comptable et financier :** incertitudes quant à la fiabilité des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que les processus de gestion des utilisateurs des applications, bases de données et systèmes d'exploitation sont encadrés par une procédure formalisée.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Les comptes génériques et nominatifs (utilisateurs et administrateurs) sont créés sur la base d'autorisations décrites dans des procédures formalisées.

Une liste des comptes existants pour les accès aux 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 ».

Levier « organisation »

Les comptes génériques sont limités au strict nécessaire. Leur utilisation doit être surveillée spécifiquement. Le mot de passe associé doit être renouvelé périodiquement (a minima 1 fois par an).

Les comptes administrateurs sont limités à un nombre restreint d'agents et autant que possible réservés aux agents internes.

Chaque administrateur dispose d'un compte d'administration nominatif, distinct du compte « utilisateur ». Ce compte d'administration est utilisé exclusivement pour des actions d'administration, dans des environnements dédiés à l'administration. A contrario, ils utilisent leur compte « utilisateur » pour les actions qui ne relèvent pas de l'administration.

Les habilitations correspondent aux missions exercées par les acteurs et aux délégations qu'ils ont reçues.

Les habilitations respectent la matrice des incompatibilités de rôles détenus pas un même acteur.

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.

Levier « traçabilité »

Les demandes de création/modification/suppression de compte sont tracées (ex : formulaires).

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 8 : REVUE DES HABILITATIONS

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
Accès aux données et aux applications par des personnes non autorisées	Absence de revue des habilitations Absence de correction des anomalies détectées lors de la revue des habilitations	**Budgétaire :** fraude **Comptable et financier :** incertitudes quant à la fiabilité des données concourant à la production des états financiers
Erreurs, Irrégularités ou fraude	Dérogation exceptionnelle à la matrice des incompatibilités non suivie de contrôles	**Comptable et financier :** incertitudes quant à la fiabilité des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que les accès aux applications, bases de données et systèmes d'exploitation clés sont régulièrement revus.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Une procédure de revue périodique des comptes génériques est réalisée pour s'assurer que ces comptes sont limités et justifiés.

Une procédure de revue périodique (a minima 1 fois par an) des comptes nominatifs (administrateurs, utilisateurs) est documentée. Elle vise à s'assurer :
- du respect de la procédure de validation et approbation de la demande d'habilitation ;
- du rattachement effectif à la structure des agents pour lesquels des comptes sont actifs ;
- de l'exactitude des différentes informations liées à l'agent;
- de la pertinence des habilitations en fonction des missions exercées par les acteurs et des délégations qu'ils ont reçues ;
- du respect de la matrice des incompatibilités entre les rôles détenus pas un même acteur.

Levier « organisation »

La revue des comptes génériques comptes nominatifs est formalisée a minima annuellement.

Un agent en charge des aspects de sécurité au sein de la DSI initie la revue en procédant à une extraction des comptes génériques et nominatifs et de leurs droits d'accès. Sur la base du fichier transmis par la DSI, le responsable de service procède à la revue périodique des comptes. Il annote le fichier en identifiant les comptes et droits d'accès injustifiés. 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.

Les anomalies détectées ont été corrigées dans un délai raisonnable (ex : dans la semaine suivant la revue).

Un contrôle de supervision est réalisé afin de s'assurer que les corrections nécessaires ont été effectuées dans des délais raisonnables et qu'elles ont été documentées et archivées.

En cas d'externalisation, la collectivité procède 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 sont justifiés et 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

Levier « traçabilité »

La revue est traçable : le contrôle est formalisé (le responsable de service annote le fichier en identifiant les comptes et droits d'accès injustifiés) et archivé.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 9 : TRAÇABILITÉ DES OPÉRATIONS

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
Absence de traçabilité des opérations	Multiplication des saisies manuelles Absence de piste d'audit Piste d'audit insuffisante/incomplète Absence de documentation des paramétrages et contrôles existants (manuels ou automatisés).	**Comptable et financier :** incertitudes quant à la fiabilité des données concourant à la production des états financiers, limites générales dans l'étendue des vérifications du certificateur

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que :
- les saisies manuelles sont limitées et auditables ;
- toutes les opérations effectuées sur des données sensibles font l'objet d'une piste d'audit suffisante.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Des guides de procédures sont rédigés, notamment pour les opérations sensibles donnant lieu à saisie manuelle.

Levier « organisation »

Les saisies manuelles sont limitées. Des contrôle automatisés sont mis en place au sein du SI de manière à alerter l'utilisateur ou bloquer la saisie d'écritures erronées. En l'absence de contrôle automatisé, un contrôle de supervision est réalisé afin de limiter le risque d'erreur.

Des interfaces sont mises en œuvre dans le SI pour les processus comportant des opérations sensibles afin de limiter les ruptures de la piste d'audit.

Une réconciliation des flux entre les applications remettantes et destinataires est réalisé.

Un contrôle de la piste d'audit est mis en œuvre afin d'évaluer la qualité des pistes (couverture, exploitabilité…), la sécurité des pistes et de ses constituants.

Levier « traçabilité »

Les saisies manuelles sont auditables : le SI permet l'édition d'états de restitution de toutes les écritures d'origine manuelle. Cette information est portée à la connaissance de l'agent avant la saisie.

Les contrôles sont traçables :
- lorsque le contrôle de réconciliation des flux est automatisé, un fichier retour doit être prévu de l'application destinataire vers l'application remettante. Il doit être conservé.
- lorsque les contrôles ne sont pas automatisés, ils sont formalisés sur des grilles de contrôle, lesquelles sont archivées.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 10 : GESTION DES PROJETS

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
Inadéquation du SI avec la stratégie de l'entité et les besoins des utilisateurs	Les études préalables (opportunité, faisabilité, etc.) n'ont pas été validées formellement Utilisateurs métiers non associés aux projets informatiques Besoins en matière de contrôle automatisés dans le SI non pris en compte	**Budgétaire :** coûts liés aux projets informatiques en échec **Organisationnel :** désorganisation de la fonction SI, perte de productivité des utilisateurs en raison du manque de performance du SI **Comptable et financier :** incertitudes quant à la fiabilité des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer de l'adéquation du projet aux besoins des utilisateurs et à la stratégie de la collectivité.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La procédure de gestion des changements est formalisée et décrit a minima le dispositif de contrôle interne à mettre en œuvre dans le cadre de chacune des phases du cycle de changement et les validations formelles intervenant dans le processus de gestion du changement.

L'expression des besoins est formalisée dans un cahier des charges détaillé (solution retenue au regard des besoins exprimés, exigences utilisateurs, populations ciblées, options et principes de gestion retenus, etc.).

Pour chaque projet majeur, une étude d'opportunité, une étude de faisabilité, une étude détaillée et une étude technique sont réalisées.

Chaque projet doit faire l'objet d'un document d'architecture technique présenté aux comités adéquats et validé par ceux-ci. La direction générale valide, in fine, les projets.

Les principes de gestion de chaque projet sont définis (gouvernance, planning, phases de tests, mise en production, suivi du projet et formalisation, indicateurs de suivi).

Levier « organisation »

Des instances de pilotage sont mises en place pour accompagner chaque projet (comité de pilotage, comité de projet, comité utilisateurs).

Les besoins en matière de contrôles automatisés dans le SI sont pris en compte à chaque étape du projet.

Des réunions périodiques des instances de pilotage sont organisées afin de suivre l'avancement du projet. La périodicité des instances est fixée dès le lancement du projet et peut être adaptée par la suite.

Une procédure d'homologation, adaptée aux enjeux de sécurité du système, est mise en œuvre avant la mise en production.

La mise en production est systématiquement validée la maîtrise d'œuvre et la maîtrise d'ouvrage.

Levier « traçabilité »

La poursuite du projet est, à chaque étape, approuvée par écrit par une personne compétente.

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.

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).

Les projets sont suivis et donnent lieu à un reporting (ex : tableau de bord permettant de suivre l'évolution du périmètre, des coûts, des délais et des indicateurs).

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 11 : DÉVELOPPEMENTS, TESTS ET PRODUCTION

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
SI non pérenne	Erreurs dans la programmation Tests réalisés de manière parcellaire Absence de traçabilité des évolutions mises en production Absence de séparation des fonctions et des environnements	**Budgétaire :** coûts liés aux projets informatiques en échec **Organisationnel :** indisponibilité totale ou partielle du réseau **Juridique :** responsabilité de la collectivité en matière de sécurité des SI et de protection des données personnelles **Comptable et financier :** altération des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer les développements s'inscrivent dans le cadre de la stratégie de la collectivité et répondent aux besoins des utilisateurs.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La procédure de gestion des changements est formalisée et décrit a minima le dispositif de contrôle interne à mettre en œuvre dans le cadre de chacune des phases du cycle de changement et les validations formelles intervenant dans le processus.

Les changements significatifs donnent lieu à la mise à jour des documentations du SI (documentations techniques, doctrine d'emploi, guide utilisateurs, etc.).

Les protocoles de test sont documentés pour chaque développement.

Levier « organisation »

Les environnements et les fonctions de développement, de tests et de production sont séparés. L'accès aux mises en production est suffisamment restreint.

Des tests sont réalisés pour chaque développement ou changement conformément aux protocoles de tests documentés.
La maitrise d'œuvre réalise des tests unitaires et d'intégration afin de s'assurer que les développements répondent aux spécifications du projet.
Des tests sont réalisés par les utilisateurs afin de s'assurer que les développements répondent à leurs attentes.

Ils sont systématiquement mis en œuvre lors des phases de tests et doivent s'intégrer autant que possible dans un dispositif d'intégration continue.

Les anomalies bloquantes identifiées font l'objet de corrections appropriées avant la mise en production des changements.

Levier « traçabilité »

Les résultats des tests font l'objet de remontées aux directions métiers et informatiques (en vue notamment d'une prise en compte dans les prochaines itérations).

La phase de test est validée par les responsables appropriés avant la mise en production. Les services métiers assument la responsabilité liée à la gestion des risques (acceptation temporaire ou non des anomalies non bloquantes).

Chaque mise en production fait l'objet :
- d'une fiche de test validée (par les services informatiques et métiers pour les parties qui leur incombent) ;
- 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 pour tracer les évolutions impactant le SI.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 12 : OPÉRATIONS DE MIGRATION

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
Carence des données reprises dans le nouveau système	Absence de fiabilisation des données sources avant migration Règles de transcodification non documentées Absence de test pré-migration Absence de contrôle post-migration	**Budgétaire :** coût lié à un retour en arrière **Comptable et financier :** perte ou altération des données, incertitudes quant à la fiabilité, l'exactitude et/ou l'exhaustivité des données constituant l'information financière

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que la gestion des opérations de migrations garantit l'intégrité et l'exhaustivité des données reprises.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Une stratégie de migration et une méthodologie de reprise des données sont définies et documentées.
Elle tient compte des adaptations logicielles, matérielles et techniques (scripts et outils notamment) à réaliser dans le cadre des migrations.

Les règles de transcodification des données et les modalités d'adaptation des logiciels, matériels et techniques sont documentées et mises à jour.

Un plan de test pré-migration est défini et validé par les services informatiques et métiers.

Un plan de retour arrière est élaboré pour être mis en œuvre en cas d'anomalie majeure suite à la reprise des données.

Levier « organisation »

Les données sources font l'objet d'un diagnostic afin d'analyser leur homogénéité, leur qualité, et leur valeur informationnelle.

Les données sources font l'objet d'une opération de fiabilisation avant migration. Les opérations de fiabilisation sont documentées et tracées.

Les données sources sont sauvegardées avant la migration.

Des tests pré-migration « à blanc » sont réalisés et traçés. Les anomalies rencontrées sont tracées et corrigées dans des délais raisonnables. Pour des applications complexes, il est recommandé de procéder à un allotissement des migrations.

Levier « traçabilité »

Les migrations (applicatives et systèmes) font l'objet d'une demande formelle de mise en production validée par la DSI et les directions métiers.

Après reprise, 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 validation formelle par la DSI et les directions métiers. Les migrations en environnement de production sont automatiquement tracées et revues.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 13 : REVUE DES TRAITEMENTS AUTOMATISÉS

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
Carence dans la conservation des données informatiques	Dysfonctionnement d'un traitement automatisé (batch, interface, sauvegarde…) non détecté Absence de contrôle régulier des Interfaces Absence de personne responsable du traitement des anomalies	**Comptable et financier :** incertitudes quant à la l'exactitude et/ou l'exhaustivité de l'information financière

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

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

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La procédure de gestion des traitements automatisés est formalisée et mise à jour régulièrement. Elle est communiquée et partagée avec la Direction et les acteurs métiers.

La liste des personnes disposant d'un accès aux programmateurs de travaux est revue a minima annuellement par la DSI.

Les modalités de corrections des incidents de traitements sont documentées.

Levier « organisation »

L'exécution des traitements automatiques (batch, interface, sauvegarde…) est contrôlée quotidiennement, par exemple sur la base de comptes-rendus d'exécution générés par le système.

Un contrôle de supervision régulier (a minima 1 fois par an) est réalisé par la DSI afin d'analyser les incidents de traitements automatisé non résolus.

Levier « traçabilité »

La possibilité de modifier le programmateur des traitements automatisés fait l'objet d'une autorisation formelle.

Les incidents de traitements automatisés sont tracés via l'outil de suivi des incidents. Ils sont analysés par le service en charge de l'exploitation et corrigés. Les corrections sont conservées pendant 3 ans.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 14 : PROCÉDURES DE SAUVEGARDE ET DE RESTAURATION

EXEMPLE DE RISQUE	EXEMPLE DE FACTEUR DÉCLENCHANT	EXEMPLE D'IMPACT
Carence dans la conservation des données informatiques	Absence de sauvegarde ou sauvegarde incomplète Échec de la procédure de restauration	**Organisationnel** : altération des données, incapacité de la collectivité à restaurer le SI en cas d'incident **Comptable et financier :** altération ou indisponibilité des données nécessaires à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

Sécuriser les données, les programmes et les environnements nécessaires à la production des états financiers afin d'en permettre la restauration en cas de détérioration.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La politique de sauvegarde et de restauration des données est formalisée et validée par la DSI et les directions métiers.

Dans le cas d'une sauvegarde portant sur des données non structurées (serveurs de fichier, fichiers bureautiques, images, fichiers audio, messagerie, etc.) la structure des fichiers sauvegardés est décrite afin de permettre, le cas échéant, de restaurer, individuellement ou en groupe, les fichiers voulus.

Levier « organisation »

Dans le cas d'une sauvegarde portant sur des données structurées (ex : base de donnée d'une application), une version appropriée de l'application, sur un support adapté, est conservée afin de permettre la lecture de la sauvegarde. Ce support doit être conservé sur un sité sécurisé distinct du site de production de l'application (protection incendie, innondation, ...).

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 ;
- du correct recensement des supports de sauvegarde ;
- de la rotation des supports de sauvegarde ;
- des modalités de stockage des supports de sauvegarde ;
- du contenu des sauvegardes ;
- du remplacement des bandes ;
- des modalités d'externalisation.

Les procédures de sauvegarde et de restauration sont testées a minima annuellement sur un périmètre représentatif.

Levier « traçabilité »

Les tests des procédures de sauvegarde et de restauration sont validés par des représentants « Métiers ».

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 15 : GESTION DES INCIDENTS

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Indisponibilité du système informatique	Signalement d'incident non pris en compte Incidents non résolus ou résolus dans des délais excessifs Actions entreprises non documentées	**Sécurité des biens et des personnes :** intrusion dans le réseau, perte ou vol de données, mise en danger des personnels **Organisationnel :** perte d'image de la DSI, perte de productivité des utilisateurs **Budgétaire :** coûts liés à la répétition des incidents ou aux incidents en chaîne **Comptable et financier :** incident générant une altération des données concourant à la production des états financiers

(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)

OBJECTIF

S'assurer que les incidents susceptibles d'avoir une incidence sur le processus de génération de l'information financière sont identifiés et résolus dans un délai raisonnable.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

Une procédure de gestion des incidents est définie et formalisée. Elle définit les moyens de suivi (acteurs, outils), les indicateurs de criticité ainsi que les dispositifs d'escalade.

Levier « organisation »

Le RSSI sensibilise, en présentiel ou via des solutions dématérialisées, les utilisateurs et l'ensemble des personnes intervenant sur le SI à la détection des incidents liés au SI.

Un outil dédié à la gestion des incidents permettant aux utilisateurs de faire remonter les incidents qu'ils rencontrent.

Tout incident de sécurité fait l'objet d'une analyse et d'une qualification en termes de criticité par le RSSI.

Un dispositif d'escalade fonctionnel et hiérarchique est prévu. Ce dispositif est formalisé et connu de l'ensemble des acteurs.

Les incidents graves sont signalés aux autorités compétentes (ANSSI, CNIL, plateforme cybermalveillance.gouv.fr).

Des revues sont réalisées régulièrement par la DSI. Elles portent sur :
- la gestion des incidents (fiche de suivi, diagnostic, mesures d'isolement prises, documentation des actions entreprises, délais de résolution, rappels de bonnes pratiques aux utilisateurs) ;
- les incidents non résolus.

En cas d'externalisation de la gestion des incidents, la collectivité s'assure du niveau de service délivré par le prestataire au regard des conditions contractuelles.

Levier « traçabilité »

Une fiche de suivi est systématiquement ouverte pour chaque incident.

Toutes les actions entreprises pour tenter de résoudre l'incident (documents, copies écran, etc.) sont documentées et archivées.

La revue est traçable : le contrôle est formalisé et archivé.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)

FICHE 16 : PLAN DE REPRISE D'ACTIVITÉ

EXEMPLE DE RISQUE	EXEMPLE DE FACTEURS DÉCLENCHANTS	EXEMPLE D'IMPACTS
Incapacité de la collectivité à redémarrer le SI	Absence de PCA / PRA Le périmètre du PCA / PRA ne couvre pas les applications critiques au regard de la production de l'information financière Le PCA / PRA existe mais n'est pas testé ou est testé sans le concours des utilisateurs Indisponibilité du SIH suite à la survenance d'un sinistre majeur relatif à un problème physique, logique ou humain Absence de documentation d'un mode de fonctionnement dégradé.	**Sécurité des biens et des personnes :** perte ou vol de données, mise en danger des personnels **Budgétaire :** coûts liés au sinistre **Organisationnel :** indisponibilité du SI **Juridique :** non respect de la réglementation en matière de sécurité des SI, de protection des données personnelles **Comptable et financier :** indisponibilité des données nécessaires à la production des états financiers
(Ces éléments non exhaustifs peuvent être complétés des risques et facteurs de risque propres à la collectivité)		

OBJECTIF

S'assurer qu'un Plan de continuité (PCA) et de Reprise d'activité (PRA) sont élaborés, régulièrement testés et mis à jour.

EXEMPLE DE BONNES PRATIQUES

Levier « documentation »

La collectivité a élaboré un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA). Ils détaillent les procédures adaptées au type de sinistre et recensent toutes les actions à entreprendre.

Levier « organisation »

Pour l'élaboration des PCA et PRA, la durée maximale d'interruption admissible du SI et la perte de données maximale admissible dans le SI ont été déterminées préalablement.

Des tests sont régulièrement mis en œuvre afin de mesurer l'adéquation des solutions de secours aux objectifs de continuité et de reprise d'activité. Ils font systématiquement l'objet d'un retour d'expérience en présence des DSI et des directions métiers.

Les PCA et PRA sont tenus à jour et font l'objet d'une mise à jour formelle 1 fois par an.

Levier « traçabilité »

Les actions à mettre en œuvre, identifiées à l'issue des tests, sont recensées dans un plan d'amélioration avec une priorisation des actions à effectuer. Leur réalisation est tracée et archivée.

PLAN D'ACTION DE LA COLLECTIVITÉ

(Compléter des actions mises en œuvre ou devant être mises en œuvre par la collectivité)