

Cour des comptes



Chambres régionales
& territoriales des comptes

GUIDE MÉTHODOLOGIQUE

AUDIT DES SYSTEMES D'INFORMATION

OCTOBRE 2020

Centre d'appui métier

Dernière mise à jour : Octobre 2020

SOMMAIRE

FICHE 1 – LA GOUVERNANCE INFORMATIQUE	7
Axe 1 – Evaluer la strategie d’evolution du systeme d’information	8
Axe 2 – Analyser la pertinence de la comitologie et des outils de pilotage	10
Axe 3 – Analyser l’organisation et les ressources de la fonction informatique	12
Axe 4 – Evaluer le contrôle interne relatif au systeme d’information	14
Axe 5 – S’assurer de la maitrise du budget informatique.....	16
FICHE 2 – L’ENVIRONNEMENT INFORMATIQUE	18
Axe 1 – Evaluer la formalisation des connaissances du SI	19
Axe 2 – Verifier les interactions entre les éléments du SI	21
Axe 3- Analyser la maitrise du parc informatique.....	23
Axe 4 – Evaluer l’urbanisation du SI	25
Axe 5 – Evaluer la maitrise de l’informatique en nuage (cloud ^{GI})	27
FICHE 3 – L’EVOLUTION DU SYSTEME D’INFORMATION	29
Axe 1 – Evaluer le maintien en condition opérationnelle des applications informatiques	31
Axe 2 – Evaluer le pilotage et l’organisation des projets d’évolution	33
Axe 3 – Contrôler les projets innovants	37
FICHE 4 – LA PRODUCTION INFORMATIQUE	39
Axe 1 – Vérifier les objectifs de la production et le suivi de la performance	40
Axe 2 – Contrôler L’organisation mise en place autour de la fonction de production	42
Axe 3 – Evaluer les procédures de gestion de l’exploitation et le dispositif de gestion des incidents... ..	44
Axe 4 – Contrôler les mesures prises pour assurer la continuité de l’activité	46
FICHE 5 – LES DONNEES	49
Axe 1 – Evaluer la maitrise de la classification de la donnée.....	50
Axe 2 – S’assurer de la qualité des données	52
Axe 3 – Evaluer la disponibilité de la donnée.....	53
Axe 4 – Vérifier la sécurisation des traitements de données	55
FICHE 6 – LA SECURITE DU SYSTEME D’INFORMATION	57
Axe 1 – Contrôler le contenu de la politique de sécurité des SI et la conformité au RGS	58
Axe 2 – S’assurer de la sécurité physique du matériel informatique	61
Axe 3 – Evaluer les dispositifs de sécurité logique.....	63
Axe 4 – Vérifier la mise en œuvre régulière des audits de sécurité	65
Axe 5 – S’assurer de la prise en compte des questions et enjeux de la cyber sécurité	66
Axe 6 - S’assurer de la conformité aux exigences d’un OIV et d’un OSE	67

FICHE 7 - LA SECURISATION DES DONNEES PERSONNELLES – CONTROLER LA CONFORMITE D'UNE ENTITE AUX DISPOSITIONS DU RGPD	68
Axe 1- Le respect des obligations incombant à l'entité contrôlée au titre du RGPD	73
Axe 2- La sensibilité de l'organisme aux questions de protection des données personnelles	75
LISTE DES ANNEXES	78
Annexe 1 - La transformation numérique de l'ETAT	78
Annexe 2 - Les acteurs du SI	80
Annexe 3- Environnement informatique	81
Annexe 4- Les méthodologies de projet	82
Annexe 5- Schéma d'un projet informatique	86
Annexe 6- L'Archivage des données	87
Annexe 7 - Bonnes pratiques sur les mots de passe	92
Annexe 8 - Les formations	93
Annexe 9 - Références	95

INTRODUCTION

POURQUOI S'INTERESSER A L'AUDIT DES SYSTEMES D'INFORMATION ?

La transformation numérique est une réalité et un enjeu majeur pour l'économie française et pour son administration.

La multiplication de l'utilisation des technologies numériques transforme le fonctionnement de l'administration et la relation à l'utilisateur notamment par la généralisation des services en ligne et des téléprocédures mais aussi au regard de l'optimisation de l'analyse des données de masse et de l'utilisation de l'intelligence artificielle.

De nombreux chantiers ont été déployés au niveau des administrations publiques pour :

- Faciliter le déploiement de l'administration électronique.
- Développer l'accessibilité de l'administration au travers d'axes tels que l'inclusion numérique et la simplification.
- Améliorer les conditions de travail des agents grâce aux outils numériques.
- Améliorer l'efficacité des politiques publiques.

[L'annexe 1](#) présente en détail ces dispositions.

Le cadre législatif s'est aussi adapté afin d'accompagner ces changements notamment avec la Loi pour une République Numérique (2016) et le Règlement Général sur la Protection des Données (RGPD - 2018). Ce dernier induit de nouvelles obligations pour l'ensemble des acteurs publics et privés.

Ainsi, les systèmes d'information (SI) deviennent à la fois plus centraux et critiques dans le fonctionnement des organismes contrôlés que ce soit dans :

- La relation avec l'utilisateur : les services rendus aux usagers par la fonction publique se présentent de plus en plus sous un format numérique.
- Les mécanismes de gestion interne : la numérisation des outils modifie les modalités de vérification du contrôle interne.
- Les supports d'échange, de traitement et de conservation des données : les données contrôlées sont sauvegardées et manipulées dans des systèmes d'information. Ces données transitent d'un système à l'autre et sont archivées sur des supports numériques.

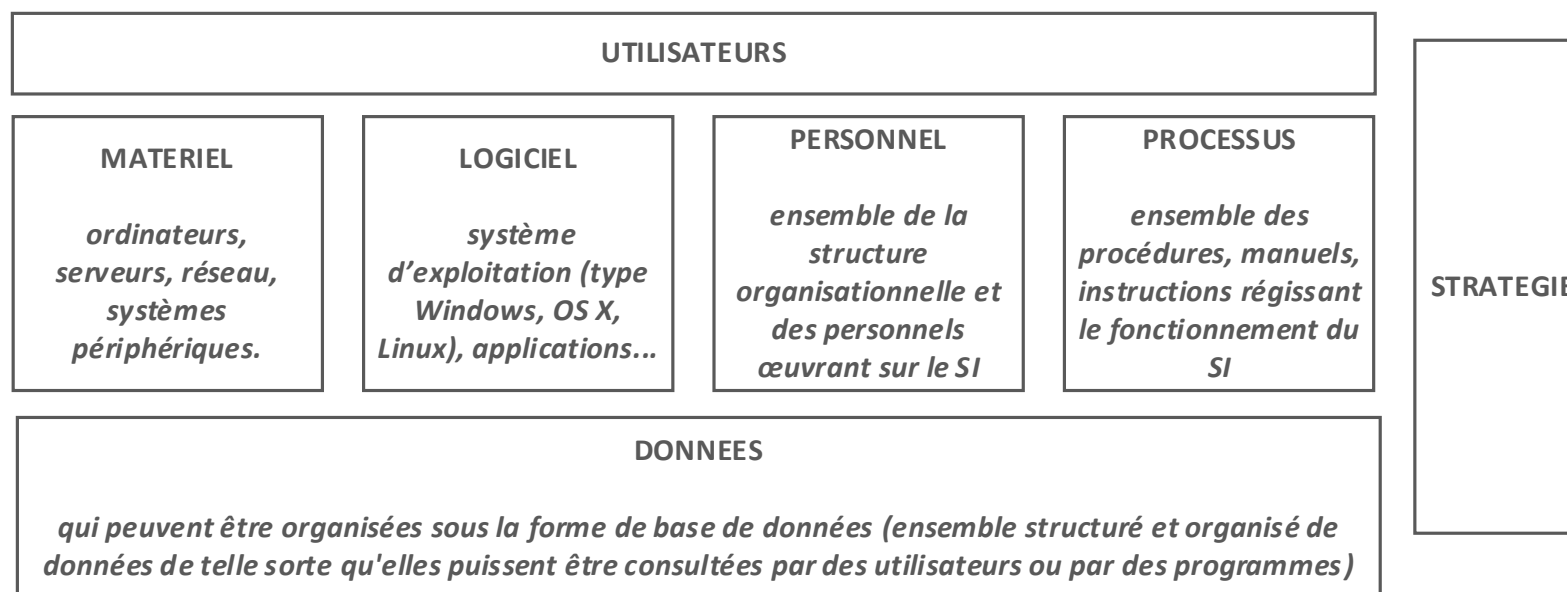
Pour les juridictions financières, cela implique :

- De nouveaux risques liés aux systèmes d'information ou aux changements induits par les nouveaux objets numériques.
- De nouveaux interlocuteurs par exemple les responsables de la production ou de la sécurité informatique, fonctions qui sont parfois externalisées.
- De nouvelles modalités de contrôle avec notamment l'automatisation d'une partie des contrôles embarqués dans les téléprocédures par exemple.

QU'EST CE QUE LE SYSTEME D'INFORMATION (SI) ?

Un système d'information (SI) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classer, de traiter et de diffuser de l'information sur un environnement donné.

Il comprend les briques suivantes :



LES OBJECTIFS DU GUIDE D'AUDIT SI

Dans un contexte de transformation numérique et face à des systèmes d'information toujours plus complexes, le contrôle des SI devient essentiel pour apprécier le fonctionnement et la gestion d'un organisme.

De nouvelles thématiques émergentes telles que la gestion de projets innovants, la vie de la donnée et l'intelligence artificielle^{Gl} nécessitent que les équipes soient préparées et accompagnées dans leurs contrôles.

Ce guide propose une approche méthodologique commune de contrôle pouvant s'appliquer à l'ensemble des organismes contrôlés. Il a pour vocation de présenter les enjeux et les risques, les bonnes pratiques et le vocabulaire des documents à demander sur l'ensemble du système d'information.

Au regard de la complexité du sujet, ce guide n'a pas pour ambition d'être exhaustif mais vise à présenter une méthodologie permettant à toute équipe de réaliser un premier état des lieux de la fonction informatique d'un organisme et d'en identifier les risques nécessitant potentiellement un niveau de diligence supérieur.

COMMENT UTILISER CE GUIDE

La méthodologie d'audit des systèmes d'information est présentée sous la forme de fiches de contrôle organisées en sept thématiques : la gouvernance, l'environnement informatique, l'évolution du SI, la production informatique, les données, la sécurité et le RGPD.

Les questionnaires proposés sont ajustables en fonction de l'envergure de l'entité ou du contexte. Au sein de chaque fiche, les questions prioritaires sont identifiées par un surlignage (**questions**) afin de mettre en avant les points essentiels.

Les termes suivis de l'exposant «^{Gl}» renvoient au glossaire des SI disponible en ligne sur le [lien suivant](#).

EVALUER LA CRITICITE DU SI

Le niveau de maturité attendu des systèmes d'information varie d'une organisation à une autre : il peut être de niveau rudimentaire (exemple : pour une association ou une petite mairie), tout comme il peut être vital et central à l'ensemble des processus (exemple : pour un ministère). Les entités dont le niveau de criticité est le plus élevé doivent mettre en place des contrôles renforcés de leur système d'information. La profondeur de l'audit SI doit donc évoluer en fonction de différents facteurs, entre autres : la maturité de l'organisation, sa complexité et la criticité des services qu'elle délivre vis-à-vis de ses bénéficiaires, agents et partenaires.

[Un outil en ligne](#) a été mise à disposition pour aider à réaliser une première évaluation du niveau de fiabilité requis. Il permet d'évaluer la criticité du SI de l'organisme et le cas échéant le degré d'intervention préconisé (autonomie, avec un auditeur spécialisé, etc.)

FICHE 1 – LA GOUVERNANCE INFORMATIQUE

PRESENTATION

Le système d'information est plus que jamais, à l'heure de la transformation numérique, au cœur de l'activité de tous les organismes. Il n'est pas une fin en soi mais un outil indispensable pour permettre aux organisations d'atteindre leurs objectifs. Le système d'information doit être construit pour appuyer les processus métier. La gouvernance informatique doit par conséquent être de la responsabilité de la direction de l'organisme.

La gouvernance consiste à bâtir un dispositif de pilotage de la fonction informatique afin de favoriser les prises de décision en vue d'augmenter la valeur de l'organisme, de maîtriser les coûts associés, tout en minimisant les risques. La gouvernance permet aussi d'organiser et de clarifier les relations entre la direction des systèmes d'information (DSI), garante des aspects techniques de l'informatique, et le reste de l'organisme.

LES RISQUES

Les risques relatifs à la gouvernance des systèmes d'information sont de façon non exhaustive :

- Un SI inadapté aux besoins métiers.
- Un SI non conforme aux exigences réglementaires.
- Un SI non sécurisé.
- Un SI non fiable.
- Un SI non pérenne (obsolescence du SI ou perte de la maîtrise du SI en interne).
- Un dérapage des dépenses informatiques.

LES OBJECTIFS

Les objectifs de cette fiche sont de vous permettre :

- **D'évaluer la cohérence entre le stratégie d'évolution du SI et les objectifs de l'organisme (axe 1).**
- De **contrôler la pertinence de l'organisation de la fonction informatique** et le dimensionnement des ressources **(axe 2).**
- De **vérifier si la comitologie et les outils de pilotage opérationnel** de la fonction informatique sont adaptés aux enjeux et risques identifiés **(axe 3).**
- De s'assurer que les **risques liés aux systèmes d'information** sont correctement appréhendés, que les **plans d'action associés** sont pertinents et que les **dispositifs de contrôle interne** sont adaptés à l'importance croissante du SI **(axe 4).**
- **D'évaluer la maîtrise des coûts de l'informatique** qui représente généralement un poste significatif des dépenses totales des organismes **(axe 5).**

AXE 1 – EVALUER LA STRATEGIE D'EVOLUTION DU SYSTEME D'INFORMATION

Enjeux pour l'organisme

- ▶ Bâtir une stratégie pluriannuelle d'évolution du système d'information, validée au plus haut niveau de l'organisation
- ▶ Aligner la stratégie informatique avec les objectifs stratégiques de l'organisme et les obligations réglementaires
- ▶ Décliner cette stratégie en objectifs opérationnels permettant son suivi régulier, et notamment l'avancement du budget

Risques

- ▶ Un SI ne répondant pas aux besoins de l'organisme (décalage entre la stratégie d'évolution du SI et la stratégie de l'organisme)
- ▶ Un SI non conforme aux exigences réglementaires
- ▶ Un SI non pérenne (non prise en compte des risques liés à l'obsolescence du SI)
- ▶ Un SI peu ou pas sécurisé



Bonnes pratiques

La stratégie d'évolution du système d'information (définie pour 3 à 5 ans) doit être formalisée dans un document validé et signé par la direction de l'organisme, sous la forme généralement d'un Schéma Directeur Informatique^{GI} (SDI) (ou schéma directeur des systèmes d'information –SDSI-).

Le SDI doit comporter à la fois des éléments techniques propres à l'informatique comme l'architecture, le matériel, le réseau, mais également des éléments opérationnels sur les applications informatiques qui supportent l'activité de l'organisme. Il est donc fondamental que le SDI soit élaboré en collaboration avec les directions métier pour permettre à l'organisme d'atteindre ses propres objectifs stratégiques (objectifs métier, budgétaires, de performance, de qualité de service, etc.)

Le SDI doit être construit dans une logique de portefeuille de projets possédant chacun des caractéristiques spécifiques en termes notamment de budget, de délais de déploiement et de réalisation. Cette approche doit permettre de garder une nécessaire flexibilité. Des revues périodiques (le plus souvent annuelles) sont indispensables pour affiner les grands axes définis au départ.



Point d'attention

Les stratégies des entités publiques relatives à la dématérialisation des procédures doivent prendre en compte des considérations spécifiques telles que les éventuelles ruptures dans l'égalité d'accès aux services proposés et les principes de continuité et d'adaptabilité. Ainsi, une enquête sur l'accès aux droits des Français réalisée en 2017 par le Défenseur des droits faisait apparaître qu'une personne sur cinq éprouvait des difficultés face aux démarches administratives en ligne, soit parce que ces administrés ne possèdent pas d'accès internet, soit parce qu'ils maîtrisent mal cet outil. Parmi eux, se trouvent des personnes âgées mais aussi des personnes en situation de précarité ([lien vers l'enquête 2019](#)).

Questionnements

Formalisation et validation de la stratégie

- ▶ L'organisme a-t-il élaboré une stratégie d'évolution de son système d'information ?
- ▶ Est-elle formalisée et validée par la direction de l'organisme ?
- ▶ Quel a été le processus d'élaboration de cette stratégie ? Notamment quelle a été l'implication des directions métier et/ou des usagers ?
- ▶ Cette stratégie est-elle alignée sur les objectifs stratégiques de l'organisme ?
- ▶ Cette stratégie est-elle déclinée en objectifs mesurables pour en permettre un pilotage satisfaisant ?
- ▶ Cette stratégie est-elle actualisée régulièrement (environ une fois par an), afin de prendre en compte les évolutions stratégiques de l'organisation ou des événements structurants (nouvelle réglementation, retard ou abandon d'un projet, etc...)
- ▶ La stratégie informatique prend-elle en compte les obligations réglementaires (RGPD^{GI}, RGS^{GI}, RGAA^{GI}, RGI^{GI}, CNIL^{GI}, OSE^{GI}) ?

Communication de la stratégie

- ▶ Quelle communication est faite en interne sur cette stratégie pour en faciliter sa compréhension et assurer l'adhésion des métiers ?
- ▶ Cette communication est-elle régulière ?

Documents à consulter :



Schéma directeur des système d'information (SDI) ou document équivalent
Plan pluriannuel des objectifs stratégiques de l'organisme (ex : COP pour les opérateurs de l'état, COG pour les organismes de sécurité sociale)
Document actualisé de suivi du SDI

Pour aller vers l'observation

Conclure sur :

L'existence et la pertinence de la stratégie d'évolution du système d'information, validée à tous les niveaux.

La déclinaison de cette stratégie en objectifs opérationnels et mesurables afin d'en permettre leur suivi.

La communication en interne de la stratégie.



Point d'attention

Le SDI est un document clé (lors d'un audit du SI) car il contient en principe:

- la situation du SI lors de son diagnostic avec les éléments saillants (forces et faiblesses),
- la présentation des axes stratégiques d'évolution du SI,
- la trajectoire d'évolution du SI (la cible), présentant l'ordonnement des principaux projets à mettre en œuvre et énonçant les principes de gouvernance retenus pour piloter la mise en œuvre et actualiser le SDI.

Pour en savoir plus :

[Guide d'audit de la gouvernance du SI d'une entreprise numérique](#) par le CIGREF, l'AFAI et l'IFACI.

AXE 2 – ANALYSER LA PERTINENCE DE LA COMITOLOGIE ET DES OUTILS DE PILOTAGE

Enjeux pour l'organisme

- ▶ Disposer d'une comitologie efficace pour piloter la fonction informatique
- ▶ Mettre en œuvre des outils adaptés pour piloter la fonction informatique au sein de l'organisme

Risques

- ▶ Un SI ne répondant pas aux besoins de l'organisme (par exemple, si les MOA^{GI} sont faiblement impliquées dans les instances de pilotage)
- ▶ Un SI non sécurisé (si la sécurité n'est pas suivie à tous les échelons de l'organisme)



Bonnes pratiques

La comitologie mise en œuvre au sein de l'organisme doit comporter plusieurs niveaux de prise de décision:

- Un comité stratégique SI, qui se réunit au moins une fois par an et qui rassemble les principaux décideurs (direction général, directions métier et direction informatique) de l'organisme.
- Un comité de pilotage informatique (plus opérationnel que celui stratégique) qui se réunit régulièrement (généralement une fois par mois).
- Un comité sécurité (stratégique) présidé par la direction de l'organisme.

Les membres de ces comités doivent disposer d'outils appropriés pour suivre et communiquer sur l'avancement de chaque thématique, et permettre de prendre les bonnes décisions. Cela inclut les enquêtes de satisfaction des utilisateurs (qualité du service rendu, qualité des applications informatiques, etc.) qui sont des indicateurs forts de la qualité du SI.

Questionnements

Comitologie

- ▶ Quelle est la comitologie (instances de pilotage) mise en œuvre au sein de l'organisme pour piloter la fonction informatique ? Est-elle formalisée ?

- ❖ *En particulier vérifier la présence, la fréquence de réunion ainsi que la composition du :*
 - *comité informatique stratégique (vérifier la présence de la direction) ;*
 - *comité de pilotage informatique ;*
 - *comité stratégique dédié à la sécurité (Voir la [fiche 6 relative à la sécurité](#))*

Vérifier la présence des directions métiers pour ces deux derniers.

Pour aller vers l'observation

Conclure sur :

La pertinence et la représentativité des membres des différents comités informatiques pour piloter la fonction informatique.

Questionnements

- ▶ Le directeur des systèmes d'information (DSI) est-il membre du comité de direction ?
- ▶ Ces comités donnent-ils lieu systématiquement à une présentation préalable et à un compte rendu de réunion incluant des plans d'action ? Si oui, les plans d'action sont-ils suivis ?

Outils de pilotage stratégique

- ▶ Quels sont les principaux outils de pilotage de la fonction informatique (y compris les différents tableaux de bord ou autres outils de reporting) à disposition de la direction de l'organisme ?
- ▶ Quels sont les principaux indicateurs de performance ? Quelle est la fréquence de publication de ces indicateurs ? Sont-ils pertinents ?
 - ❖ Vérifier notamment la présence de :
 - reporting sur l'avancement de la mise en œuvre du SDI ;
 - tableaux de bord de suivi de la production (disponibilité des applications, taux de performance, niveau de respect des contrats de services, etc.) ;
 - reporting sur les incidents informatiques ;
 - reporting sur les projets en cours (avancement, risques, budget, etc.) ;
 - tableaux de bord de suivi de la sécurité du SI.

Enquête utilisateurs

- ▶ Des enquêtes de satisfaction sont-elles réalisées auprès des usagers ? Comment sont-elles exploitées ?

Pour aller vers l'observation



Point d'attention

Il faut s'assurer du degré d'implication de la direction générale dans le pilotage de l'informatique et des directions métier dans le suivi des applications informatiques métier (déjà en production ou en cours de développement).

Les tableaux de bord de pilotage de l'informatique doivent être diffusés et analysés régulièrement au plus niveau de la hiérarchie de l'organisme.

Conclure sur :

L'exhaustivité et l'efficacité des outils de pilotage de la fonction informatique.



Point d'attention

« 250 démarches administratives 'phares' accessibles en ligne pour les citoyens, avec un haut niveau de qualité ». C'est la promesse du Gouvernement pour 2022, rappelée lors du 3^e comité interministériel de la transformation publique (CITP), qui s'est tenu le jeudi 20 juin 2019. Pour tenir cet objectif, la direction interministérielle du numérique (DINSIC), a lancé [un observatoire de la qualité des services numériques, ainsi qu'un dispositif pour recueillir la satisfaction des usagers](#). Ces deux outils doivent permettre d'identifier les pistes d'amélioration prioritaires.

Voir également [le rapport de la Cour sur les relations aux usagers et la modernisation de l'Etat- vers une généralisation des services publics numériques \(2016\)](#) et le [RPA 2020- Tome II](#).

Documents à consulter :



Document descriptif de la gouvernance informatique

Compte-rendu des instances de gouvernance

Reportings et tableaux de bord de pilotage (suivi de la production, suivi des projets, suivi budgétaire)

Enquêtes de satisfaction des utilisateurs du SI

AXE 3 – ANALYSER L'ORGANISATION ET LES RESSOURCES DE LA FONCTION INFORMATIQUE

Enjeux pour l'organisme

- ▶ S'assurer de la cohérence de l'organisation de la fonction informatique en lien avec ses objectifs stratégiques
- ▶ S'assurer que les ressources dédiées à la fonction informatique sont correctement calibrées en volume et en qualité

Risques

- ▶ Un SI non fiable ou non adapté aux besoins métier (par exemple, en raison d'une faible implication des équipes métiers dans la phase de validation des évolutions informatiques)
- ▶ Perte de la maîtrise en interne du SI (en cas de dépendance forte avec des personnes clés ou une utilisation trop large de prestataires externes par exemple)



Bonnes pratiques

La DSI doit être rattachée à la direction générale de l'organisme.

Une séparation forte entre les équipes de production et les équipes de développement (cf. [annexe 2](#)) est indispensable pour garantir la sécurité des solutions quand elles sont mises en production.

Les MOA^{GI} jouent un rôle clé dans la fonction informatique. Elles doivent notamment :

- spécifier les besoins fonctionnels et établir un cahier des charges pour la MOE^{GI} ;
- piloter la MOE par une comitologie adaptée ;
- valider la solution de la MOE avant la mise en production.

Concernant la sécurité, il est fortement recommandé que le responsable de la sécurité du système d'information (RSSI) ne soit pas rattaché à la DSI mais au directeur de l'organisme pour assurer son indépendance et pour faciliter le reporting à sa hiérarchie.

Questionnements

Organisation de la fonction informatique

- ▶ La DSI est-elle rattachée à la direction générale de l'organisme?
- ▶ Le rôle de chaque acteur est-il formalisé? En particulier, concernant les principales applications en production et en développement, les MOE et les MOA sont-elles clairement identifiées ?
- ▶ La séparation des fonctions entre les équipes de production et les équipes développement est-elle stricte ?

(cf. [annexe 2](#) pour la définition des acteurs)

Pour aller vers l'observation

Conclure sur :

La correcte organisation de la fonction informatique.

L'identification des maîtrises d'ouvrage dans l'organisation et la correcte adéquation de leur rôle dans la fonction informatique.

Questionnements

Recrutement et formation

- ▶ Comment sont organisés le recrutement et la formation du personnel de la DSI ?
- ▶ Existe-t-il des difficultés de recrutement sur certains domaines d'expertise ?

- ▶ Quel est le taux de rotation du personnel au sein de la DSI ?

Un turnover supérieur à 15% par an au sein de la DSI est généralement considéré comme élevé. Il faut dans ce cas identifier les causes et vérifier les actions mises en œuvre pour pallier la dépendance vis-à-vis de personnes clés.

Gestion des prestataires

- ▶ Dans quel cas l'organisme fait-il appel à des prestataires informatiques ? Pour des missions de MOE ? De MOA ou d'AMOA ? Quel pourcentage cela représente-t-il par rapport à l'ensemble des ETP de la fonction informatique ?

- ▶ Une personne interne à l'organisme est-elle en charge de la gestion des prestataires pour assurer la complétude des projets et le transfert des compétences (documentation notamment) ?

- ▶ Les équipes sont-elles en capacité d'avoir une vision critique vis-à-vis des réalisations du prestataire ?

- ▶ Est-ce que l'organisme semble dépendant de certains prestataires ?

- ▶ Existe-t-il un plan d'action pour réduire l'usage de prestations en cours ? (Internalisation de certains projets, formation sur des nouvelles technologies, etc.)

Pour aller vers l'observation

Conclure sur :

L'adéquation des recrutements et des formations aux besoins des ressources de la fonction informatique.

La pertinence du recours aux prestations externes.



Point d'attention

Le rôle de la maîtrise d'ouvrage dans la supervision d'une application informatique ou dans le développement d'une nouvelle application est fondamental. Si la MOA ne remplit pas son rôle, les risques de dérapage sont importants. Les effectifs (et/ou la formation) de la MOA peuvent ne pas être suffisants pour jouer pleinement son rôle. Une partie de cette fonction est parfois externalisée (via un marché d'assistance à maîtrise d'ouvrage).



Point d'attention

Le recours trop fréquent à des prestataires, notamment dans les activités de MOE, peut faire perdre progressivement la maîtrise du système d'information de l'organisme. Il convient donc de s'assurer que les risques induits soient couverts (documentation adaptée, recrutement de personnes qualifiées) pour assurer une continuité de la connaissance en interne et une maîtrise suffisante des prestataires.

Le [ISAE 3402^{GI}](#) (Rapport SOC 1 type 1 et 2) est un standard permettant aux utilisateurs de prestations externalisées d'obtenir une assurance sur la fiabilité du contrôle interne de leur prestataire de service.

Documents à consulter :



Organisation de la DSI et description des rôles et des responsabilités

Organisation des MOA et description des rôles et responsabilités

Liste des prestataires et objet de leurs missions

AXE 4 – EVALUER LE CONTROLE INTERNE RELATIF AU SYSTEME D'INFORMATION

Enjeux pour l'organisme

- ▶ Recenser et évaluer les risques liés aux SI et mettre en œuvre des actions adaptées
- ▶ Mettre en œuvre des dispositifs de contrôle interne spécifiques aux systèmes d'information

Risques

- ▶ Un SI non sécurisé (faiblesses dans la détection de risques liés à la sécurité du SI)
- ▶ Un SI non fiable (dans le cas d'un contrôle interne sur le SI défaillant)
- ▶ Un SI non conforme aux exigences réglementaires (dispositif de contrôle interne défaillant)



Bonnes pratiques

Quelle que soit la taille de l'organisme, il est fondamental qu'une cartographie des risques liés au SI soit élaborée et mise à jour régulièrement, et que des contrôles internes soient mis en œuvre pour mitiger les principaux risques. Cette cartographie spécifique doit être reliée à la cartographie des risques de l'organisme.

Suivant la taille de l'organisme et l'importance des systèmes informatiques, une équipe dédiée à l'évaluation de ce contrôle interne spécifique doit être déployée, avec idéalement des auditeurs SI. Un plan d'audit interne informatique doit être élaboré chaque année.

Questionnements

Cartographie des risques informatiques

- ▶ Une cartographie des risques informatiques a-t-elle été élaborée ? Couvre-t-elle l'ensemble du SI ? Est-elle à jour ? Est-elle en lien avec la cartographie des risques de l'organisme ?
- ▶ En particulier, existe-t-il une cartographie des risques liés à la sécurité du SI ?
- ▶ Ces risques sont-ils qualifiés notamment en termes de fréquence et d'impact ?
- ▶ Y-a-t-il un comité de maîtrise des risques au sein de l'organisme ? Si oui, est-ce que les risques liés aux systèmes d'information sont évoqués lors de ces comités ?

Pour aller vers l'observation

Conclure sur :

La fiabilité et l'exhaustivité des risques identifiés et la qualité des plans d'action associés.

Questionnements

Plan d'action

- ▶ En fonction de la gravité des risques recensés et évalués dans la cartographie, est-ce que des plans d'action sont mis en œuvre pour réduire les risques ?
- ▶ Et notamment, des contrôles ont-ils été embarqués dans les applications informatiques majeures pour couvrir les risques identifiés ? (cf. [fiche 5- axe 2](#))
- ▶ Qui est en charge de suivre ces plans d'action ?

Audits sur les systèmes informatiques

- ▶ Des audits (en interne ou en externe) portant sur les systèmes informatiques sont-ils réalisés ? A qui sont communiqués les rapports d'audit sur le SI ?
- ▶ Est-ce que ces audits sont programmés afin de couvrir l'ensemble du SI sur une base pluriannuelle ?
- ▶ Ces audits donnent-ils lieu à des plans d'action ? Qui est en charge de suivre la mise en œuvre de ces plans d'action ?

Pour aller vers l'observation

Conclure sur :

La pertinence et l'efficacité du contrôle interne lié aux systèmes d'information.



Point d'attention

Les organisations, face à la prépondérance de plus en plus grandissante des systèmes informatiques dans la gestion des processus métier, n'ont souvent pas fait évoluer leurs dispositifs de contrôle interne pour prendre en compte la composante informatique à sa juste mesure.

Les risques liés au SI sont souvent dispersés dans l'ensemble de l'organisme, et ne sont pas couverts de façon exhaustive par les dispositifs de contrôle interne.

Il est fondamental que ces risques soient recensés et consolidés dans un même outil pour disposer d'une cartographie exhaustive des risques.

Documents à consulter :



Cartographie des risques informatiques
Plan de contrôle interne informatique
Résultat des contrôles portant sur le système d'information (revue des habilitations, etc.)
Rapports d'audit portant sur SI
Compte rendu de comité de maîtrise des risques

Pour en savoir plus :

GTAG1-2^{ème} édition, [Les contrôles et le risque des systèmes d'information](#), CRIPP Institute of Internal Auditors,

[GTAG8- Audits des contrôles applicatifs](#), CRIPP Institute of Internal Auditors,

Les [résultats de l'étude « Risk in Focus »](#) basée sur les réponses de plus de 300 professionnels de l'audit interne travaillant dans des organisations à travers l'Europe, l'enquête cartographie les 10 principaux risques auxquels les entreprises des secteurs privé et public devraient être confrontées en 2019

AXE 5 – S'ASSURER DE LA MAITRISE DU BUDGET INFORMATIQUE

Enjeux pour l'organisme

- ▶ Mettre en œuvre un dispositif de suivi du budget informatique
- ▶ Mettre en œuvre des procédures spécifiques pour la gestion des marchés de prestation informatique

Risques

- ▶ Pilotage insuffisant et dérapage des dépenses SI
- ▶ Marchés informatiques comportant des risques juridiques (par exemple, en raison d'une expertise SI insuffisante)



Bonnes pratiques

Dans le cas d'un organisme d'une taille importante, un contrôle de gestion dédié aux dépenses informatiques ainsi que des outils appropriés de suivi budgétaire et de comptabilité analytique est fortement recommandé.

Par ailleurs, dans le cadre de la passation des marchés de prestations externes informatiques, il est nécessaire de faire appel à des experts métier et des professionnels de l'informatique pour la rédaction des cahiers des charges et l'analyse des offres.

Questionnements

Suivi du budget informatique

- ▶ Comment et par qui est élaboré et validé le budget informatique ?
- ▶ Est-ce que le périmètre du budget informatique est exhaustif ?
- ▶ Existe-t-il une correspondance directe entre le budget validé dans le cadre du SDI et le budget informatique annuel ?
- ▶ Comment est organisé le contrôle de gestion informatique ? Existe-t-il un contrôleur de gestion dédié au sein de la DSI ?
- ▶ Quels sont les outils et procédures de suivi analytique, de contrôle des coûts, d'analyse des écarts ?
- ▶ Quels sont les tableaux de bord de suivi budgétaire ? A quelle fréquence sont-ils actualisés ?
- ▶ Existe-t-il des comités spécifiques de suivi de l'exécution budgétaire des dépenses informatiques ?

Pour aller vers l'observation

Conclure sur :

Le dispositif d'élaboration et de suivi du budget informatique.

Questionnements

Marchés informatiques (selon le contexte)

- ▶ L'organisme a-t-il recours à des marchés de prestation informatique ?
- ▶ Y-a-t-il un département spécifique pour gérer les marchés informatiques (rédaction, passation, dépouillement, exécution)?
- ▶ Comment est associée la DSI pour l'élaboration des cahiers des clauses techniques particulières (CCTP), le dépouillement des offres et la notification des services faits pour déclencher les paiements ?
- ▶ Des clauses de réversibilité^{GI}, de confidentialité, de pénalité, de RGPD et de propriété des données ont-elles été définies ?
 - ❖ *Si oui, qui est en charge de suivre l'application de ces pénalités ? Ont-elles déjà été appliquées ? Si non, pourquoi ?*

Pour aller vers l'observation

Conclure sur :

Le choix du prestataire réalisé sur une base rigoureuse et justifiée.

L'existence de contrats définissant un cadre précis d'intervention et permettant de prévenir tous cas litigieux.



Point d'attention

Les risques liés aux marchés informatiques sont multiples notamment financiers (certains marchés peuvent avoir des coûts finaux prohibitifs) et pénaux (si les marchés sont mal rédigés, mal passés ou mal exécutés ils peuvent être requalifiés par un juge en prêt illégal de main d'œuvre ou en délit de marchandage – Article [L. 8231-1](#)- [L. 8241-1](#) et [L. 8241-2](#) du code du travail).

Documents à consulter :



Budget annuel informatique
Tableaux de suivi des dépenses informatiques
Procédure de passation des marchés informatiques
Liste des marchés de prestation informatique
Exécution budgétaire des marchés informatiques

Attention :

Les marchés de prestation informatique peuvent comporter des aspects techniques qui sont difficilement compréhensibles. Les auditeurs informatiques du CAM (dmd@ccomptes.fr) se tiennent à votre disposition pour comprendre et analyser les marchés informatiques, notamment pour détecter si l'objet du marché correspond bien aux travaux réalisés.

FICHE 2 – L'ENVIRONNEMENT INFORMATIQUE

PRESENTATION

Auditer l'environnement informatique d'une organisation consiste à :

- prendre connaissance du système d'information de l'entreprise : applications, matériels, dispositifs logiques, processus ainsi que les interactions entre les différents éléments du SI pouvant servir de base pour appuyer le reste de la démarche d'audit des SI ;
- évaluer le niveau d'exhaustivité, de fiabilité et de pertinence des connaissances de l'entité vis-à-vis de son système d'information. L'entité doit appuyer toute démarche ayant pour finalité l'évolution du SI sur des éléments concrets, quantifiés et à jour. Pour ce faire, un processus d'acquisition, de mise à jour et d'amélioration continue des connaissances liées au SI doit être mis en place.

La connaissance du SI doit faire l'objet d'une formalisation et d'un suivi régulier sous la forme de cartographies le décrivant de différents points de vue (métier, applicatif, infrastructure, risques) dont le niveau de détails doit être adapté en fonction des enjeux du SI (criticité des données, taille de l'organisme, impact potentiel d'une défaillance).

LES RISQUES

Sans connaissances précises des éléments composants le système d'information, l'entité met en péril l'ensemble de ses processus. Cela peut entraîner :

- Une évolution du SI non cohérente avec les besoins du métier.
- Une incapacité à répondre rapidement à un incident (absence de vision globale des causes et impacts potentiels par exemple).
- Des défaillances sur la sécurité des données (absence d'identification des zones de faiblesse et des possibles chemins d'attaque par exemple).
- Des difficultés à faire évoluer le SI pouvant entraîner une obsolescence (défaut d'homogénéité dans les applications par exemple).

LES OBJECTIFS

Cette fiche doit permettre :

- **D'évaluer la formalisation des connaissances liées au SI (axe 1)**, cela passe notamment par la cohérence des cartographies produites et leurs mises à jour ainsi que le partage de cette connaissance avec l'ensemble des acteurs du SI (cf. [annexe 2](#)).
- **De vérifier les interactions entre les éléments du SI (axe 2)** et la supervision des flux de données. Le cas particulier des ERP^{GI} est abordé.
- **D'analyser la maîtrise du parc informatique (axe 3)** en identifiant la politique de suivi et de renouvellement du parc informatique et logiciel, et d'analyser sa cohérence par rapport aux enjeux de la structure.
- **D'évaluer l'urbanisation du SI^{GI} (axe 4)** c'est à dire la stratégie mise en œuvre pour simplifier le système d'information et améliorer sa cohérence.
- **D'évaluer la maîtrise de l'informatique en nuage (« CLOUD ») (axe 5).**

AXE 1 – EVALUER LA FORMALISATION DES CONNAISSANCES DU SI

Les enjeux pour l'organisme

- ▶ Une vision globale et à jour du SI
- ▶ La formalisation des connaissances liées au SI permettant de faire des choix cohérents d'évolution alignés avec les objectifs de l'organisation
- ▶ Un format adapté aux différents besoins et points de vue

Les risques

- ▶ Non maîtrise des évolutions
- ▶ SI obsolète
- ▶ Absence d'alignement avec les besoins du métier
- ▶ Vulnérabilité aux intrusions extérieures et aux incidents



Bonnes pratiques

Le système d'information doit être connu des agents de l'entité et doit être formalisé sous forme de différentes cartographies (applicative et infrastructure), chacune offrant un point de vue différent.

La cartographie permet de représenter le système d'information (SI) d'une organisation ainsi que ses connexions avec l'extérieur. Cette représentation peut être plus ou moins détaillée et inclure, par exemple, les biens matériels, logiciels, les réseaux de connexion, mais aussi les informations, activités et processus qui reposent sur ces biens. La cartographie est un outil essentiel de maîtrise du système d'information pour chaque organisme. Elle vise à rendre lisibles et compréhensibles différents aspects du système d'information.

Concrètement, la cartographie doit permettre de :

- réaliser l'inventaire du système d'information, à savoir la liste des composants du SI et leur description détaillée ;
- présenter le système d'information selon différents points de vue (technique, applicatif, fonctionnel), afin de documenter son fonctionnement interne et ses relations avec l'extérieur.

Il est fondamental que ces cartographies mettent en exergue les éléments les plus importants pour l'organisation. L'entité doit également s'appuyer sur une démarche de mise à jour et d'amélioration continue des cartographies, dans un souci de clarté, d'accessibilité, d'exhaustivité et d'efficacité. Pour les entités de taille intermédiaire ou grande, ou dont l'activité est sensible, une cartographie des risques informatiques est aussi nécessaire.

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

Cartographie applicative

► L'entité a-t-elle réalisé un inventaire des applications sur lesquelles le métier s'appuie et formalisé le résultat en cartographie applicative^{GI} ?

► Cette dernière prend-elle en compte le découpage fonctionnel ?

► Spécifie-t-elle les caractéristiques de chaque application : mode d'hébergement, propriétaires métier et processus couverts, prestataires ?

❖ *En l'absence de cartographie demander un recensement des applications dans un tableur en indiquant les éléments mentionnés dans [l'annexe 3](#).*

Autres cartographies

► Une cartographie des flux permet-elle de décrire la manière dont l'information circule entre les applications internes (interfaces) et avec l'extérieur ?

► L'entité dispose-t-elle d'une cartographie de l'infrastructure^{GI}, qui décrit le matériel informatique et les dispositifs logiques composant le SI ? Celle-ci inclut-elle les dispositifs de sécurité ?

► Existe-t-il un processus formalisé de mise à jour des cartographies ? Est-il appliqué ?

❖ *Vérifier la dernière date de mise à jour des cartographies et leur mode de révision (cf. [Axe 4](#)).*

Conclure sur :

La formalisation de la connaissance du SI sous la forme de cartographies complètes et compréhensibles.

Documents à consulter :



Cartographie applicative ou liste des applications (acquises et développées)

Liste des immobilisations informatiques

Cartographie réseau

Toute documentation sur des applications et des évolutions apportées

Pour en savoir plus

[Guide ANSSI](#) pour la réalisation de cartographie

AXE 2 – VERIFIER LES INTERACTIONS ENTRE LES ELEMENTS DU SI

Les enjeux pour l'organisme

- ▶ Maîtriser la manière dont l'information circule dans le système d'information
- ▶ Garantir la fiabilité, l'exhaustivité et la sécurité inhérente des données

Les risques

- ▶ Défaut d'exhaustivité et d'intégrité des données (augmente avec le nombre d'applications et d'interfaces^{GI})




Bonnes pratiques

D'une manière générale, un système d'information fortement intégré permet à l'information de circuler de manière plus rapide et fiable. Cette intégration est l'un des principaux atouts des progiciels de gestion intégrés^{GI} (en anglais : Enterprise Resource Planning ou ERP), qui permettent la circulation des données en temps réel et offrent un large choix de contrôles paramétrables. Parmi les plus répandus, on peut citer ORACLE, SAP ou encore Berger Levrault pour les collectivités.

La centralisation des fonctionnalités vers un nombre restreint d'applications, permet de limiter au maximum le risque de perte ou d'altération des données. Pour faciliter l'échange d'information entre les applications qui n'ont pas été conçues pour fonctionner ensemble, on peut constater le recours à un intergiciel^{GI} (logiciel qui agit comme une passerelle entre les autres applications, outils et bases de données pour offrir aux utilisateurs des services unifiés).

Des contrôles automatiques doivent être mis en place pour assurer la bonne transmission des données entre les applications.

Questionnements	Pour aller vers l'observation
<p>Interface entre les applications</p> <ul style="list-style-type: none"> ▶ L'entité s'appuie-t-elle sur un progiciel de gestion intégré ? Ce choix est-il justifié vis-à-vis de l'entité (taille, secteur d'activité, enjeux propres...) ? ❖ <i>NB : les ERP sont des produits coûteux à court terme, même si à long terme ils permettent souvent de faire des économies.</i> ▶ Quelles sont les applications les plus importantes pour l'activité de l'organisme ? Le nombre d'applications pourrait-il être réduit en centralisant certaines fonctionnalités ? 	<p>Conclure sur :</p> <p>Le degré d'intégration du SI.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p style="text-align: center;"> Point d'attention</p> <p>La mise en place d'un ERP ne signifie pas nécessairement d'une amélioration du flux de données si celui-ci doit cohabiter et échanger avec d'autres applications.</p> </div>

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

- ▶ Quel est le degré d'intégration du SI ? Des interfaces semi-automatiques ou manuelles entre les applications existentielles ? L'entité s'appuie-t-elle sur un intergiciel ?

Conclure sur :

Le niveau de contrôle des flux de données.

Contrôles mis en place

- ▶ Quels sont les contrôles mis en place par l'entité au niveau des interfaces entre les applications ?

- ▶ Y a-t-il des interfaces semi-automatiques (ou purement manuelles), nécessitant des interventions manuelles de la part des utilisateurs ? Y a-t-il des déversements manuels de données ? Quels sont les contrôles en place sur ces deux cas de figure ? (Voir point d'attention et [fiche 5-Axe 4](#))

- ▶ Pour les interfaces automatiques, comment sont traitées (recyclées) les données rejetées par les contrôles ?

- ❖ *Pour les collectivités locales : faire un focus sur l'interface (PESV2^{GI}) entre le système de l'ordonnateur et celui du comptable public.*

- ▶ Y a-t-il des contrôles forts sur cette interface pour s'assurer de l'exhaustivité et de l'exactitude des données échangées ?



Point d'attention

Les interfaces entre les applications sont les principales zones de risques d'un SI. A chaque interface, l'information peut circuler de manière automatique, de manière semi-automatique ou assistée, ou de manière manuelle. Plus le degré d'intervention humaine est fort (interfaces semi-automatiques ou manuelles) plus l'erreur est possible et par conséquent plus de contrôles robustes sont attendus.

Documents à consulter :



Liste des interfaces et des contrôles en place
Procédure de supervision des flux

Attention :

S'il est nécessaire de réaliser une revue ciblée des interfaces, nous vous conseillons de faire appel à un auditeur SI spécialisé en contactant la direction des méthodes et des données.

AXE 3- ANALYSER LA MAITRISE DU PARC INFORMATIQUE

La gestion de parc informatique regroupe un ensemble de tâches visant à entretenir, développer et optimiser l'ensemble des ressources informatiques de l'entreprise. Sont couverts dans cet axe :

- Le recensement et la localisation de l'ensemble des éléments du parc informatique.
- La définition de l'organisation du système informatique.
- La mise en place de procédures de renouvellement des postes informatiques, serveurs et équipements réseau en fonction d'un cycle de vie prédéfini.

Les enjeux pour l'organisme

- ▶ Connaître le patrimoine de l'entreprise et ses caractéristiques
- ▶ Être capable de mettre en place une stratégie de renouvellement des matériels et logiciels
- ▶ Faire des économies d'échelle et optimiser les ressources informatiques

Les risques

- ▶ Coûts de maintenance et de renouvellement disproportionnés
- ▶ Licences ou logiciels non utilisés (coûts)
- ▶ Incapacité de rappeler les matériels informatiques en cas de départ des employés par exemple
- ▶ Solution informatique inadapté aux exigences métier



Bonnes pratiques

Des dispositifs d'identification^{GI} des matériels et des recensements réguliers (inventaire du parc a minima annuel) doivent être mis en place. Chaque matériel doit pouvoir être lié/attribué à un collaborateur ou un service. À la suite de l'inventaire, les écarts identifiés sont envoyés à la DSI et à la comptabilité qui saisit les écritures d'écart.

Il est fondamental que la DSI réalise régulièrement un inventaire des licences utilisées et vérifie que l'ensemble des licences correspondent à des versions maintenues par l'éditeur.

Questionnements

Parc de matériel

- ▶ La fonction informatique réalise-t-elle un inventaire du parc informatique ? Si oui, selon quelle fréquence ? Sur quel dispositif / outil ?
- ▶ Une politique de renouvellement du parc a-t-elle été mise en place ? (Une bonne pratique consiste à changer les ordinateurs tous les 3 ans en moyenne)

❖ *Vérifier l'âge des principaux matériels pour identifier une éventuelle obsolescence*

Pour aller vers l'observation

Conclure sur :

La fréquence, l'exhaustivité et la qualité des inventaires réalisés (matériels et logiciels).

Les procédures d'actualisation suite aux départs des employés.

Questionnements

- ▶ Combien de serveurs, d'ordinateurs, smartphones, tablettes, téléphones, imprimantes, scanners etc. sont-ils mis à disposition par l'organisme ?
 - ❖ *Le comparer au nombre d'ETP pour vérifier la cohérence.*
- ▶ Vérifier les écarts identifiés entre l'inventaire physique et les données du logiciel de suivi.
 - ❖ *Il s'agit de vérifier la bonne maîtrise du parc informatique à travers le logiciel de suivi.*
- ▶ Comment les écarts sont-ils corrigés dans le logiciel de suivi mais également en comptabilité ?

Parc de logiciels

- ▶ Comment sont définis les logiciels autorisés ? L'entité dispose-t-elle d'un répertoire de logiciels ?
- ▶ Est-ce que l'entité réalise un suivi des coûts des licences de l'organisme ?
- ▶ Comment la DSI s'assure-t-elle que les versions des logiciels installées sont toujours maintenues par l'éditeur ?

Procédure en cas de départ

- ▶ En cas de départ des employés, la fonction informatique en est-elle informée afin de récupérer les matériels informatiques et fermer les accès logiciels, droits sur les répertoires partagés ainsi que pour récupérer les licences ?

Pour aller vers l'observation



Point d'attention

Le parc informatique est un actif indispensable au bon fonctionnement de l'organisation. Il comprend le matériel et les logiciels.

L'utilisation d'un outil dédié lors de la réalisation des inventaires témoigne d'un certain degré de professionnalisme, mais ne signifie pas nécessairement que ces inventaires sont réalisés à une fréquence suffisante.

NB : Le parc informatique volant (tablettes, ordinateurs et téléphones portables) doit faire l'objet d'une attention particulière en ce qui concerne les vols et leur utilisation hors du cadre du travail.



Point d'attention

L'inventaire des licences est au moins aussi important que celui du matériel physique. La présence de contrôle des logiciels installés par les utilisateurs est nécessaire, voire pour les entités les plus matures, la mise en place d'un répertoire de logiciels autorisés et d'un processus formalisé de demande d'installation de nouveaux logiciels.

Se référer à la [fiche 6- axe 3](#) pour les questions relatives ce point.

Documents à consulter :



Dernier inventaire du parc informatique
Liste des licences de logiciels

Pour aller plus loin

Le [Socle Interministériel de Logiciels Libres](#) est le catalogue de référence des logiciels libres recommandés par l'État répondant aux besoins des administrations françaises.

AXE 4 – EVALUER L'URBANISATION DU SI

L'urbanisation du SI est un concept qui vise à simplifier le système d'information et à améliorer la communication entre ses composants avec comme objectif de disposer d'un système d'information structuré, évolutif et performant. C'est une démarche globale de rationalisation progressive du SI aux niveaux fonctionnels, applicatifs et techniques, qui doit permettre d'anticiper les besoins et évolutions futures du SI et répondre aux nouvelles demandes des utilisateurs.

Les enjeux pour l'organisme

- ▶ Meilleure flexibilité du SI : possibilité d'isoler, d'ajouter ou de remplacer un élément du système (application, module, infrastructure^{GI} logique ou technique) avec facilité
- ▶ Amélioration de la lisibilité du SI
- ▶ Rationalisation des coûts

Les risques

- ▶ Incapacité à faire évoluer et à répondre aux besoins du métier
- ▶ Augmentation des coûts de maintien du SI en l'absence de rationalisation des nouveaux développements
- ▶ Obsolescence



Bonnes pratiques

La démarche d'urbanisation s'articule sur trois axes clés qui s'alimentent mutuellement :

- la **cartographie des systèmes existants** (métier, fonctionnels, applicatifs, techniques) : une démarche d'urbanisation efficace s'appuie d'abord sur la formalisation des connaissances liées au SI ([voir axe 1](#)). Avant même de définir une stratégie d'urbanisation, il convient de réaliser un état des lieux du SI afin d'en identifier les faiblesses et les points forts.
- La **modélisation de la stratégie** : toute démarche d'urbanisation doit aussi être déclinée à partir de la stratégie de l'entreprise (cf. [fiche 1 – axe 1](#)). Elle doit faire partie intégrante du schéma directeur informatique^{GI} et en respecter les principes, c'est-à-dire s'appuyer sur l'existant, être justifiée, être décrite clairement en termes de délai, de qualité et de budget, et faire l'objet d'un suivi régulier. Elle définit les déclinaisons fonctionnelles et techniques de cette stratégie.
- La **détermination des systèmes cibles** (métier, fonctionnels, applicatifs, techniques). L'urbanisation rationalise chaque strate du SI et se décline en mesures concrètes, telles que la mise en place d'un progiciel de gestion, l'externalisation des processus à faible valeur ajoutée, l'achat de nouveaux matériels ou la définition de technologies privilégiées.

Les entités de grande envergure ont généralement un pôle dédié à l'urbanisation. Dans le cas d'une entité sujette à des évolutions d'origine externe ou interne structurantes, on attend, peu importe sa taille, qu'une démarche d'urbanisation soit mise en place. Cette démarche se traduit notamment par la présence de comités ad hoc dédiés à la définition de la démarche d'urbanisation et à son suivi.

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

- ▶ Une stratégie d'urbanisation a-t-elle été formalisée ?
- ▶ Comment a-t-elle été définie ? A partir de quels éléments ? Avec quels objectifs ?
- ▶ Quelle est la comitologie mise en place (fréquence, parties, etc.) ?
 - ❖ *La méthodologie choisie doit permettre à cette stratégie de s'adapter aux enjeux de l'organisme (risques et failles identifiés précédemment) ainsi qu'au schéma directeur des SI (cf. bonnes pratiques).*
- ▶ La stratégie d'urbanisation a-t-elle été déclinée en plan d'action ?
 - ❖ *Ce plan d'action doit comporter des actions concrètes pour les systèmes cibles (cf. bonnes pratiques).*
- ▶ Des indicateurs ont-ils été définis (budget, délais, qualité) ?
- ▶ La démarche d'urbanisation fait-elle l'objet d'un suivi et d'une actualisation ?

Conclure sur :

L'adéquation entre la stratégie d'urbanisation, les enjeux de l'organisme et les risques du SI.

La déclinaison de la stratégie en un plan d'action concret faisant l'objet d'un suivi.



Point d'attention

Urbaniser un SI est un travail constant, car fortement soumis aux évolutions extérieures (nouvelles technologies, réglementations, etc.)

Cette démarche doit être traduite opérationnellement en actions, et vos interlocuteurs doivent être en mesure de justifier chacune d'entre-elles, notamment du point de vue de la sécurité du SI, de sa flexibilité et des coûts de maintien.

Attention :

Pour une revue en profondeur, de la démarche d'urbanisation, vous pouvez contacter les auditeurs SI de la DMD à DMD@ccomptes.fr.

Documents à consulter :



- Schéma directeur informatique
- Documents descriptif des orientations technologiques sélectionnées
- Documents de suivi de la mise en place de la stratégie d'urbanisation
- PV de réunion des comités ad hoc

Pour en savoir plus

La [démarche d'urbanisation du SI de l'Etat](#)

AXE 5 – EVALUER LA MAITRISE DE L'INFORMATIQUE EN NUAGE (CLOUD^{GL})

L'informatique en nuage, correspond à l'accès à des services informatiques (serveurs, stockage, mise en réseau, logiciels, etc.) via des serveurs distants (internet pour le cloud public - réseau privé pour le cloud d'entreprise) plutôt qu'un stockage local. Les principaux avantages de l'informatique en nuage sont une flexibilité accrue, des économies d'échelle et l'externalisation de sujet à faible valeur ajoutée (ex : la sécurité des serveurs). Pour l'administration, se superposent des **enjeux en terme de souveraineté et de sécurité (parce que les données sont hébergées sur des serveurs pouvant être implantés dans des pays hors de portée de la réglementation nationale ou européenne)**. Une [stratégie française](#) pour le cloud a été définie en juillet 2018. Plus récemment (juin 2020), le [projet européen Gaia-X](#) ambitionne d'offrir une alternative aux solutions de Google, Amazon et Microsoft au travers d'une entité de gouvernance et d'un meta-cloud décentralisé (plateforme intégrée pour l'utilisation de plusieurs prestations de services de stockage cloud).

Les enjeux pour l'organisme

- ▶ Mise en place d'applications web accessibles depuis tout périphérique
- ▶ Externalisation de l'hébergement vers une entité spécialisée, plus à même de répondre aux problématiques de sécurité et de mise à l'échelle de l'infrastructure^{GI}
- ▶ Optimisation du SI et amélioration de la qualité de service
- ▶ Flexibilité
- ▶ Maîtrise et réduction potentielle des coûts

Les risques

- ▶ Perte de contrôle de l'organisation vis-à-vis de ses données et de son SI
- ▶ Problèmes de conformité vis-à-vis des réglementations européennes et françaises (exemple : RGPD)
- ▶ Risques inhérents à l'externalisation, tels que la disparition des compétences clés et la dépendance à une entité tierce



Bonnes pratiques

Le recours au cloud doit s'inscrire dans une démarche pertinente vis-à-vis de la sensibilité des données traitées et de ses enjeux: réduction des coûts, mise à niveau de la sécurité, mutualisation des services.

Cette prestation étant souvent externalisée, le choix du prestataire nécessite de prendre en compte les enjeux en terme de sécurité des données par exemple au travers d'un référencement SecNumCloud (voir encadré « point d'attention » ci-après).

Les modalités de sauvegarde des données doivent être négociées avec les prestataires et être pertinentes vis-à-vis des processus métiers couverts par l'application sujette au cloud.

Il est nécessaire que le plan de continuité d'activité du prestataire soit pris en compte et intégré au plan de continuité d'activité de l'entité (cf. [fiche 4- Axe 4](#)). Les opérations de réversibilité^{GI} (possibilité de récupérer ses données à l'issue de la fin de contrat) doivent être explicitement définies dans le contrat.

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

- ▶ L'entité s'appuie-t-elle sur l'informatique en nuage ? Si non, cela a-t-il fait l'objet d'un questionnement ? Le choix de ne pas recourir à l'informatique en nuage est-il justifié du point de vue de son activité et de ses enjeux ?
- ▶ Si l'entité s'appuie sur l'informatique en nuage, quelles sont les activités concernées ? Cela s'inscrit-il dans une démarche d'urbanisation du SI ?
- ▶ Est-ce que les modalités d'hébergement de données sont cohérentes par rapport à la sensibilité des données et les dispositions de la [circulaire du 8 novembre 2018](#) ?
- ▶ Comment ont été sélectionnés les prestataires ? Sont-ils qualifiés SecNumCloud ?
- ▶ Quelles sont les modalités de contractualisation avec les prestataires de services d'informatique en nuage ?
 - ❖ *Obtenir les contrats et évaluer la définition du niveau de service, des responsabilités et pénalités, des clauses de réversibilité etc.*
- ▶ L'entité a-t-elle connaissance des mesures de sécurité garanties par le prestataire (plan de continuité, contrôles d'accès aux serveurs, etc...) ?
- ▶ Dispose-t-elle des rapports de tests des plans de continuité de son prestataire ? S'est-elle astreinte à conserver un plan de continuité d'activité propre pour les services concernés par l'informatique en nuage (cf. [fiche 4- Axe 4](#)) ?

Conclure sur :

La pertinence du choix de l'entité vis-à-vis de l'informatique en nuage (implémentation ou non).

La cohérence du choix du prestataire au regard des enjeux de l'organisation.

Le degré de contrôle de l'entité sur les parties de son SI sujettes à l'informatique en nuage.

Point d'attention

L'ANSSI (agence nationale de la sécurité des systèmes d'information) propose un visa destiné à certifier qu'un [prestataire de services d'informatique en nuage](#) respecte un certain nombre de règles et de bonnes pratiques (référentiel [SecNumCloud](#).)

Point d'attention

Les activités sensibles peuvent être externalisées à un prestataire de services en nuage pour disposer d'une expertise en sécurité des données et continuité d'activité souvent difficile à acquérir en interne.

Une [nouvelle offre a été proposée par l'UGAP](#) sur un catalogue d'offres de cloud public répondant aux besoins des applications et des données les moins sensibles.

Documents à consulter :

Contrat et niveaux de services
Certification de l'ANSSI

Pour en savoir plus

Le [forum de la communauté numérique](#) présente des ressources actualisées sur ce sujet.

FICHE 3 – L'ÉVOLUTION DU SYSTÈME D'INFORMATION

PRESENTATION

On entend par évolution du SI toute modification simple ou complexe de l'existant.

On distingue la **gestion des maintenances correctives** (suite à un incident ou une faille de sécurité) de celles **évolutives** (pour améliorer une application avec de nouvelles fonctionnalités par exemple). Cette évolution peut relever d'une décision stratégique (par exemple un regroupement dans le cas de l'intercommunalité) comme d'une nécessité technologique ou réglementaire (prise en compte d'une nouvelle législation par exemple).

En premier lieu, il est donc nécessaire de caractériser le changement opéré qui peut être décliné en deux catégories :

- Le **changement « standard »** est préautorisé et à risque faible. Il est fréquemment implémenté et suit une procédure ou une instruction de travail spécifique. Les changements standards étant pré-approuvés, ils suivent un processus optimisé dans lequel les étapes d'autorisation et d'approbation sont adaptées.
- Le **changement non standard** ou « normal » suit la procédure de changement de l'entité (mode projet) et le niveau de prise de décision est adapté aux risques et impacts attendus (de l'administrateur au comité de direction). Il se subdivise en trois catégories:
 - **Mineur** : les ressources, coûts et risques sont faibles (par exemple changement modéré de charte graphique, évolution de la documentation).
 - **Significatif** : les ressources, coûts et risques sont importants (par exemple modification de règles de calculs, mise à jour d'une application, modification du paramétrage d'authentification).
 - **Majeur** : les ressources, coûts et risques sont majeurs (par exemple migration d'une application critique vers le cloud, montée de version d'un logiciel critique, changement de prestataire informatique ou d'hébergeur, changement de localisation de l'activité de l'entité).

Par ailleurs, la démarche d'évolution dépendra de la temporalité du changement qui définira son niveau de priorité. On note en particulier **les changements urgents**, par exemple pour résoudre un incident majeur ou implémenter un correctif de sécurité. Ce changement est d'une priorité telle qu'il contourne le cycle de vie complet d'un changement normal en raison de la rapidité avec laquelle il doit être autorisé.

LES RISQUES

- Obsolescence du SI : standards dépassés ou délais dans l'implémentation des normes.
- Manque d'efficacité des projets informatiques : dépassement des délais et mauvaise utilisation des moyens humains ou financiers.
- Défaut dans la continuité de l'activité : altération / perte des données sensibles.
- Mauvaise intégration des évolutions : non alignement du projet à la stratégie globale de l'organisme.

- Inadéquation au besoin ou manque de communication qui conduit à une résistance au changement de la part des utilisateurs.
- Indisponibilité des services : problèmes d'exploitation et de maintenance de la nouvelle solution.

LES OBJECTIFS

NB : Les questions relatives à la gouvernance et à la stratégie d'évolution sont abordées dans la [Fiche 1 \(axe 1\)](#). Les considérations relatives à la comitologie et au pilotage dans l'axe 2 de cette même fiche.

Les objectifs de cette fiche sont de permettre :

- **D'évaluer le maintien en condition opérationnelle des applications informatiques (axe 1)**

Le premier type d'évolution concerne la maintenance des applications existantes. Leur réussite nécessite de disposer des ressources adéquates ainsi que de mettre en place une planification et des procédures adaptées.

- **D'évaluer le pilotage et l'organisation des projets d'évolution (axe 2)**

Dans le cas de changements plus importants ou pour la mise en place de nouvelles briques applicatives, le projet d'évolution doit suivre des étapes précises du cadrage du besoin à la rédaction des spécifications et aux tests (fonctionnels et techniques).

La démarche d'évolution doit être inclusive tant au niveau de la direction générale (notamment pour le déploiement des ressources nécessaires) que des métiers (définition du besoin et adhésion de l'ensemble des collaborateurs à la nouvelle solution proposée).

- **De contrôler les projets innovants (axe 3)**

Les projets d'innovation s'inscrivent dans une vision à long terme et s'évaluent donc par rapport à la stratégie globale de l'entité. Ils ont des caractéristiques (coûts entre autres) et des modalités de réalisation spécifiques.

AXE 1 – EVALUER LE MAINTIEN EN CONDITION OPERATIONNELLE DES APPLICATIONS INFORMATIQUES

Le maintien en condition opérationnelle des applicatifs consiste à corriger (maintenance) ou à faire évoluer les applications afin de maintenir un haut niveau de qualité et répondre aux besoins évolutifs des métiers.

Les enjeux pour l'organisme

- ▶ Continuité de service
- ▶ Maintien à niveau (mise à jour, ajout d'extensions) permettant d'optimiser la performance des applications

Les risques

- ▶ Incidents fréquents menant à une indisponibilité des différentes applications
- ▶ Obsolescence des applications informatiques
- ▶ Non-respect des obligations réglementaires
- ▶ Non adéquation des applications avec les besoins des utilisateurs



Bonnes pratiques

Le niveau de satisfaction des utilisateurs et la qualité des applications doivent faire l'objet d'un suivi (par exemple au travers d'analyses régulières des incidents ou d'enquêtes auprès des utilisateurs-cf. [Fiche 1 – axe 2](#)). La mise en place d'une comitologie est nécessaire afin de prioriser et de suivre les actions correctives à mettre en œuvre.

Il est recommandé qu'une procédure et des contrôles soient mis en place afin de s'assurer que les modifications apportées aux applications sont tracées, correctement testées et validées avant la mise en production. Ce processus doit être contrôlé par l'audit interne.

Questionnements

Planification des besoins de maintenance

- ▶ Des maintenances ou des corrections applicatives sont-elles réalisées suite à l'identification d'incidents ? (Cf. [fiche 4 – axe 3](#) sur la gestion des incidents)
- ▶ Des comités réguliers ont-ils lieu afin de classer ces anomalies (CCC – *comité consultatif de changement* / CAB – *change advisory board*) ?
- ▶ Des instances d'arbitrage décident-elles de l'ordre de priorité des corrections applicatives ? L'entité a-t-elle mis en place un suivi de la réalisation des actions ?
- ▶ Un suivi des correctifs des éditeurs est-il réalisé ? Quelle est la temporalité choisie

Pour aller vers l'observation

Conclure sur :


La mise à jour dans les meilleurs délais du parc applicatif de l'entité.

La robustesse des actions correctives mises en place en cas d'incident.



Point d'attention

Le processus à suivre pour déclarer et résoudre un incident doit être connu de l'ensemble des agents et rigoureusement suivi.

Questionnements	Pour aller vers l'observation
<p>pour installer les mises à jour des éditeurs ? (Immédiate ou dans un délai pour avoir du recul sur les éventuelles anomalies)</p>	
<p>Ressources opérationnelles</p> <p>► Existe-t-il une équipe dédiée au maintien en condition opérationnelle de(s) l'application(s) ?</p> <p>❖ <i>Vérifier :</i></p> <ul style="list-style-type: none"> - <i>Le dimensionnement et la composition de l'équipe.</i> - <i>La séparation des fonctions entre développement et production (cf. annexe 2).</i> 	<p>Conclure sur :</p> <p>La disponibilité des équipes pour intervenir sur l'application.</p>
<p>Existence d'une procédure liée à la gestion des évolutions</p> <p>► Existe-t-il une procédure rédigée de gestion des modifications applicatives</p> <p>❖ <i>Vérifier notamment la présence :</i></p> <ul style="list-style-type: none"> - <i>d'une documentation assurant la traçabilité des modifications ;</i> - <i>d'un circuit de validation adapté ;</i> - <i>d'une politique de test avant production. Cf. fiche 4 sur la production ;</i> - <i>d'une validation formelle du métier avant la mise en production.</i> <p>► Existe-t-il une procédure spécifique rédigée pour les maintenances correctives urgentes ?</p> <p>► Est-ce que l'implémentation des correctifs de sécurité est formalisée au sein de la procédure ?</p>	<p>Conclure sur :</p> <p>La robustesse des procédures relatives aux modifications.</p> <p>La cohérence de ces processus par rapport aux objectifs.</p> <p>Conclure sur :</p> <p>Le contrôle interne associé à ces procédures.</p>
<p>Suivi du respect des procédures</p> <p>► Existe-t-il une instance (audit interne, etc.) chargée de s'assurer du respect des procédures de gestion des changements et de la sensibilisation des équipes dédiées?</p>	<div style="border: 1px solid black; padding: 10px;"> <p style="text-align: center;"> Point d'attention</p> <p>Le caractère urgent des maintenances correctives représente un risque car les développements sont souvent insuffisamment testés ce qui peut entraîner de nouvelles anomalies.</p> </div>

Documents à consulter :



- Les derniers comptes rendus de comité d'arbitrage des changements (CCC ou CAB)
- La liste des maintenances ou actions correctives réalisées suite à des incidents
- Processus de mise à jour des correctifs de sécurité

AXE 2 – EVALUER LE PILOTAGE ET L'ORGANISATION DES PROJETS D'EVOLUTION

Les enjeux pour l'organisme

- ▶ Définir l'implication, les rôles et les responsabilités de chaque partie prenante
- ▶ Utiliser une méthode de projet adaptée aux enjeux ([Cf. annexe 4](#))
- ▶ S'assurer que l'avancement du projet est conforme aux attendus (agenda, budget...)
- ▶ Accompagner les utilisateurs vers le changement

Les risques

- ▶ Evolution non adaptée aux besoins.
- ▶ Manque d'optimisation des ressources de la structure
- ▶ Projets mis en place de manière désorganisée menant à des délais longs, des abandons, etc.
- ▶ Résistance au changement





Bonnes pratiques

Un pilotage opérationnel doit être mis en place. Il s'appuie sur une lettre de mission clairement définie, des indicateurs de performance et rend régulièrement compte aux instances stratégiques.

L'équipe ne doit pas se résumer au chef de projet. Ce dernier doit être accompagné par une équipe dont les profils et l'implication permettent un regard critique. La mobilisation de la créativité des utilisateurs peut être sollicitée par le déploiement de « pilotes » avant la mise en place du projet en « grandeur nature ». La mise en place d'un retour d'expérience permet de capitaliser sur l'expérience afin de définir des axes d'amélioration futurs. Chaque modification doit être testée dans des conditions réelles.



A. Vérifier le pilotage du projet et la distribution des tâches

Questionnements	Pour aller vers l'observation
<p>Cohérence de la méthode liée à la gestion des évolutions</p> <ul style="list-style-type: none"> ▶ Une méthode de gestion de projet adaptée a-t-elle été choisie (type cycle en V ou Agile cf. annexe 4) ? ▶ La méthodologie de projet est-elle formalisée? <p><i>Lorsque la méthodologie n'est pas formalisée, vérifier a minima par entretien, sur un échantillon de projets, que des étapes du projet sont respectées (cf. ci-dessous et annexe 4 et 5).</i></p> <p>Pilotage du projet</p> <ul style="list-style-type: none"> ▶ Une matrice des risques liés au projet a-t-elle été réalisée ? Quelles actions ont été mises en place pour couvrir ces risques ? 	<p>Conclure sur :</p> <p>La pertinence et la formalisation de la méthodologie.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p style="text-align: center;"> Point d'attention</p> <p>La méthodologie de projet peut être formalisée au sein d'une procédure succincte, contenant les étapes, les acteurs impliqués, les livrables et les dispositifs suivis.</p> </div> <p>Le présence d'un pilotage opérationnel identifié.</p>

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none"> ▶ Le projet dispose-t-il d'un sponsor ? A quel niveau hiérarchique se situe-t-il ? ▶ Un chef de projet a-t-il été désigné? <p>Suivi du projet</p> <ul style="list-style-type: none"> ▶ Des comités de pilotage ont-ils été mis en place ? ▶ Des indicateurs ont-ils été établis ? Si oui, comment ? Par qui ? Sont-ils quantitatifs ou qualitatifs ? ▶ Des indicateurs de performance ont-ils été définis pour les aspects financiers et temporels (respect des délais)? Montrent-ils des résultats positifs? <p>Distribution des tâches</p> <ul style="list-style-type: none"> ▶ Une matrice RACI^{GI} a-t-elle été définie et chaque personne connaît-elle ses responsabilités ? <p><i>NB : L'acronyme RACI signifie</i></p> <p><i>Responsible - qui réalise ;</i> <i>Accountable - qui supervise et rend des comptes ;</i> <i>Consulted - qui conseille ;</i> <i>Informed - qui est informé</i></p> <p>Les moyens humains et financiers</p> <ul style="list-style-type: none"> ▶ Les initiatives d'évolutions bénéficient-elles de ressources (matérielles, humaines, budgétaires) alignées avec l'ampleur du projet? ▶ Des indicateurs de suivi de budget ont-ils été créés ? ▶ Le profil/les formations des équipes sont-ils adaptés ? ▶ Ces ressources sont-elles rapidement mobilisables ? <ul style="list-style-type: none"> ❖ <i>Vérifier que le chef de projet est entouré d'experts qui peuvent apporter un regard critique sur les méthodes de travail et les choix réalisés lors du projet.</i> 	<p>Conclure sur :</p> <p>La pertinence des indicateurs de suivi de projet</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"> Point d'attention</p> <p>MAREVA 2 (Méthode d'Analyse et de Remontée de la Valeur) est une méthode pour calculer la valeur stratégique et économique générée par les projets SI lors des différentes étapes de leur cycle de vie.</p> </div> <p>Conclure sur :</p> <p>La prise en compte des responsabilités de chacun.</p> <p>Conclure sur :</p> <p>La corrélation entre les moyens alloués et les ambitions de l'évolution souhaitée.</p> <p>La cohérence des ressources mises en place au sein de l'organisation pour accompagner les projets de la phase d'idéation à la mise en production.</p> <p>La capacité à conduire le projet et à avoir une vision critique.</p>
<p>Dans le cas d'un recours à une prestation de services, se référer à la Fiche 1 – axe 3 et axe 5 sur les marchés informatiques et vérifier les conventions/contrats de partenariat avec les tiers externes à l'entité.</p>	

B. Vérifier les temps forts du projet (cf. annexe 5)

Quelle que soit la méthode de gestion de projet, un projet significatif ou majeur doit systématiquement faire l'objet d'une planification précise et inclure les grandes étapes présentées dans [l'annexe 5](#).

Questionnements	Pour aller vers l'observation
<p>Etude du besoin et conception fonctionnelle</p> <ul style="list-style-type: none"> ▶ Une étude précise de besoin a-t-elle été réalisée? Si oui, comment a-t-elle été réalisée? Par qui? Les équipes métier ont-elles été impliquées ? 	<p>Conclure sur :</p> <p>Si le cadrage réalisé est réaliste, adapté et correspond aux besoins métier de l'organisme.</p> <p>L'implication des métiers dans le projet.</p>
<p>Documentation liée au projet</p> <ul style="list-style-type: none"> ▶ Les spécifications fonctionnelles et techniques ont-elles été rédigées ? ▶ Les évolutions sont-elles documentées et validées en collaboration avec les équipes métier ? 	<p>Conclure sur :</p> <p>L'existence et la qualité de la documentation liée au projet.</p>
<p>Politique de tests</p> <ul style="list-style-type: none"> ▶ Des tests fonctionnels sont-ils réalisés par l'AMOA et les futurs utilisateurs pour s'assurer que les résultats sont ceux attendus? ▶ Ces tests sont-ils documentés? Quelles en sont les conclusions? 	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;"> Point d'attention</p> <p>Le changement en cas de projet ne concerne pas seulement l'outil mais également : l'organisation, les conditions de travail, les responsabilités, les compétences, les pratiques, la stratégie...</p> </div> <p>Conclure sur :</p> <p>La robustesse des tests réalisés.</p>
<p><i>Pour les parties liées à la pré-production et la production, se référer à la fiche 4</i></p>	<div style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;"> Point d'attention</p> <p>Le cadrage entre les spécifications fonctionnelles et les développements réalisés est essentiel.</p> </div>
<p>Communication et conduite du changement</p> <ul style="list-style-type: none"> ▶ Quelles communications ont été réalisées pour les métiers ? Les utilisateurs ? A quelles étapes et à quelle fréquence ? ▶ Le nouvel outil est-il accepté et utilisé par les métiers ? La solution répond-elle aux besoins des utilisateurs ? ▶ Un retour d'expérience a-t-il été réalisé afin de capitaliser sur les actions réalisées ? 	<p>Conclure sur :</p> <p>La diffusion de l'information autour de la stratégie à l'ensemble des organes de l'entité.</p> <p>La capacité des métiers à s'approprier le nouvel outil et à l'utiliser dans les meilleures conditions.</p>

Documents à consulter :



Comptes rendus et décisions des différentes instances (coordination, inspection, évaluation)

Tableaux RH et plans de formation

Analyses préalables au déploiement des dispositifs

Comptes rendus et décisions des instances de suivi des projets

Indicateurs et tableaux de bord / Critères d'évaluation

Audits (internes et externes)

Pour en savoir plus

Rapport de la Cour des Comptes- [La conduite des grands projets numériques de l'État](#) (Octobre 2020):

« À la demande de la commission des finances du Sénat, la Cour des comptes a enquêté sur la conduite des grands projets numériques de l'État. Celle-ci a connu ces dernières années des réussites notables, comme le prélèvement à la source, mais aussi des échecs retentissants, notamment dans le domaine de la gestion des ressources humaines. Une cinquantaine de grands projets numériques sont actuellement suivis par la direction interministérielle du numérique Dinum, chacun pour un coût supérieur à 9 M€. Les bonnes pratiques en matière de conduite de projets restent trop souvent méconnues, alors que l'inadaptation des trajectoires des projets et de leur gouvernance, l'insuffisance du financement et des moyens humains ou encore la nécessité d'une responsabilité unique en gestion de projet sont régulièrement relevées. Les réorganisations en cours au sein des ministères doivent permettre de mieux maîtriser les enjeux techniques et de veiller à la satisfaction des besoins des usagers et des agents. Les mutualisations entre ministères doivent être encouragées. Des mesures sont également indispensables côté RH pour se doter des profils nécessaires et mieux former les cadres dirigeants. La Cour formule au total 11 recommandations pour la réussite de la transformation numérique du service public. »

AXE 3 – CONTROLER LES PROJETS INNOVANTS

L'innovation est la recherche constante d'améliorations de l'existant, par contraste avec l'invention, qui vise à créer du nouveau. Elle permet à une entité d'augmenter sa productivité, d'améliorer la qualité de ses produits ou de ses services et de développer des compétences clés.

Bien que les projets d'innovation peuvent s'auditer par le même biais que les autres projets (voir axe 2), il existe quelques particularités qui sont développées dans cette fiche.

Les enjeux pour l'organisme

- ▶ Garantir la capacité d'évolution de l'organisme
- ▶ Pouvoir identifier et décliner les opportunités de nature technologique
- ▶ Créer les conditions favorables au développement d'innovations : veille technologique, parangonnage, lab, open innovation, etc.

Les risques

- ▶ Manque d'attractivité RH (recrutement, départs, turnover ...) et de compétences adéquates pour faire face aux évolutions technologiques
- ▶ Manque d'avantage concurrentiel et défaut d'image de l'organisme
- ▶ Absence d'organisation adaptée à l'innovation

Questionnements

Stratégie d'innovation

- ▶ Existe-t-il une stratégie formalisée en matière d'innovation ?
- ▶ Est-elle cohérente avec la stratégie globale de l'organisme ?
- ▶ Une veille technologique et réglementaire est-elle réalisée? Quel(s) service(s) en sont chargés ?

Moyens humains et financiers

- ▶ Les projets d'innovation ont-ils un financement séparé des projets standards ? Comment est organisé le suivi des coûts des projets d'innovation ?
- ▶ Les initiatives d'innovation bénéficient-elles de ressources internes ou externes (financières, humaines, etc.) permettant d'aboutir à des projets finis ?

Pour aller vers l'observation

Conclure sur :


L'existence et l'efficacité de dispositifs innovants au sein de l'entité.



Point d'attention

Même si l'innovation peut procurer de nombreux avantages, sa rentabilité ou finalité étant incertaine, elle est également un risque majeur pour l'entité. Elle s'inscrit dans la stratégie à long terme de l'entité.

L'analyse effectuée sur la base des différents critères d'évaluation permet de déterminer l'impact de la nouveauté de ces projets sur l'organisation de l'entité et sur son efficacité vis-à-vis du service au citoyen.

Questionnements	Pour aller vers l'observation
<p>Pilotage des projet d'innovation</p> <ul style="list-style-type: none">▶ Quelle comitologie et quels indicateurs sont mis en place afin de piloter les projets innovants ?▶ La DSI a-t-elle été associée aux analyses préalables et à la décision finale liée aux dispositifs d'innovation?▶ La correcte intégration des projets innovants dans le SI de l'entité a-t-elle été prévue ? <p>Retours et lien avec la stratégie globale</p> <ul style="list-style-type: none">▶ S'il existe plusieurs dispositifs de projets innovants, travaillent-ils de manière indépendante ou existe-t-il une feuille de route transversale construite à partir de la stratégie d'innovation ? Si oui, des retours sont-ils effectués au sein de l'entité ? <p>Travail collaboratif</p> <ul style="list-style-type: none">▶ Des espaces d'innovation ont-ils été mis en place à destination de l'ensemble des agents ? Si oui, quels sont-ils (environnements ou temps dédiés, pour les activités d'innovation, etc.) ? <p>Vers l'extérieur</p> <ul style="list-style-type: none">▶ L'entité a-t-elle entrepris une démarche de collaboration avec différents instituts de recherche, des établissements d'enseignement supérieur, chercheurs, associations? Si oui, pour quel type de projet ? Quelles sont les modalités de cette collaboration ?	<p>Conclure sur :</p> <p>L'intégration des projets innovants à la stratégie et au schéma directeur de l'organisation.</p> <div data-bbox="847 468 1460 936" style="border: 1px solid black; padding: 10px;"><p> Point d'attention</p><p>L'innovation peut être développée en parallèle des équipes propres à l'organisation. On peut citer par exemple le recours aux entrepreneurs d'intérêt général (EIG) ou à des hackathons ainsi que la collaboration avec des startups d'état ou des laboratoires d'innovation. Ces projets sont alors développés en mode pilote. Le contrôle devra s'assurer du pilotage de l'organisme sur ces projets ainsi que de sa possible intégration dans le SI de l'entité.</p></div> <p>Conclure sur :</p> <p>L'acculturation à l'innovation au sein de l'entité.</p> <p>Les retours d'expériences de l'ensemble des collaborateurs.</p> <p>Conclure sur :</p> <p>La qualité et la plus-value de la collaboration avec les instituts de recherche et les différents dispositifs d'innovation.</p>

Documents à consulter :



- Stratégie d'innovation formalisée
- Liste des projets innovants
- Liste des démarches (partenariats ou actions) permettant l'innovation
- Plans de formation

FICHE 4 – LA PRODUCTION INFORMATIQUE

PRESENTATION

La production informatique (cf. [annexe 2](#) – RUN ou Exploitation/maintenance) est un service à géométrie variable suivant l'organisation de la DSI de l'organisme. Ce service regroupe l'ensemble des méthodes et compétences nécessaires pour :

- Exploiter une infrastructure matérielle et logicielle répondant aux besoins opérationnels définis par les directions utilisatrices.
- Superviser efficacement l'exploitation et résoudre les incidents d'exploitation.
- Gérer les sauvegardes et les reprises en cas d'incident, afin d'assurer la continuité d'exploitation.

Un audit plus approfondi, demandant une expertise technique en audit SI, consisterait de façon non exhaustive à s'assurer de la maîtrise par l'organisme des enjeux suivants :

- Définir des architectures systèmes homogènes et cohérentes.
- Assurer un dimensionnement des matériels en adéquation avec les risques et objectifs de continuité d'activité.
- Optimiser les systèmes et les bases de données.

LES RISQUES

- Indisponibilité du SI (pouvant aller jusqu'à une perte de continuité d'activité).
- Détérioration des temps de réponse du SI.
- Perte ou corruption de données sensibles.
- Perte de maîtrise de l'exploitation.
- SI non fiable.
- SI ne répondant pas aux besoins métier.

LES OBJECTIFS

Les objectifs de cette fiche sont de permettre :

- De vérifier que les **objectifs de la production** sont bien définis et que le **suivi de la performance** est satisfaisant (**axe 1**).
- De contrôler la **pertinence de l'organisation** mise en place permettant d'atteindre ces objectifs (**axe 2**).
- De s'assurer que les **procédures de gestion de l'exploitation** sont satisfaisantes et que le **dispositif de gestion des incidents** est pertinent et efficace (**axe 3**).
- De contrôler les **mesures prises pour assurer la continuité de l'activité** : plan de continuité de l'activité, gestion des sauvegardes et de la reprise (**axe 4**).

AXE 1 – VERIFIER LES OBJECTIFS DE LA PRODUCTION ET LE SUIVI DE LA PERFORMANCE

Enjeux pour l'organisme

- ▶ Définir les niveaux de service attendus par la production informatique au regard des besoins opérationnels du système d'information (disponibilité, intégrité et confidentialité)
- ▶ Mettre en œuvre un dispositif de suivi de la performance de la production

Risques

- ▶ SI non aligné avec les besoins des utilisateurs
- ▶ Perte de la continuité d'activité du SI
- ▶ Indisponibilité du SI
- ▶ Perte de maîtrise de l'exploitation



Bonnes pratiques

La production doit disposer d'objectifs clairs et d'indicateurs de performance simples et mesurables (qui peuvent être formalisés dans des conventions de services), définis et validés par l'ensemble des parties prenantes (DSI, directions métier et prestataires externes dans le cas de services externalisés).

Sur la base de ces objectifs et de ces indicateurs, des instances de suivi de la performance et des outils doivent être mis en place (reporting, tableaux de bord, etc.), ainsi que des reportings réguliers auprès des directions utilisatrices.

Questionnements

Objectifs de la production

- ▶ Les objectifs assignés à la production sont-ils clairement définis ? Notamment, les enjeux de disponibilité, d'intégrité et de confidentialité des différents systèmes ?
- ▶ Ces objectifs sont-ils définis de façon globale ou différenciée pour les applications les plus critiques ?
- ▶ Des indicateurs simples et mesurables ont-ils été associés à ces objectifs et formalisés ?
- ▶ Comment cette démarche a-t-elle été menée ?
 - Les directions métiers ont-elles été associées ?
 - Quelle est la fréquence de révision des objectifs et des indicateurs associés ?
- ▶ En fonction de la taille de la structure et de la présence ou non d'une externalisation :

Pour aller vers l'observation

Conclure sur :

La cohérence de la méthodologie utilisée pour définir, valider et diffuser les objectifs et indicateurs par rapport aux enjeux de la structure.

La pertinence des indicateurs fixés au regard des objectifs définis.

Questionnements

- Les objectifs et indicateurs font-ils l'objet de documents contractuels entre la production et les directions métier (conventions de services, contrats de prestation par exemple) ?
- Ces documents sont-ils cohérents avec les objectifs et les indicateurs définis ?

Suivi de la performance

- Existe-t-il un suivi organisé et planifié des conventions de services et/ou des indicateurs de performance ? Notamment :

- *Quels sont les instances permettant de suivre la performance de la production ?*
- *Quelle est la fréquence des réunions ?*

- Quels sont les outils permettant de suivre la performance de la production ? Sont-ils automatisés ou alimentés manuellement ?
- Comment sont formalisés les résultats (reporting, tableaux de bord, etc.) ?

Le cas échéant, obtenir les tableaux de bords de production et juger de leur pertinence aussi bien que de leur complétude.

- En cas de non-respect des objectifs assignés à la production, est-ce que des actions correctrices sont décidées ? Par qui ? Le cas échéant, qui est en charge de les suivre ?

Pour aller vers l'observation



Point d'attention

Traditionnellement un engagement du service production sur le niveau de service attendu se retrouve au sein de conventions¹ de services et de plans d'assurance qualité (PAQ). Cela s'applique non seulement dans le cadre d'une prestation externalisée mais aussi dans le cas d'une production interne.

Les conventions de services ne s'entendent pas comme un ensemble unilatéral de responsabilités de la production mais comme un ensemble de règles régissant les rapports entre la production et les directions utilisatrices.

Conclure sur :

La robustesse du dispositif mis en place pour suivre les objectifs et indicateurs définis en amont.

Conclure sur :

La pertinence et le suivi des actions correctrices engagées en cas d'écarts par rapport aux niveaux de service attendus.

Documents à consulter :



Objectifs formalisés assignés à la production
Conventions de service entre la production et les directions métier
Indicateurs de performance formalisés
Comptes rendus de réunion d'instances de pilotage de la production
Reporting et tableaux de bord de la production

¹ On trouve souvent le terme anglais de Service Level Agreement (SLA)

AXE 2 – CONTROLER L'ORGANISATION MISE EN PLACE AUTOUR DE LA FONCTION DE PRODUCTION

Enjeux pour l'organisme

- ▶ Mettre en œuvre une organisation adaptée permettant de respecter les engagements de service de la production
- ▶ Disposer de compétences spécialisées couvrant l'ensemble des besoins techniques liés à la production

Risques

- ▶ SI non aligné avec les besoins des utilisateurs
- ▶ Perte de maîtrise de l'exploitation



Bonnes pratiques

La production doit être indépendante du département des études, en charge des évolutions informatiques. Les compétences et l'organisation des équipes doivent être en lien avec les caractéristiques techniques du SI et les missions assignées à l'équipe de production. Des procédures doivent être formalisées.

Questionnements

Organisation

▶ Comment est-organisée la production ?

- ❖ *Il convient notamment de valider l'indépendance de la production par rapport au service en charge des études.*

▶ Existe-t-il une bonne maîtrise des différentes missions de la production ?

- ❖ *Identifier le périmètre couvert par la production et en déduire les principales missions assurées. Valider que les descriptions de postes couvrent ces différentes missions.*

▶ Existe-il une description des rôles et responsabilités de chaque membre de la production (découpage par application, par technologie, par type de support – 1^{er}, 2^e, 3^e niveau – cf. 'Pour en savoir plus' ci-après) ?

Pour aller vers l'observation

Conclure sur :

La cohérence de l'organisation et les compétences techniques du personnel en fonction des enjeux et des objectifs assignés à la production.

Questionnements

Pour aller vers l'observation

- ❖ *Il convient alors d'apprécier si l'organisation de la production est adaptée aux objectifs opérationnels de l'organisme décrits dans l'axe 1, notamment les enjeux de disponibilité, de sécurité et d'intégrité.*

► Existe-t-il des risques de pertes de compétences sur les technologies/applications clés (personnes clés sans suppléance) ?

► Quel est le patrimoine documentaire (dossier d'exploitation, gestion des sauvegardes, procédures, séquençement des tâches, points de reprise...) utilisé par le service d'exploitation ? Est-il à jour ?

Documents à consulter :



Organigramme de la production
Description du rôle et des responsabilités du personnel de la production
Grille croisée de compétences/individus
Support de formation du personnel de la production
Procédures d'exploitation
Comptes rendus d'exploitation

Pour en savoir plus

En fonction de la taille et de la criticité de la structure on trouve au sein de la production des profils spécialisés outre les responsables de départements (exploitation, systèmes et réseaux) :

- des pupitreurs ou opérateurs de production ;
- des Ingénieurs systèmes et réseaux ;
- des administrateurs de bases de données (DBA), systèmes et réseaux ;
- des analystes d'exploitation (en charge de la préparation, de la planification, du lancement et du contrôle des traitements).

Se référer à [l'annexe 2](#)

AXE 3 – EVALUER LES PROCEDURES DE GESTION DE L'EXPLOITATION ET LE DISPOSITIF DE GESTION DES INCIDENTS

Enjeux pour l'organisme

- ▶ Assurer la supervision des tâches d'exploitation en fonction des niveaux de services attendus
- ▶ Mettre en place un dispositif pour détecter et corriger les incidents de production

Risques

- ▶ Perte de la continuité d'activité du SI
- ▶ Indisponibilité du SI
- ▶ Fiabilité du SI (en cas d'incidents non résolus)



Bonnes pratiques

Une exploitation sous contrôle se caractérise par :

- des procédures d'exploitation exhaustives, à jour et comportant une description précise des actions à mener en cas de problème ;
- un système de remontée d'alerte permettant l'identification et la qualification d'incidents de production ;
- un dispositif d'escalade couvrant l'ensemble des besoins en cas de problème ;
- idéalement, l'existence d'astreintes de production.

La typologie des incidents et leur gravité (en fonction de critères précis) doivent être explicitement définis. Les délais de résolution attendus en fonction de la gravité nécessitent d'être formalisés en accord avec les conventions de services passées entre la DSI et les directions utilisatrices du SI.

Il est recommandé qu'un comité de suivi des incidents (incluant le cas échéant les MOA concernées par les incidents fonctionnels) analyse régulièrement la situation des incidents non résolus.

Questionnements

Supervision de l'exploitation

- ▶ Les outils utilisés permettent-ils une bonne supervision de l'exploitation ?

❖ *Incluant notamment les éléments suivants :*

- *Les alertes sont remontées en temps réel à la console d'administration de la production.*
- *Les applications et les systèmes opérés génèrent des fichiers d'erreurs exploitables.*
- *Les outils systèmes offrent des garanties de retour en arrière si un traitement est interrompu.*

Pour aller vers l'observation

Conclure sur :

La supervision des tâches d'exploitation.

La gestion correcte des incidents (notamment le respect des engagements de service attendus).

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none">▶ Existe-t-il une astreinte pendant les traitements de nuit ?▶ Existe-t-il un outil traçant tout événement anormal survenu et les actions correctives entreprises ?	

Gestion des incidents

- ▶ Existe-t-il un **référentiel/ une procédure** de gestion des incidents ?

❖ *Précisant :*

- *les typologies d'incidents ;*
- *une échelle de gravité (exemple : critique, urgent, important, faible etc..) en fonction de critères définis (indisponibilité du système, impact potentiel, urgence, etc.) ;*
- *les délais de résolutions attendus ;*
- *les actions de résolution à entreprendre et notamment les procédures d'escalade.*

- ▶ Quels sont les outils utilisés pour recenser et suivre la résolution des incidents ?

❖ *Mentionnant entre autres la date de l'incident, description, gravité, statut (en cours, fermé, abandonné, résolu, etc.), demandeur, personne en charge de la résolution, modalité de résolution, etc.*

- ▶ Des tableaux de bord des incidents sont-ils élaborés ? A qui sont-ils communiqués et à quelle fréquence ?



Point d'attention

La gestion des problèmes est un processus complémentaire à celui de la gestion des incidents, visant à analyser les causes fondamentales de certains incidents, notamment ceux récurrents, pour éviter que ceux-ci ne se reproduisent.

Gestion des problèmes (cf. point d'attention)

- ▶ Existe-t-il un dispositif de gestion des problèmes ?

Documents à consulter :



Procédures de gestion des incidents
Comptes rendus de comités de suivi des incidents
Tableaux de bord des incidents
Procédures de gestion des problèmes et tableaux de bord des problèmes

AXE 4 – CONTROLER LES MESURES PRISES POUR ASSURER LA CONTINUITE DE L'ACTIVITE

La continuité d'activité correspond à la capacité d'un organisme (entreprise ou administration) à poursuivre son fonctionnement et l'atteinte de ses objectifs à un niveau acceptable défini par avance, suite à la survenance d'un évènement perturbateur.

Enjeux pour l'organisme

- ▶ Assurer la continuité de l'activité
- ▶ Mettre en œuvre un dispositif de sauvegarde permettant la reprise du SI en cas de problème
- ▶ Mettre en place des procédures de tests réguliers, des sauvegardes et de restauration des systèmes

Risques

- ▶ Absence de continuité (partielle ou totale) du système d'information en cas de sinistre survenant sur le SI
- ▶ Perte de données (en cas de mauvaise sauvegarde ou sauvegarde incomplète)



Bonnes pratiques

Un plan de continuité de l'activité^{GI} (PCA) doit être formalisé et testé au sein de l'entité. Il décrit la stratégie de continuité adoptée pour faire face, par ordre de priorité, à des risques identifiés et sérieux selon la gravité de leurs effets et leur plausibilité. Il décline cette stratégie en termes de ressources, d'organisation et de procédures documentées.

Le PCA doit définir des indicateurs d'objectifs par exemple à travers la quantité maximale de données perdues acceptable par l'entreprise (Recovery Point Objective – RPO exprimé en intervalle de temps) et la durée maximale d'interruption acceptable entre le moment de la notification de l'incident et la reprise normale du service. (Recovery Time Objective – RTO). Ces objectifs doivent être cohérents avec la stratégie de sauvegarde de l'organisme.

Les procédures de sauvegarde du SI doivent être dûment documentées et scrupuleusement appliquées par des acteurs identifiés et responsables.

Idéalement, l'organisme doit disposer d'outils permettant une automatisation des sauvegardes et comportant des fonctions de diagnostic remontant des alertes en cas de problèmes d'exécution.

Un plan de test de restauration des systèmes doit être réalisé régulièrement pour assurer la fiabilité des procédures de sauvegarde et la capacité à reconstituer le système à partir des données sauvegardées. Les organismes doivent *a minima* disposer des sauvegardes suivantes :

- une sauvegarde quotidienne de toutes les applications (données, programmes, paramètres) conservée 7 jours, externalisée sauf pour la sauvegarde la plus récente conservée sur site mais hors du local où sont stockés les serveurs ;
- une sauvegarde hebdomadaire complète (incluant les sauvegardes des systèmes d'exploitation) externalisée et conservée pendant 5 semaines ;
- une sauvegarde mensuelle complète, conservée 12 mois ;
- une sauvegarde annuelle de tous les systèmes contribuant à établir le résultat fiscal, conservée au minimum 3 ans (plus en cas d'exercices déficitaires).

Questionnements

Plan de continuité

- ▶ Un plan de continuité a-t-il été formalisé ? Est-il validé par la direction de l'organisme ?
- ▶ Les moyens de secours et de repli sont-ils suffisamment dimensionnés pour assurer les besoins de continuité validés ?
- ▶ La documentation est-elle suffisante ?
- ▶ Ce plan est-il régulièrement communiqué, testé et évalué ?

Procédures de sauvegarde

- ▶ Les procédures de sauvegarde ont-elles été définies et formalisées ? Répondent-elles aux besoins et objectifs (RPO-RTO) ?

Valider que les éléments suivants font partie intégrante *a minima* des procédures de sauvegarde :

- un plan de sauvegarde identifiant par serveur / application, le périmètre de sauvegarde (fichiers, programmes, paramètres, systèmes d'exploitation, etc.) et la cyclicité ;
- les acteurs (personnel, système de sauvegarde) en charge de la réalisation et du contrôle des sauvegardes ;
- des clauses de révision des procédures de sauvegardes et des périmètres, en fonction des évolutions du SI (nouvelle livraison applicative, changement de serveur, etc.)

Dispositif de restauration

- ▶ Vérifier qu'il existe des procédures de restauration précisant les modalités selon lesquelles on peut remonter partiellement ou totalement un système en partant des sauvegardes ? Ces procédures de restauration couvrent-elles les systèmes les plus sensibles ?
- ▶ Le planning prévisionnel de tests de restauration est-il correctement suivi ?

Pour aller vers l'observation

Conclure sur :

La cohérence du plan de continuité de l'activité.



Point d'attention

En amont du sinistre, plusieurs actions sont nécessaires pour satisfaire les exigences relatives à la gestion de la continuité d'activité :

- L'engagement de la direction vis-à-vis du programme de gestion de la continuité d'activité.
- Procéder à une évaluation du risque de non-continuité d'activité et réduire ce risque.
- Procéder à une analyse d'impact.
- Définir les stratégies de continuité et de reprise d'activité au travers 4 principales composantes :
 - * une organisation de gestion de crise ;
 - * un système documentaire éprouvé et mis à jour ;
 - * une stratégie de sauvegarde efficace et testée ;
 - * une solution technique de secours qui couvre les besoins de continuité et qui est testée.

L'efficacité du processus de sauvegarde et de récupération des données.



Point d'attention

Les sauvegardes du système d'information sont indispensables pour restaurer le système d'information de façon complète ou partielle en cas de grave incident. Toutefois, les sauvegardes peuvent s'avérer incomplètes (oubli de certains fichiers, paramètres manquants, etc.). Des tests réguliers sont nécessaires pour vérifier la complétude des sauvegardes.

Documents à consulter :



Plan de continuité de l'activité
Procédures et résultats des tests relatifs au PCA
Procédures de sauvegarde
Comptes rendus de l'exécution des sauvegardes
Documentation relative aux sauvegardes et aux tests de restauration
Comptes rendus des tests de restauration

Pour en savoir plus

[Guide d'audit de la continuité de l'activité d'un organisme](#)

[Cahier de recherche de l'IFACI sur l'audit des plans de continuité](#)

[Guide pratique](#) sur la gestion de la continuité de l'activité

[Guide pour réaliser un plan de continuité de l'activité](#)

Différents mécanismes de sauvegarde peuvent être mis en place au sein des organismes.

Mécanisme	Principe
Sauvegarde complète	Elle consiste à enregistrer le périmètre total des données à sauvegarder que celles-ci soient récentes, anciennes, modifiées ou non. Cette méthode s'avère peu adaptée à un usage professionnel car elle est à la fois très longue et très lourde en espace de stockage.
Sauvegarde incrémentale	Elle se concentre sur les fichiers modifiés depuis la dernière sauvegarde complète, elle est donc un peu plus rapide que la sauvegarde complète mais également coûteuse en espace de stockage dans la mesure où toute restauration nécessite de faire appel à la dernière sauvegarde complète.
Sauvegarde différentielle	C'est la plus évoluée et la plus efficiente des méthodes mais elle nécessite une parfaite maîtrise technique de l'éditeur. Le logiciel se focalise sur les éléments modifiés depuis la dernière opération de sauvegarde. Il peut s'agir des fichiers modifiés ou même des blocs de données modifiés à l'intérieur même des documents.

FICHE 5 – LES DONNEES

PRESENTATION

Les données sont la représentation d'informations stockées sous différentes formes (textes, vidéos, images, sons, chiffres, etc.) dans un programme (base de données, logiciel, site internet, répertoire réseau, etc.)

Les données sont un des actifs les plus précieux d'une organisation. Elles sont au cœur des systèmes d'information : elles permettent d'aboutir à une action ou à un traitement qui produit de la valeur ajoutée pour l'entité.

Le cycle de vie de la donnée peut être décomposé en cinq étapes principales: la collecte, le stockage, le partage, l'analyse, et la suppression. Il convient d'analyser les risques associés à chacune de ces étapes afin d'assurer **la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT)** des données (cf. [fiche 6](#)).

LES RISQUES

Les risques relatifs aux données sont de manière non exhaustive :

- L'indisponibilité et/ou la perte de la donnée.
- Les accès inappropriés aux données pouvant conduire à une utilisation ou une divulgation non autorisée.
- L'altération de la donnée.
- La mauvaise qualité des données.
- La non-traçabilité des accès à la donnée et des modifications éventuelles.

LES OBJECTIFS

Les objectifs de cette fiche sont de vous permettre :

- D'évaluer la maîtrise de **la classification de la donnée (axe 1)**.
- De vérifier l'opérabilité **des contrôles de la qualité des données (axe 2)**.
- D'évaluer **la disponibilité de la donnée** (à travers les politiques de sauvegarde, de récupération et d'archivage) **(axe 3)**.
- De vérifier **la sécurisation des traitements de la donnée (axe 4)**.

AXE 1 – EVALUER LA MAITRISE DE LA CLASSIFICATION DE LA DONNEE

Les enjeux pour l'organisme

- ▶ Inventorier les données
- ▶ Classer les données en fonction de leur sensibilité et de leur cycle de vie
- ▶ Recenser les équipements qui hébergent des données

Les risques

- ▶ Insuffisante sécurisation des données due à une mauvaise connaissance du système d'information



Bonnes pratiques

Les données doivent être classifiées selon leur sensibilité :

- public : la donnée peut être diffusée à l'extérieur de l'organisation ;
- interne : la donnée ne doit pas être diffusée à l'extérieur de l'organisation et peut être accessible par l'ensemble des collaborateurs ;
- confidentiel : la donnée doit être protégée pour n'être accessible que par un nombre restreint de personnes. Sa divulgation pourrait entraîner des conséquences graves pour l'organisme.

L'entité doit mettre en place un inventaire des données c'est à dire un référentiel qui liste l'ensemble des données produites ou utilisées par l'organisme et qui précise pour chacune d'entre elle sa description, sa confidentialité, les applications où elle est hébergée, sa durée de vie, son mécanisme de conversation, son propriétaire, etc. Cet inventaire est mis à jour *a minima* annuellement ([cf. fiche RGPD](#)).

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none">▶ L'organisme a-t-il mis en place une classification des données ? Cette classification couvre-t-elle l'exhaustivité du système d'information (documents, courriels, impressions, etc.) ?	<p>Conclure sur :</p> <p>La mise en œuvre d'une politique de classification des données couvrant l'exhaustivité du système d'information</p>
<ul style="list-style-type: none">▶ L'organisme a-t-il mis en place un inventaire des données, le revoit-il régulièrement pour l'enrichir et le mettre à jour ?	<p>L'établissement d'un inventaire des données à jour et exhaustif</p>
<ul style="list-style-type: none">▶ L'organisme a-t-il recensé l'ensemble des équipements (ex : bases de données, serveurs, disques, applications, etc.) y compris externes (ex : cloud) qui hébergent des données ? Cf. fiche 2- axe 5	<p>Le recensement des équipements internes et externes à l'organisation qui hébergent des données</p> <p>La gouvernance autour de la donnée en termes d'organisation, de comités, de rôles et de responsabilités</p>

Questionnements

Pour aller vers l'observation

- L'organisation a-t-elle mis en place une gouvernance autour de la donnée afin de définir le rôle et les responsabilités de chaque partie prenante ?



Point d'attention

Les données accessibles par des partenaires et/ou hébergées à l'extérieur du système d'information de l'entité (ex : cloud) doivent faire l'objet de contrôles renforcés.

Documents à consulter :



Politique de classification des données et du cycle de vie des données
Inventaire des données et recensement des hébergements associés

Pour en savoir plus

Tableau [classifiant la sensibilité des données et la réglementation applicables](#) par type d'entité, ANSSI

AXE 2 – S'ASSURER DE LA QUALITE DES DONNEES

Les enjeux pour l'organisme

- ▶ Assurer la qualité des données tout au long du cycle de vie de la donnée
- ▶ Améliorer le service rendu aux utilisateurs du système d'information

Les risques

- ▶ Données non fiables, incohérentes ou non exploitables dans le système d'information



Bonnes pratiques

Les données sont utilisées, traitées et hébergées au sein d'applications informatiques. Les applications doivent embarquer des contrôles qui imposent des champs obligatoires (exemple : un nom, un prénom, une adresse) et vérifient les saisies des utilisateurs (exemple : un champ « date de naissance » ne peut accepter que des chiffres) afin de limiter les revues manuelles *a posteriori* sur les données.

Les revues manuelles peuvent porter sur la complétude et la fiabilité des champs renseignés (par exemple le nombre d'utilisateurs ayant une adresse courriel renseignée) mais également permettent de vérifier leur crédibilité vis-à-vis de sources externes (par exemple les adresses clients avec les référentiels INSEE ou la Poste).

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

- ▶ L'organisme a-t-il mis en place des contrôles embarqués^{GI} dans ses applications pour contrôler les données saisies par les utilisateurs?

- ▶ L'organisme (ou le CAC assigné) revoit-il régulièrement les données de son système d'information pour vérifier la complétude et identifier les erreurs afin d'en améliorer la qualité ? [Cf. fiche 2, axe 2](#)

- ▶ L'organisation a-t-elle automatisé ses processus afin de limiter les saisies manuelles, les ressaisies d'un système à un autre et les saisies doubles ?

- ▶ L'organisme a-t-il défini un cycle de vie des données et pris des mesures cohérentes pour assurer la qualité de celles-ci tout au long du cycle ?

Conclure sur :

La mise en place de contrôles embarqués

Les revues manuelles effectuées pour vérifier la complétude et la fiabilité des champs

La définition d'un cycle de vie des données et les contrôles relatifs à la qualité tout au long du cycle



Point d'attention

Les données qui proviennent d'une source externe et qui ne sont pas produites par le système d'information de l'organisme doivent faire l'objet de contrôles renforcés.

Documents à consulter :



Gouvernance de la donnée (politique, organisation, comités)

Liste des contrôles embarqués dans les applications

Extraction des bases de données pour vérifier la complétude et la fiabilité des champs

AXE 3 – EVALUER LA DISPONIBILITE DE LA DONNEE

Les enjeux pour l'organisme

- ▶ Assurer la disponibilité de la donnée en fonction des besoins de l'entité
- ▶ Sauvegarder la donnée pour garantir un mécanisme de secours en cas d'incident
- ▶ Assurer l'authenticité, l'intégrité et la fiabilité des données
- ▶ Gérer le cycle de vie : conserver et détruire la donnée lorsque c'est nécessaire

Les risques

- ▶ Donnée indisponible et/ou non récupérable car non sauvegardée
- ▶ Non-respect de la durée légale d'archivage
- ▶ Vol de données au moment de la destruction



Bonnes pratiques

La réplication de la donnée consiste à copier la donnée à plusieurs endroits du système d'information afin d'en garantir la disponibilité à tout moment. La réplication peut s'effectuer à plusieurs niveaux : au niveau des serveurs, des bases de données ou des disques.

L'archivage garantit la qualité des données en capitalisant sur les données originales (authenticité), n'ayant pas été altérées (intégrité) et dont le contenu est à jour (fiabilité) (Référence : Norme ISO15489 sur le 'Records management').


Questionnements

- ▶ L'organisme a-t-il mis en place un mécanisme de réplication de la donnée pour assurer la disponibilité de celle-ci à tout moment ?
- ▶ L'organisme a-t-il mis en place un mécanisme de sauvegarde ? Si oui, celui-ci est-il testé à fréquence régulière et validé par les métiers ? cf. [fiche 4-, axe 4](#)

Pour aller vers l'observation

Conclure sur :

- L'existence et l'efficacité des mécanismes de :
- réplication,
 - sauvegarde,
 - archivage,
 - et destruction de la donnée.

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none">▶ L'organisme a-t-il mis en place une politique d'archivage régissant le cycle de vie des informations (durées de conservation, sorts finaux) ? Comment cette politique est-elle mise en œuvre (cf. annexe 6 sur l'archivage) ? ▶ Comment l'organisme s'assure-t-il que les données sont intégralement détruites ? A-t-elle mis en place des circuits séparés de destruction pour les informations sensibles et non sensibles ?	<p>Conclure sur :</p> <p>Le mécanisme d'archivage.</p> <div data-bbox="815 611 1428 936" style="border: 1px solid black; padding: 10px;"><p> Point d'attention</p><p>Certains organismes font appel à des sociétés extérieures pour détruire physiquement leur donnée stockée sur des disques durs. Cette externalisation doit être surveillée afin d'assurer la protection de la donnée et de se garantir contre le vol de données.</p></div>

Documents à consulter :



Politique de sauvegarde, d'archivage et de destruction de la donnée
Schéma d'architecture de réplication de la donnée
Procès-verbal (PV) des destructions de données

Pour en savoir plus

Il existe différents mécanismes de sauvegarde qui peuvent être mis en place au sein des organismes (cf. [fiche 4, axe 4](#)).

AXE 4 – VERIFIER LA SECURISATION DES TRAITEMENTS DE DONNEES

Les enjeux pour l'organisme

- ▶ Favoriser l'interopérabilité des applications
- ▶ Partager les données avec des acteurs externes
- ▶ Sécuriser les opérations à risque
- ▶ Assurer l'efficacité des traitements
- ▶ Réparer les erreurs

Les risques

- ▶ Traitements de données en erreur, n'ayant pas abouti
- ▶ Transferts de données non sécurisées qui rendent possible la divulgation non autorisée



Bonnes pratiques

La DSI doit établir et mettre régulièrement à jour son plan d'architecture et d'urbanisation du système d'information ([cf. fiche 2, axe 1](#)). Elle cherche à favoriser les échanges inter-applicatifs pour créer de la valeur, à supprimer les redondances entre applications (applications assurant les mêmes fonctionnalités) et à remplacer les composants ou applications devenus obsolètes ([cf. fiche 2, axe 2](#)). Les transferts de données mis en place entre les différentes applications doivent être sécurisés par des mécanismes et surveillés à fréquence régulière pour vérifier leur bon fonctionnement.

Questionnements

- ▶ L'organisme a-t-il établi un plan d'architecture et d'urbanisation du système d'information ? Si oui, l'organisme a-t-il défini une architecture cible vers laquelle tendre ? [cf. fiche 2, axe 1](#)
- ▶ L'organisme a-t-il sécurisé les transferts de données inter-applicatifs et inter-systèmes d'information (en interne pour l'intégrité et en externe pour la sécurité) ?
- ▶ Les traitements automatisés sont-ils surveillés quotidiennement afin de détecter les traitements en erreur ?

Pour aller vers l'observation

Conclure sur :

La pertinence du plan d'architecture, du plan d'urbanisation et de l'architecture cible définis (échanges inter-applicatifs à développer, applications à remplacer ou à supprimer, etc.).

La confidentialité et la sécurité des données partagées avec des acteurs externes.

Les mécanismes utilisés pour transférer la donnée d'une application vers une autre ou d'un système d'information vers un autre.

Le nombre de traitements automatisés et le nombre de traitements en erreur sur une année.

Questionnements

- ▶ Les traitements en erreur, n'ayant pas abouti, font-ils l'objet de créations automatiques d'incident ?
- ▶ L'organisme a-t-il défini une politique d'ouverture de données (cf. pour en savoir plus) ? Si oui, l'organisme a-t-il pris le soin de retirer les informations sensibles et confidentielles et de normaliser la donnée ?

Pour aller vers l'observation



Point d'attention

Les transferts de données peuvent altérer l'intégrité des données. Les organismes doivent donc mettre en place des mécanismes qui permettent d'assurer que la donnée initiale, avant transfert, n'a pas été modifiée durant le transfert. Un des mécanismes consiste à utiliser des fonctions de « hashage » qui permettent de vérifier que la donnée transférée est identique à la donnée originale à l'aide d'une empreinte numérique.

Documents à consulter :



Plan d'architecture et d'urbanisation du système d'information
Politique interne d'ouverture des données (open data^{GI}, etc.)

Schéma des flux inter-applicatifs

Liste des traitements placés dans l'ordonnanceur^{GI}

Liste des traitements en erreur, n'ayant pas abouti, sur une année glissante

Pour en savoir plus

- Etude sur le [cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales](#)
- **L'ouverture des données^{GI}**

La France s'est engagée dans une démarche d'ouverture des données publiques. Elle a signé en 2013 la « [charte du G8 pour l'ouverture des données publiques](#) », puis rejoint en 2014 le [partenariat pour un gouvernement ouvert](#). Désormais, **les données publiques doivent être ouvertes par défaut**.

Plus concrètement l'article [L. 322-6](#) du code des relations entre le public et l'administration impose aux administrations de tenir un répertoire des principaux documents contenant des informations publiques qu'elles produisent ou détiennent et d'en publier en ligne chaque année une version mise à jour. L'article [L. 312-1-1](#) du même code prévoit que toute administration (Etat, collectivités ou structures chargées d'exploiter un service public) de plus de 50 agents et de plus de 3500 habitants, est désormais dans l'obligation de diffuser, dans un standard ouvert et aisément diffusable, les documents et données suivantes :

- les documents communiqués à la suite d'une demande d'accès,
- les documents figurant dans les répertoires d'informations publiques,
- les bases de données mises à jour de façon régulière,
- les données, mises à jour de façon régulière présentant un intérêt économique, social, sanitaire ou environnemental.

Plus d'information sur [Data.gouv.fr](#) : plateforme ouverte des données publiques françaises

- **Protection des données**

Règles de [sauvegarde des Systèmes d'Information de Santé \(SIS\)](#) ([Agence du numérique en santé](#)).

[Guide des mécanismes de protection de l'intégrité des données stockées](#)

FICHE 6 – LA SECURITE DU SYSTEME D'INFORMATION

PRESENTATION

La sécurité a pour objectif de réduire les risques pesant sur le système d'information afin de limiter les impacts sur le fonctionnement et les activités métier des organisations. Elle permet de maîtriser :

- la confidentialité des données : limiter l'accès aux données sensibles aux seules personnes autorisées ;
- la disponibilité des données : les données et systèmes doivent être disponibles durant les plages d'utilisation prévues ;
- l'intégrité des données : aucune altération ou destruction volontaire ou accidentelle n'est possible lors du traitement, de la transmission et de la conservation des données ;
- la preuve : retrouver avec une confiance suffisante, la traçabilité des actions menées, l'authentification^{GI} des utilisateurs et l'imputabilité à un responsable de chaque action effectuée.

Le niveau de sécurité du système d'information requis dépend de la criticité des données manipulées. Diverses réglementations encadrent le niveau de sécurité requis pour les entités publiques (PSSI et RGS^{GI} notamment détaillés dans l'axe 1). Pour les collectivités territoriales, l'ANSSI^{GI} a rédigé un [guide de synthèse](#) sur la réglementation applicable.

LES RISQUES

- L'altération ou la perte des données en masse.
- La consultation inappropriée ou la divulgation de données sensibles.
- Le risque d'amende ou d'image en cas de non-respect de la réglementation en vigueur.
- La cyber menace.

LES OBJECTIFS

Les objectifs de cette partie sont de permettre :

- De contrôler le contenu de la **politique de sécurité des systèmes d'information et la conformité au RGS (axe 1)**.
- De s'assurer de la **sécurité physique^{GI}** du matériel informatique **(axe 2)**.
- D'évaluer les dispositifs **de sécurité logique^{GI}** **(axe 3)**.
- De vérifier la mise en œuvre régulière des **audits de sécurité (axe 4)**.
- De s'assurer que les organismes prennent en compte les questions et enjeux de la **cyber sécurité (axe 5)**.
- De vérifier la conformité aux exigences d'un OIV et d'un OSE **(axe 6)**.

AXE 1 – CONTROLER LE CONTENU DE LA POLITIQUE DE SECURITE DES SI ET LA CONFORMITE AU RGS

Les enjeux pour l'organisme

- ▶ Connaître les règles et les enjeux en matière de sécurité interne et externe
- ▶ Prévoir un plan d'action correctives et des règles associées
- ▶ Etre en conformité avec le référentiel général de sécurité

Les risques

- ▶ Perte de données en masse
- ▶ Fragilité face à la cyber menace
- ▶ Non-conformité
- ▶ Service de mauvaise qualité
- ▶ Non implication des utilisateurs dans la sécurité informatique

A. Contrôler le contenu de la politique de sécurité des systèmes d'information



Bonnes pratiques

Une politique de sécurité du système d'information (PSSI^{GI}) doit être définie afin d'assurer la bonne connaissance des utilisateurs sur la sécurité des SI. La PSSI doit être validée par la direction de l'entité et communiquée au personnel travaillant pour la DSI (ressources internes et externes) et aux prestataires informatiques. Une charte informatique (recueil des règles et bonnes pratiques sur le SI) est communiquée aux utilisateurs du SI. Ces deux documents nécessitent une mise à jour et une communication régulières (à l'embauche et tous les ans pour sensibilisation).

Questionnements

Définition de la PSSI

- ▶ Une analyse des risques interne a-t-elle été réalisée (cf. [fiche 1, axe 4](#)) ?
- ▶ Y a-t-il une politique de sécurité des systèmes d'information (PSSI) ?
- ▶ Contient-elle l'ensemble des chapitres importants (cf. *Pour en savoir plus*) ?

Calendrier, méthodologie et gouvernance de la PSSI

- ▶ Quand a-t-elle été formalisée ? Quels sont les acteurs impliqués dans sa conception ?
- ▶ Par qui a-t-elle été validée ? Existe-t-il une comitologie ?
- ▶ La PSSI est-elle communiquée à l'ensemble des salariés et prestataires travaillant sur le SI ? Selon quelle modalité ?

Pour aller vers l'observation

Conclure sur :

L'existence de la PSSI.

La cohérence et le contenu attendu.



Point d'attention

La [politique de sécurité des systèmes d'information](#) de l'État (PSSIE) fixe les règles de protection applicables aux systèmes d'information de l'État (les ministères, les établissements publics sous tutelle d'un ministère, les services déconcentrés de l'État et les autorités administratives indépendantes).

La mise à jour et l'enrichissement régulier de la PSSI par l'entité.

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

Suivi de la PSSI

- ▶ Des évaluations régulières sont-elles mises en place par l'audit interne ou par des organismes extérieurs ?
- ▶ La PSSI est-elle mise à jour en fonction de ces retours ?

Charte informatique

- ▶ Y a-t-il une charte informatique formellement définie ? Quand a-t-elle été formalisée et validée ? Par qui a-t-elle été validée ?
- ▶ La charte est-elle communiquée systématiquement à l'embauche d'un nouvel agent et est-elle signée par l'agent ?
- ▶ Les agents sont-ils ensuite régulièrement sensibilisés sur la sécurité du SI ?
 - ❖ Exemples : envois régulier de rappels sur les bonnes pratiques, communication d'actualités aux personnels concernés, rappel de la charte sur l'intranet...
- ▶ Des campagnes de formation aux risques informatiques ont-elles été menées ?
 - ❖ Exemples : tests d'hameçonnage^{GI}, formations régulières...

La bonne communication et implication de l'ensemble des utilisateurs.



Point d'attention

Le manque de sensibilisation des utilisateurs aux sujets de sécurité des SI pourrait entraîner des pratiques contournant les dispositifs de sécurité en place :

- partage des mots de passe entre collègues,
- accès de données sensibles via des comptes personnels,
- communication sur les réseaux sociaux sur des sujets sensibles,
- fraude externe (par exemple fraude au président)
- usurpation d'identité,
- utilisation de plate-forme non sécurisée (type Dropbox, Google Docs...),
- utilisation de périphériques non homologués (clé USB ou tablette personnelles...),
- consultation de documents douteux envoyés par mail et contenant des virus, etc.

Documents à consulter :



Politique de sécurité des systèmes d'information
Référentiels mis en place
Charte informatique

Procédure et exemples de communication de la PSSI et de la charte
Supports de sensibilisation aux sujets informatiques des utilisateurs

Pour en savoir plus

La PSSI doit comporter plusieurs grands chapitres dont le degré de détail dépend de la taille de l'organisme, de son secteur d'activité et de sa maturité technique et organisationnelle.

- Le domaine d'application de la PSSI : est-elle applicable à l'ensemble du système d'information de l'organisme ? A l'extérieur de l'entreprise ?
- Les documents associés par exemple les référentiels (politique de cryptographie, normes, règlements, etc.)
- Les enjeux internes, externes : pourquoi une politique est-elle mise en œuvre ?

- La gouvernance : il est important d'identifier les fonctions et les rôles spécifiques de chaque intervenant (DG, DSI, RSSI, DPO...) ainsi que des instances mises en place pour contrôler, auditer et piloter la sécurité de l'information de l'organisme.
- Les règles : la PSSI doit spécifier les principes directeurs et les règles auxquels l'entreprise adhère pour garantir la sécurité de son système d'information.


Attention : Vous pouvez contacter la direction des méthodes et des données (DMD) si vous souhaitez faire des revues approfondies des thèmes abordés par une PSSI.

B. S'assurer de la conformité au référentiel général de sécurité (RGS)



Bonnes pratiques

Le RGS^{GI} est un référentiel destiné à sécuriser les échanges électroniques de la sphère publique. Pour une autorité administrative, appliquer le RGS permet de garantir aux citoyens et autres administrations que le niveau de sécurité de ses systèmes d'information est bien adapté aux enjeux et aux risques et qu'il est harmonisé avec ceux de ses partenaires.

Questionnements	Pour aller vers l'observation
<p>▶ Comment le RGS est-il intégré aux différentes contraintes opérationnelles de l'opérateur ?</p>	<p>Conclure sur :</p> <p>Les objectifs du RGS ainsi que les actions correspondantes qui doivent être clairement définies et comprises par l'entité.</p>
<p>▶ Comment est suivie la conformité au RGS ?</p>	<p>L'existence de réunions de suivi et de pilotage.</p>
<p>▶ Les équipes informatiques sont-elles impliquées dans un processus de conformité au référentiel général de sécurité ?</p>	<div style="border: 1px solid black; padding: 5px;"><p> Point d'attention</p><p>Le Référentiel Général de Sécurité (RGS) est le cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.</p><p>Le RGS s'impose spécifiquement aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers (il s'agit de télé-services tels que le paiement de contraventions auprès de l'Administration).</p></div>

Documents à consulter :



Comptes rendus de comités de pilotage
Avancement des actions entreprises

AXE 2 – S'ASSURER DE LA SECURITE PHYSIQUE DU MATERIEL INFORMATIQUE

Les enjeux pour l'organisme

- ▶ Protéger physiquement les locaux contenant les biens sensibles
- ▶ S'assurer que seules les personnes habilitées ont accès aux équipements physiques (serveurs, salles informatiques, etc.)
- ▶ S'assurer que le matériel informatique n'est pas soumis à un risque environnemental

Les risques

- ▶ L'espionnage, le vol et la destruction accidentelle ou intentionnelle du système d'information de l'entité
- ▶ Des dégâts environnementaux (eau, feu, vétusté, etc.) peuvent mener à la perte partielle ou totale de ressources informatiques



Bonnes pratiques

Il est recommandé que les accès à la salle informatique contenant les infrastructures informatiques soient protégés par des badges nominatifs. Un processus d'attribution et de revue régulière des badges nominatifs doit être mis en place.

Des dispositifs de protection contre les risques environnementaux doivent exister, être entretenus et révisés régulièrement : double climatisation, faux plafond ou faux plancher contenant les câblages, contrôle de la température et de l'humidité, onduleurs électriques^{GI}, dispositifs anti-incendie.

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none">▶ Où se trouvent physiquement les équipements informatiques ? Sont-ils hébergés en interne ou bien chez un prestataire ? <p>S'ils sont hébergés en interne :</p> <ul style="list-style-type: none">▶ L'accès à la salle informatique est-il protégé (badge, clé, digicode, etc.) ?▶ Qui peut accéder à la clé de la salle ? Qui connaît le digicode d'entrée ?<ul style="list-style-type: none">❖ <i>Visiter la salle et vérifier qu'elle est bien fermée.</i> <ul style="list-style-type: none">❖ Seuls les utilisateurs ayant un profil technique doivent pouvoir accéder aux salles informatiques.❖ <i>Vérifier que les accès aux salles informatiques sont historisés et revus régulièrement.</i>	<p>Conclure sur :</p> <p>La politique d'attribution des accès physiques aux ressources informatiques.</p> <p>Le suivi régulier des accès.</p> <p>Les modalités de protection physique des équipements. Il est nécessaire de s'assurer que l'ensemble des menaces environnementales sont prises en compte.</p>

Questionnements	Pour aller vers l'observation
-----------------	-------------------------------

- ▶ Quels sont les dispositifs de sécurisation contre les risques environnementaux (inondation, chaleur, incendie, perturbation électrique) ?

S'ils sont hébergés chez un prestataire :

- ▶ Fait-il l'objet d'une certification type ISAE3402GI ? Si oui, il-y-a-t-il des anomalies significatives ? Quelles actions ont été mises en place pour les corriger ?
- ▶ En cas d'absence de certification, des audits de sécurité réguliers sont-ils menés par l'organisme afin de vérifier la mise en place des bonnes pratiques ?



Point d'attention

Une sécurité physique des infrastructures informatiques défaillante peut avoir pour conséquences des vols, pertes et/ou destructions des données en masse.

L'absence d'onduleurs peut entraîner en cas de coupures électriques, une interruption des systèmes informatiques, pouvant aller, en cas d'impossibilité de les redémarrer, jusqu'à l'arrêt de l'activité d'un organisme.



Point d'attention

Dans le cas où les ressources sont externalisées, il est nécessaire que l'hébergeur puisse fournir les preuves que ses installations permettent une sécurité physique satisfaisante.

Documents à consulter :



Procédures de gestion des accès aux salles informatiques
Dernière revue des accès attribués aux salles informatiques
Dernier rapport ISAE3402 (hébergement externalisé)

AXE 3 – EVALUER LES DISPOSITIFS DE SECURITE LOGIQUE

Les enjeux pour l'organisme

- ▶ Les données ne sont consultées que par les personnes autorisées
- ▶ Les modifications de données sont encadrées afin d'assurer leur intégrité et leur disponibilité

Les risques

- ▶ Fuite, altération ou perte d'informations sensibles
- ▶ Consultation non appropriée de données
- ▶ Vulnérabilités/fragilités face à la malveillance



Bonnes pratiques

Les accès aux outils informatiques doivent être attribués via des profils utilisateurs, correspondant strictement aux besoins métier. Toute demande de création, modification et désactivation de compte utilisateur doit être tracée formellement et faire l'objet d'une validation par le responsable hiérarchique de l'agent concerné. Les utilisateurs ne doivent pas être administrateurs de leurs ordinateurs et ne peuvent donc pas installer de logiciels sans obtenir l'aval de la DSI (demande formalisée). Il est fondamental que les accès administrateurs soient limités aux personnes appropriées du service informatique. Les actions réalisées par ces administrateurs font l'objet de revues régulières.

Des inventaires logiques sont également nécessaires, en comparant les accès aux répertoires partagés/logiciels/licences installés par rapport aux besoins des équipes d'une part et la politique mise en place par l'organisme d'autre part. Lors du changement de poste ou lors du départ d'un collaborateur, le suivi des accès logiques associés est à réaliser.

Questionnements

- ▶ Les utilisateurs sont-ils administrateurs de leurs postes de travail ? Peuvent-ils installer n'importe quels logiciels ?

Pour l'application auditée ou celle produisant les informations contrôlées :

- ▶ Comment peut-on accéder à l'application ?
 - ❖ *L'accès aux applications doit se faire par exemple via un identifiant unique, nominatif et un mot de passe (cf. point d'attention sur les comptes génériques)*

- ▶ Y a-t-il des profils d'accès définis dans l'application, permettant de restreindre les accès aux données sensibles ?

Pour aller vers l'observation

Conclure sur :


La politique de mots de passe ([annexe 2](#)) et la présence ou non de comptes génériques.



Point d'attention

L'utilisation de comptes génériques, partagés par plusieurs utilisateurs, ne permet pas d'assurer la traçabilité des opérations réalisées dans l'outil informatique. Il est nécessaire de comparer les contraintes des mots de passe définis au niveau des applications avec les bonnes pratiques présentées en [annexe 2](#).

L'absence de profils utilisateurs ne permet pas une gestion fine des accès aux données et pourrait conduire à des accès inappropriés à tout ou à une partie d'une application.

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none"> ❖ <i>Vérifier la cohérence entre la politique des droits d'accès et la politique de classification de l'information des différents systèmes et réseaux.</i> <p>► Combien de comptes utilisateurs disposent d'un accès d'administration (par application) ? Sont-ils nécessaires et justifiés ? Y a-t-il des revues régulières des actions réalisées par les administrateurs ?</p> <ul style="list-style-type: none"> ❖ <i>Les accès à forts privilèges doivent être limités aux personnes appropriées. Si elle est techniquement possible, une revue des actions réalisées par les administrateurs devrait être mise en place.</i> <p>► Y a-t-il un processus clairement défini de création, modification, suppression des comptes utilisateurs ?</p> <ul style="list-style-type: none"> ❖ <i>Vérifier le cloisonnement des rôles pour le contrôle d'accès : la demande d'accès, l'autorisation d'accès et l'administration des accès.</i> <p>► Les comptes utilisateurs, les droits associés (par exemple l'accès aux répertoires partagés) et les licences utilisateurs font-ils l'objet de revues régulières ?</p> <ul style="list-style-type: none"> ❖ <i>Si les revues existent, il est nécessaire de vérifier qu'elles sont efficaces sur un échantillon de revues réalisées.</i> 	<p>L'adéquation des habilitations aux rôles/fonctions/responsabilités des agents.</p> <p>La nécessité et la justification des comptes à forts privilèges.</p> <p>La fréquence, le périmètre et la qualité des revues de comptes et des licences.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <p style="text-align: center;"> Point d'attention</p> <p>Une absence de revues régulières des comptes, des droits et des licences utilisateurs peut conduire à :</p> <ul style="list-style-type: none"> - des comptes utilisateurs encore actifs après le départ de l'employé (avec parfois la possibilité pour l'ancien agent d'accéder à des données internes après son départ) ; - des accès aux données trop larges ou inappropriés ; - des licences utilisateurs actives alors que les employés ont quitté la société. </div>

Documents à consulter :



- Procédure de gestion des accès logiques à l'application
- Liste des profils utilisateurs
- Contraintes des mots de passe définis dans l'application
- Dernière revue des comptes, droits associés et licences utilisateurs
- Liste des comptes d'administrateurs et revues des actions réalisées par ces comptes
- Dernier rapport d'audit interne/externe ainsi que les plans d'action suite à cet audit
- Procédure de création, modification, suppression des comptes utilisateurs

AXE 4 – VERIFIER LA MISE EN ŒUVRE REGULIERE DES AUDITS DE SECURITE

Les enjeux pour l'organisme

- ▶ Identifier des zones de fragilité sur son système d'information
- ▶ Identifier et mettre en oeuvre des plans d'action et des axes d'améliorations

Les risques

- ▶ Mesures de sécurité non alignées avec l'état de l'art
- ▶ Non détection de menaces et de fragilités



Bonnes pratiques

La mise en place d'audits extérieurs réguliers doit permettre à l'entité d'obtenir des indicateurs sur son niveau de sécurité. Il est nécessaire que la direction de l'organisme demande à la DSI de définir des plans d'action pour répondre aux risques relevés par les audits internes ou externes. Les deux directions doivent faire un suivi régulier de la mise en œuvre des recommandations.

Questionnements

- ▶ Y a-t-il des audits de sécurité réguliers ? Notamment des internes et/ou externes et des tests d'intrusion.

❖ *Les audits peuvent être effectués dans différents buts*

- réagir à une attaque ;
- évaluer le niveau de sécurité du SI ;
- tester la mise en place effective de la PSSI ;
- tester un nouvel équipement ;
- évaluer l'évolution de la sécurité (implique un audit périodique).

❖ *Récupérer les rapports d'audit et vérifier que des plans d'action ont été mis en œuvre. En cas d'absence de plans d'action, les observations formulées dans ces audits sont a priori toujours d'actualité.*

Pour aller vers l'observation

Conclure sur :

La tenue régulière d'audits de sécurité.

La prise en compte des recommandations émises dans le cadre d'une comitologie dédiée, la mise en place de plans d'action suite aux audits, et le suivi de l'avancement de ceux-ci.



Point d'attention

L'audit ne doit pas être confondu avec l'analyse de risques. Il ne permet que de trouver les vulnérabilités, mais pas de déterminer si celles-ci sont tolérables. Au contraire, l'analyse de risque permet de dire quels risques sont pris en compte, ou acceptés pour le SI. L'auditeur (le prestataire) dresse donc des recommandations, que l'audit (l'organisme) suivra, ou ne suivra pas. L'organisme déterminera s'il suivra les recommandations ou non, en se référant à la politique de sécurité interne.

Documents à consulter :



Audits de sécurité réalisés en interne ou par des organismes externes
Plan d'action suite aux audits réalisés

AXE 5 – S'ASSURER DE LA PRISE EN COMPTE DES QUESTIONS ET ENJEUX DE LA CYBER SECURITE

Les enjeux pour l'organisme

- ▶ Anticiper les menaces
- ▶ Adapter le SI


Les risques

- ▶ Perte ou divulgation d'informations confidentielles
- ▶ Perte financière liée à la perte de service ou à un logiciel de rançon (rançongiciel)
- ▶ Altération de l'image de l'entité



Bonnes pratiques

La menace « cyber » doit être régulièrement évaluée sur la base de données internes et externes. Les zones de vulnérabilité de l'organisme doivent être identifiées et prises en compte dans un dispositif adapté (tests d'intrusion).

Questionnements	Pour aller vers l'observation
<ul style="list-style-type: none"> ▶ Comment l'entité évalue l'état de la menace ? Existe-t-il un recensement de l'impact des attaques externes passées ? Qui est en charge de la menace cyber ? ▶ Un suivi des éléments d'actualité est-il mis en place ? <ul style="list-style-type: none"> ❖ <i>Par exemple à l'aide d'une veille sur les incidents de sécurité les plus significatifs et sur l'évolution de la menace cyber (type, cibles connues, etc.)</i> ▶ Comment l'entité identifie-t-elle les zones de vulnérabilité ? Une gestion des risques techniques et opérationnels est-elle déployée ? ▶ L'entité dispose-t-elle d'un dispositif de gestion des risques cyber couvrant : <ul style="list-style-type: none"> - la collecte des comportements des utilisateurs du SI ; - l'analyse de ces comportements ; - la réaction aux événements de sécurité. 	<p>Conclure sur :</p> <p>La présence d'une analyse de risques faisant état de la menace cyber.</p> <p>La comitologie dédiée à la gestion des risques cyber.</p> <p>Les incidents majeurs de cyber sécurité.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center;"> Point d'attention</p> <p>Il est essentiel que l'entité prenne en compte l'ensemble des risques cyber qui est protéiforme. Les menaces principales sont les suivantes :</p> <ul style="list-style-type: none"> - hameçonnage^{GI} et ingénierie sociale ; - fraude interne ; - violation d'accès ; - virus informatique ; - rançongiciel ; - déni de service distribué. </div>

Documents à consulter :



Politique de sécurité des systèmes d'information
Analyses de risques
Comptes rendus d'évaluation des menaces

AXE 6 - S'ASSURER DE LA CONFORMITE AUX EXIGENCES D'UN OIV ET D'UN OSE

Un **OIV** (pour opérateur d'importance vitale) est un opérateur économique ayant un rôle primordial pour le fonctionnement de la nation (grandes administrations, réseaux télécoms etc...). Un **OSE** (pour opérateur de service essentiel) est un opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

Les enjeux pour l'organisme

- ▶ Etre en mesure de garantir son service en tant qu'OSE ou OIV (cf. pour en savoir plus)
- ▶ Respect de la réglementation

Les risques

- ▶ Non-conformité aux réglementations
- ▶ Perte de données et de services essentiels à la nation



Bonnes pratiques

L'entité doit nommer un coordinateur chargé de la représenter auprès de l'ANSSI^{GI}.

Ses systèmes d'information essentiels (SIE) doivent être déclarés dans un délai de 3 mois à compter de la date de désignation. Les incidents sont consignés et font l'objet d'une communication à l'ANSSI. Les OSE et OIV doivent respecter les obligations et recommandations d'équipement et d'organisation en vue de leur protection contre les cyberattaques. Ces obligations et recommandations comprennent la mise en place d'une architecture de réplication de trafic, d'un service et de sondes de détection, et incite à la mise en place de moyens et d'une organisation appropriés.

Questionnements

- ▶ Si l'entité est opérateur de service essentiel ou d'importance vitale, quel est le degré de mise en conformité vis-à-vis de l'ANSSI (cf. bonnes pratiques et pages dédiées de l'ANSSI)?
- ▶ L'entité consigne-t-elle l'ensemble de ses déclarations d'incidents ?
- ▶ L'entité déclare-t-elle ses incidents de sécurité à l'ANSSI ?

Pour aller vers l'observation

Conclure sur :

La conformité par rapport aux exigences réglementaires spécifiques.



Point d'attention

La cyber sécurité des OIV s'intègre dans le dispositif interministériel plus large de [sécurité des activités d'importance vitale](#) (SAIV) inscrit dans le code de la défense.

Documents à consulter :



P V de nomination du coordinateur
Registre des incidents
Avancement de la conformité à l'ANSSI

FICHE 7 - LA SECURISATION DES DONNEES PERSONNELLES – CONTROLER LA CONFORMITE D'UNE ENTITE AUX DISPOSITIONS DU RGPD

LES ENJEUX DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL^{GL}

Les organismes contrôlés par les juridictions financières collectent, utilisent, sauvegardent et détruisent un grand nombre de données à caractère personnel plus ou moins sensibles, dans le cadre de leur fonctionnement courant (ex : fichiers de paie de leurs personnels, dispositifs de vidéosurveillance de leurs bâtiments, coordonnées des prestataires de leurs marchés, etc) et/ou des activités spécifiques qu'ils exercent (ex : données de santé dans un établissement médical, données fiscales par un centre des impôts, coordonnées de donateurs pour les organismes faisant appel à la générosité publique, etc).

Les obligations qui incombent à ces organismes à chaque étape du **cycle de vie de la donnée** (collecte, sauvegarde, destruction) sont nombreuses, en particulier depuis l'entrée en vigueur du **règlement général sur la protection des données** (RGPD), le 25 mai 2018.

Au-delà des enjeux de droit, la protection des données à caractère personnel constitue aussi un point d'attention, voire d'inquiétude, de plus en plus fort chez nos concitoyens, dont les attentes vont croissantes vis-à-vis des tiers qui traitent leurs données.

Aussi, le contrôle du respect des obligations pesant sur les entités publiques en matière de protection des données et, plus largement, en matière de sécurité informatique, est donc désormais un domaine d'examen incontournable lors d'un audit des systèmes d'information.

On parle de **données à caractère personnel** à l'égard de toutes les informations, manuscrites ou numériques, qui permettent d'identifier directement ou indirectement une personne. Sont ainsi des données à caractère personnel, un relevé d'identité bancaire, un CV, une adresse, une plaque d'immatriculation, une adresse IP^{GI}, une photographie d'identité, etc...

On parle de **traitement de données à caractère personnel** lorsque ces données font l'objet d'une opération², quel que soit le procédé utilisé, qu'il soit automatisé ou non. Ainsi, un dossier papier de recrutement contenant des CV est un traitement de données à caractère personnel, de même qu'un dispositif de vidéosurveillance, un logiciel de paie, un fichier Excel contenant des adresses e-mail, une base de données^{GI}, etc.

On parle de **responsable de traitement** à l'égard de la personne morale (entreprise, collectivité, association, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Le cadre juridique applicable à la protection des données personnelles date de la **loi dite « informatique et libertés » de 1978**, qui définit pour la première fois les règles et principes à respecter

² Constituent des opérations de traitement de données la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication ou toute autre forme de mise à disposition, le rapprochement, etc.. de données à caractère personnel.

lors d'un traitement de données à caractère personnels. Elle précise également les compétences et missions de la Commission nationale de l'informatique et des libertés, la CNIL, pour en assurer le respect.

Adopté en 2016 et entré en vigueur le 25 mai 2018, le RGPD vise à donner aux citoyens européens davantage de visibilité et de contrôle sur leurs données personnelles. Ses dispositions ont été transposées par **la loi du 20 juin 2018 relative à la protection des données personnelles** et son décret d'application du 1^{er} août 2018, puis par l'ordonnance du 12 décembre 2018 et le décret du 29 mai 2019.

Le champ d'application du RGPD est particulièrement vaste : il s'applique à toute organisation publique ou privée, établie sur le territoire de l'Union européenne et/ou qui traite des données personnelles appartenant à des citoyens de l'Union, qu'elle le fasse pour son compte ou pour le compte d'un tiers.

Contrairement à l'esprit de la loi « informatique et libertés » de 1978, le dispositif établi pour le RGPD ne soumet plus les traitements de données à caractère personnel à un régime d'autorisation préalable ; il met en place un **dispositif de responsabilisation des acteurs du traitement** et fixe à leur égard une obligation de moyens et non de résultats. Chaque entité doit ainsi être en mesure de démontrer sa conformité aux principes et règles posés dans le règlement.

Le RGPD donne aussi compétence aux autorités nationales – en France, la CNIL – pour contrôler *a posteriori* et, éventuellement, pour sanctionner les entités qui méconnaîtraient les obligations fixées par le règlement. La CNIL, sur la base de signalements ou de plaintes, et en fonction de sa propre analyse de risque, est ainsi habilitée à effectuer des contrôles sur pièce et sur place dans un très large champ d'organismes. Les sanctions encourues en cas de non-conformité peuvent être particulièrement lourdes³.

*

La protection des données garantie par le RGPD repose sur cinq principes fondamentaux ; **ils doivent guider toutes les opérations de traitement de données à caractère personnel réalisées par les entités contrôlées**, quelle que soit leur activité :

- **Le principe de licéité** : le traitement doit avoir un fondement juridique (ex : le consentement de la personne, l'exécution d'un contrat, le respect d'une obligation légale, la sauvegarde d'intérêts vitaux, l'exécution d'une mission d'intérêt public ou la poursuite d'intérêts légitimes par le responsable de traitement),
- **Le principe de loyauté** : les personnes dont les données sont traitées doivent en être informées de façon claire, lisible et compréhensible. Elles doivent connaître notamment le périmètre du traitement, la base juridique qui l'autorise, la durée de conservation des données et les coordonnées des personnes auprès de qui pour faire valoir leurs droits,
- **Le principe de finalité** : les données traitées le sont pour une finalité déterminée, explicite et légitime. Une fois collectées, elles ne peuvent donc pas être utilisées pour satisfaire une autre finalité,
- **Le principe de minimisation** : au regard de leur finalité, les données traitées sont adéquates, pertinentes, limitées au strict nécessaire, exactes et tenues à jour,
- **Le principe de limitation de la durée de conservation** : sauf rares exceptions – notamment la conduite de recherches scientifiques ou historiques – les données traitées ne sont conservées que pendant la durée nécessaire à la poursuite de la finalité pour laquelle elles ont été

³ Pour plus d'informations : <https://www.cnil.fr/le-contrôle-de-la-cnil>

collectées.

Chacun de ces principes fait l'objet d'exceptions limitativement énumérées dans le texte du règlement.

*

Dans toutes les entités qui y sont soumises, le RGPD fixe aussi un certain nombre d'obligations concrètes de conformité, parmi lesquelles :

- **La nomination d'un(e) délégué(e) à la protection des données** (DPO, pour *data protection officer*),
- **La tenue d'un registre de l'ensemble des traitements de données** à caractère personnel réalisés dans cette entité, quelle qu'en soit la nature.

Quel est le rôle du (de la) délégué(e) à la protection des données (DPO) ?

Sa désignation est obligatoire pour toute entité soumise au RGPD, quelle que soit la nature et le volume des traitements qui y sont réalisés. La fonction de DPO peut être mutualisée entre plusieurs entités, notamment pour les organismes de petite taille, et/ou externalisée. En interne, elle peut être exercée à titre exclusif ou à temps partiel, en complément d'autres activités.

La nomination du / de la DPO doit être déclarée à la CNIL. Pour exercer ses missions, le / la DPO doit disposer de moyens dédiés et suffisants.

Il n'existe pas de profil-type ou de fiche de mission-type établis pour effectuer cette mission ; néanmoins, la CNIL a fixé quelques conditions à sa désignation⁴, parmi lesquelles :

- Disposer d'une expertise sur la protection des données et d'une bonne connaissance de l'organisme,
- Bénéficier d'un positionnement visible, qui lui permette notamment de rapporter à un niveau élevé,
- Ne pas être en situation de conflits d'intérêt, c'est-à-dire occuper une fonction qui le ou la conduirait à déterminer lui-même les moyens et finalités d'un traitement ; c'est le cas pour exemple si le/la DPO exerce les fonctions suivantes : secrétaire ou directeur-trice général(e) de la structure, directeur-trice des systèmes informatiques, directeur-trice financier, etc...

*

Le ou la DPO dispose de **six missions** :

- Informer et conseiller l'organisme en matière de protection des données,
- Veiller au respect des principes et droits fixés par le RGPD dans les activités courantes de l'entité,
- Etre le point de contact de la CNIL, notamment en cas de contrôle de l'entité,
- Etre le point de contact de toute personne externe ou interne à l'organisme qui souhaite exercer ses droits ou signaler une violation de ses données,
- Tenir à jour la documentation relative aux traitements réalisés par l'entité,
- Réaliser un bilan d'activité annuel (non obligatoire).

⁴ Pour plus d'informations : <https://www.cnil.fr/fr/designation-dpo>

Qu'est-ce que le registre des activités de traitement ?

C'est un document-clé de la mise en conformité qui recense la totalité des traitements réalisés par une entité soumise aux dispositions du RGPD.

Le texte du règlement ne prévoit pas de formalisme particulier pour ce document mais, quelle que soit la forme du registre, elle doit permettre d'identifier pour chaque traitement les catégories de données traitées, les parties prenantes concernées, à quoi les données sont utilisées, qui y accède, quelles sont les mesures de protection mises en place à leur égard et combien de temps ces données sont conservées.

Le registre est piloté et mis à jour régulièrement par le/la DPO.

Outre la nomination du/de la DPO et la formalisation d'un registre de traitement, le RGPD crée pour les entités qui y sont soumises un certain nombre d'obligations vis-à-vis des personnes dont les données sont traitées par celles-ci. Sans être exhaustif, on citera trois d'entre elles :

- L'obligation pour un organisme de **donner suite dans un délai d'un mois à toute demande d'exercice de leurs droits par les personnes** dont les données font l'objet d'un traitement. Cela inclut notamment – sauf rares dispositions contraires – de leur donner le droit d'accéder à leurs données, de leur donner toute information qu'elles requièrent sur l'existence et le périmètre d'un traitement les concernant, de leur permettre de rectifier les données qui ont été traitées ou de les faire effacer, ou encore de leur permettre de demander la limitation ou de s'opposer au traitement réalisé.
- L'obligation de **documenter toute violation de données à caractère personnel**, qu'elle soit accidentelle ou illicite, dès lors qu'elle entraîne la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé aux données qui ont été collectées. En cas de risque pour les droits et libertés des personnes concernées, la notification de la violation doit être faite sans délai à la CNIL et, en cas de risque élevé, les personnes concernées doivent être directement informées par l'organisme⁵.
- L'obligation de **réaliser des études d'impact** (ou *privacy impact assessment* – PIA) lorsque des projets susceptibles d'exposer à un risque élevé la protection de la vie privée de tiers sont envisagés dans l'entité.

Le respect de ces obligations constitue des signaux forts de la conformité RGPD, **mais d'autres signaux faibles peuvent aussi témoigner du degré d'appropriation par un organisme du RGPD :**

- Des **actions de sensibilisation** à la protection des données personnelles doivent par exemple d'être conduites dans l'organisme, en particulier auprès du personnel et des directions les plus exposés (direction des systèmes d'information, direction des ressources humaines, etc),
- Des **mesures organisationnelles fondées sur une analyse des risques détaillée** doivent être prises pour protéger les données qui y sont traitées, en particulier les plus sensibles (données de santé, données bancaires, données de paie),
- Des **clauses spécifiques** doivent être introduites dans les marchés passés par l'organisme pour tenir compte des obligations incombant aux différentes parties au titre du RGPD.

Dans tous ces questionnements, la mission de conseil et d'alerte du/de la DPO est essentielle.

*

⁵ Pour plus d'informations : <https://www.cnil.fr/fr/les-violations-de-donnees-personnelles>

La liste des diligences de contrôle ci-après vise donc à tester et analyser :

- Le respect des obligations de mise en conformité incombant à l'entité contrôlée au titre du RGPD,
- L'appropriation plus générale par l'organisme des questions relatives à la protection des données à caractère personnel.

Ces diligences sont à adapter selon la nature et le volume des données à caractère personnel qui sont traitées par l'organisme ; le traitement de données de santé doit notamment faire l'objet d'une attention renforcée de la part des auditeurs.

En dehors de tels signes manifestes de conformité ou non aux dispositions du RGPD, **l'audit des SI doit permettre à l'équipe d'appréhender le respect par l'entité contrôlée des principes posés par le RGPD** (licéité, finalité, proportionnalité, etc), et, ce, dans l'ensemble des traitements qu'elle réalise, papiers ou numériques. En ce sens, des diligences complémentaires sont indiquées en fin de fiche afin de tester quelques signaux faibles, qui, bien que non exhaustifs, constituent autant de marqueurs indicatifs de la conformité RGPD d'un organisme.

AXE 1- LE RESPECT DES OBLIGATIONS INCOMBANT A L'ENTITE CONTROLEE AU TITRE DU RGPD

Questionnements	Pour aller vers l'observation
<p>Le/ la délégué(e) à la protection des données</p> <ul style="list-style-type: none">▶ Existe-t-il un(e) DPO ? Quand il / elle a-t-il / elle été nommé(e) ?▶ Le / la DPO exerce-t-il /elle ses fonctions à titre principal ? Sa fonction est-elle mutualisée avec d'autres organismes ? Est-elle externalisée ?▶ Sa nomination respecte-t-elle les conditions fixées par la CNIL (formation et compétences suffisantes, positionnement adapté, etc.) ? Son positionnement le ou la prémunit-il d'éventuels conflits d'intérêt et lui garantit une indépendance vis-à-vis des responsables de traitement ?▶ Quels sont les moyens et le temps dédiés à cette mission ? A-t-il ou elle bénéficié de formations consacrées à la protection des données personnelles ou/et à la sécurité informatique ?▶ Le / la DPO est-il/elle bien identifié(e) par les agents de la structure ? Sa nomination a-t-elle donné lieu à une communication à l'interne et/ ou à l'externe ? À quelle(s) instance(s) de gouvernance est-il/elle associé(e) ?▶ Le / la DPO a-t-il/elle reçu des sollicitations internes ou externes ? Combien et sur quels sujets ? Prendre connaissance de son dernier rapport d'activité, s'il a été réalisé.	<p>Conclure sur :</p> <p>La réactivité de l'entité contrôlée à mettre en œuvre les dispositions du RGPD et, ce faisant, le degré de priorité accordé à ce sujet ainsi que sa visibilité dans l'organisme,</p> <p>La pertinence du profil retenu pour exercer les fonctions de DPO, le dimensionnement et la solidité de son positionnement, sa capacité potentielle à influencer sur l'activité de l'organisme et à exercer sa mission en toute indépendance,</p> <p>La qualité du pilotage de la mise en conformité réalisé par le/la DPO et l'adaptation des moyens dont il/elle dispose aux enjeux de protection des données identifiés dans l'organisme.</p>



Point d'attention

Pour faciliter la conduite de sa mission, une bonne communication autour de la nomination du / de la DPO est importante, tant à l'externe qu'à l'interne (ex : coordonnées dédiées figurant sur le site internet, présentation dans l'annuaire, interventions devant les instances, etc).

Documents à consulter :



Confirmation de nomination établie par la CNIL et arrêté de nomination du / de la DPO
Le cas échéant, contrat d'externalisation ou de mutualisation du / de la DPO
Bilan annuel d'activité du / de la DPO (document non obligatoire)
Recensement des sollicitations reçues par le / la DPO, leur origine et les suites qui y ont été données

Questionnements

Pour aller vers l'observation

Le registre des activités de traitement

- ▶ Consulter le registre de l'organisme ; évaluer la qualité, la complétude et l'exhaustivité des informations recensées par rapport à l'activité de l'entité.

- ▶ Quelles sont les procédures en œuvre pour assurer la mise à jour des données figurant dans ce registre ? Les différents services de l'entité sont-ils correctement associés au processus ?

- ▶ Certaines données particulièrement sensibles sont-elles signalées ? Font-elles l'objet d'une procédure de sécurisation particulière ?

- ▶ La confection du registre de traitement a-t-elle donné lieu à un exercice de cartographie des risques liés à la protection des données à caractère personnel ?

- ▶ À partir d'un échantillon de traitements sensibles (ex : données de santé, données de paie), vérifier la complétude des informations recensées pour chaque traitement, en particulier les :
 - Nom et coordonnées du responsable de traitement,
 - Finalité du traitement et base juridique,
 - Catégories de données conservées,
 - Délais de conservation ;
 - Description des mesures de sécurité techniques et organisationnelles mises en place.

Conclure sur :

L'exhaustivité du registre et la qualité du suivi réalisé,

La sensibilisation de l'entité aux principaux risques affectant son activité en matière de sécurité des données personnelles et la pertinence des mesures mises en place pour s'en prémunir.





Point d'attention

Certaines données à caractère personnel doivent faire l'objet d'une attention toute particulière ; c'est le cas des RIB, des données de santé, des données relatives à la situation familiale d'un individu ou encore des données qui concernent des mineurs.

Elles doivent être explicitement signalées dans le registre de traitements et à faire l'objet de mesures de sécurisation particulières.

AXE 2- LA SENSIBILITE DE L'ORGANISME AUX QUESTIONS DE PROTECTION DES DONNEES PERSONNELLES

Questionnements	Pour aller vers l'observation
<p>Le degré d'appropriation des dispositions du RGPD par l'organisme</p> <ul style="list-style-type: none">▶ Une communication spécifique a-t-elle été proposée aux agents sur les bons réflexes à adopter en matière de protection des données à caractère personnel ? Des formations ont-elles été organisées ?▶ Des réclamations ont-elles été formulées à l'encontre de l'entité, soit par des agents, soit par des tiers ? Ont-elles été traitées dans les délais ? Des signalements à la CNIL ont-ils été faits à l'encontre de l'entité ?▶ Des clauses spécifiques relatives à la protection des données dans les marchés passés par l'entité ont-elles été insérées depuis l'entrée en vigueur du RGPD ?▶ Des violations de données ont-elles été détectées ? Ont-elles donné lieu à une notification à la CNIL ? Les personnes concernées ont-elles été informées ?▶ L'entité a-t-elle mis en place des procédures pour limiter les menaces et risques pesant sur les données personnelles qu'elle détient ?▶ Certains projets sensibles du point de vue de la protection des données ont-ils donné lieu à la réalisation d'études d'impact (ou PIA) ?▶ Les durées de conservation des données les plus sensibles sont-elles clairement formalisées et cohérentes avec les autres documents internes des services métiers de l'organisme ? Correspondent-elles aux pratiques observées ?▶ Les conventions relatives aux entités liées à l'organisme indiquent-elles clairement le champ des responsabilités des parties en matière de données à caractère personnel ? Prévoient-elles des mécanismes de résolution des litiges ?	<p>Conclure sur :</p> <p>L'appropriation par l'entité des principes fondamentaux posés par le RGPD (finalité, licéité, minimisation, limitation de la durée de conservation et loyauté),</p> <p>Son degré d'exposition au risque de violation des données personnelles – risque contentieux et juridique et risque d'image,</p> <p>La pertinence des mesures de sécurité techniques et organisationnelles mises en place selon les traitements concernés.</p> <p>En cas d'atteinte grave aux dispositions figurant dans le RGPD, en particulier si l'entité contrôlée traite de données à caractère personnel nombreuses et/ ou sensibles, l'équipe de rapporteurs peut proposer à la collégialité, à l'issue de son contrôle, de faire procéder par le Parquet général à un signalement à la CNIL.</p> <div data-bbox="815 1294 1401 1809" style="border: 1px solid black; padding: 10px;"><p> Point d'attention</p><p>Pour déterminer le degré d'appropriation d'une entité des principes posés par le RGPD, on utilise parfois les notions de <i>privacy by design</i> et de <i>privacy by default</i>.</p><p>Elles signifient, d'une part, que l'entité intègre les enjeux relatifs à la protection des données personnelles dès la conception de ses produits, services ou projets et, d'autre part, que, par défaut, elle paramètre chacune de ses activités avec le plus degré de protection des données personnelles possible.</p></div>

Questionnements	Pour aller vers l'observation
<p>Tests de conformité RGPD dans les activités récurrentes d'organismes publics (* liste non exhaustive à adapter selon les organismes) :</p> <ul style="list-style-type: none"> ▶ <i>[Mentions légales]</i> Les supports de communication externes de l'organisme, notamment son site internet, comportent-ils des mentions légales à jour de l'entrée en vigueur du RGPD ? ▶ <i>[Bases de données]</i> Choisissez une base de données dont le contenu vous paraît sensible en termes de protection de la vie privée (données de paie, données RH, etc) : <ul style="list-style-type: none"> - évaluez le respect du principe de minimisation dans la collecte des données ; - déterminez l'effectivité des restrictions d'accès selon le nombre d'agents ayant accès à ces informations, leur qualité, la nécessité pour eux d'en connaître et le degré d'actualisation de la gestion de ces droits ; - évaluez les modalités et l'efficacité du suivi des violations d'accès : la journalisation de toutes les écritures portant sur des données à caractère personnel, quelle que soit l'application en cause, est-elle garantie ? ▶ <i>[Dispositif de vidéosurveillance]</i> Si l'organisme en dispose, assurez-vous de sa conformité aux dispositions en vigueur⁶. ▶ <i>[Gestion des accès physiques]</i> Quelles données personnelles sont demandées aux visiteurs qui se présentent dans le bâtiment de l'organisme ? Vous paraissent-elles respecter le principe de minimisation ? Combien de temps sont-elles conservées ? Les visiteurs en sont-ils informés ? 	<p>Conclure sur :</p> <p>L'appropriation par l'entité des principes fondamentaux posés par le RGPD (finalité, licéité, minimisation, limitation de la durée de conservation et loyauté),</p> <p>Son degré d'exposition au risque de violation des données personnelles – risque contentieux et juridique et risque d'image,</p> <p>La pertinence des mesures de sécurité techniques et organisationnelles mises en place selon les traitements concernés.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <p style="text-align: center;"> Point d'attention</p> <p>Au-delà des défauts de conformité flagrants, les organismes contrôlés peuvent avoir conservé de mauvaises pratiques à l'heure du RGPD. C'est fréquemment le cas de la conservation très extensive de données à caractère personnel, numériques ou papiers (ex : données conservées en doublon dans différents services et/ ou sur de multiples supports, données personnelles conservées alors qu'elles n'ont plus d'utilité ou sont techniquement « périmées »).</p> <p>Ces mauvaises habitudes mettent en risque l'organisme et peuvent facilement être corrigées à travers des dispositifs de communication interne voire des revues périodiques conduites par le ou la DPO.</p> </div>

⁶ <https://www.cnil.fr/fr/la-videosurveillance-vidéoprotection-au-travail>

- [Gestion des recrutements] Listez l'ensemble des acteurs intervenants dans un processus de recrutement. Combien de personnes disposent des dossiers de candidature ? Quelles sont les informations demandées aux candidats ? Combien de temps sont-elles conservées ? Les candidats en sont-ils informés ?

Documents à consulter :



Etude(s) d'impact réalisée(s) par l'entité en amont de projets particulièrement sensibles
Plainte(s) éventuellement déposée(s) à la CNIL par des tiers à l'encontre de l'entité contrôlée ou PV d'éventuels contrôles conduits par la CNIL dans l'entité contrôlée
(demande à adresser à la CNIL par l'intermédiaire du Parquet général)

Pour en savoir plus

Le ou la délégué(e) à la protection des données des juridictions financières, placé(e) au secrétariat général, peut vous fournir des conseils lors de la conduite de votre contrôle (dpo-jf@ccomptes.fr). Il ou elle peut notamment vous mettre en contact avec les équipes de la CNIL ou avec les DPO d'autres entités publiques.

- **Ressources CNIL**

MOOC « *l'atelier RGPD* » de la CNIL, accessible gratuitement en ligne (6-8 heures pour l'ensemble de la formation),

Fiches pratiques très nombreuses et veilles d'actualité mises en ligne sur le site internet de la CNIL,
Guide de la CNIL sur la sécurité des données personnelles (édition 2018), disponible gratuitement en ligne,

Rapport d'activité annuel de la CNIL.

- **Corpus juridique**

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD),

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles,

Décret n° 2018-687 du 1^{er} août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles,

Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel,

Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

LISTE DES ANNEXES

ANNEXE 1 – LA TRANSFORMATION NUMERIQUE DE L'ETAT

i. [La loi pour une République numérique](#)

Promulguée le 7 octobre 2016 et issue d'une consultation citoyenne participative inédite, la [loi pour une République numérique](#) a pour objectif de faciliter la transformation numérique de la France et de préparer l'économie de demain.

Elle entend promouvoir l'innovation en faisant circuler les informations et les savoirs afin de permettre à la France de faire face aux enjeux de l'économie de la donnée. Elle doit permettre de créer un cadre de confiance clair, garant des droits des utilisateurs et protecteur des données personnelles. Enfin, elle ambitionne de construire une République numérique ouverte et inclusive, pour que les opportunités liées à la transition numérique profitent au plus grand nombre.

Un [site internet dédié](#) permet de suivre les évolutions mises en place par loi et les décrets applicatifs pris ou à venir.

ii. [Le règlement général sur la protection des données \(RGPD\)](#)

Entré en application le 25 mai 2018, le RGPD est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne.

Il s'inscrit dans la continuité de la [loi française Informatique et Libertés de 1978](#) établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Le RGPD a été conçu autour de trois objectifs :

- renforcer les droits des personnes,
- responsabiliser les acteurs traitant des données,
- crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

iii. [Les dispositions pour accompagner la transformation de l'administration](#)

La transformation de l'action publique a été définie par le gouvernement comme un impératif pour répondre aux transformations profondes qui traversent la société et bouleversent les métiers et les modes d'action publique. Cet engagement s'est traduit dans l'organisation de l'Etat⁷ ainsi que dans des programmes ciblés. Ces chantiers peuvent être regroupés en quatre thématiques :

- **Le déploiement de l'administration électronique** qui a été initié à la fin des années 1990, notamment par le Programme d'action gouvernemental pour la société de l'information (PAGSI) et qui continue au travers d'[Action publique 2022](#) lancé en octobre 2017.

⁷ [Décret du 25 octobre 2019](#)

La transformation numérique fait partie d'un des cinq chantiers prioritaires définis afin de **bâtir un nouveau modèle de conduite des politiques publiques** qui prenne en compte la révolution digitale. Dans ce cadre, les administrations ont lancé [des plans de transformation](#) qui déclinent les priorités à atteindre suivant leurs périmètre d'action. L'objectif du gouvernement est notamment de dématérialiser d'ici mai 2022 les [250 démarches "phares"](#) les plus utilisées par les citoyens.

- **L'accessibilité de l'administration** au travers deux axes principaux qui sont l'inclusion numérique et la simplification.

Sur l'inclusion, il s'agit de mieux détecter et accompagner les usagers en difficulté avec les outils numériques. Par ailleurs, l'État a lancé [TECH.GOUV](#), le nouveau programme pour accélérer la transformation numérique du service public, piloté par la DINUM (ex. DINSIC) avec l'appui de tous les ministères. Axé autour de 6 enjeux prioritaires - simplification, inclusion, attractivité, maîtrise, économies, alliances - ce programme se décline en un plan d'action sur 3 ans.

- **Améliorer les conditions de travail** des agents grâce aux outils numériques

Pour mettre en œuvre la transformation des services publics, le gouvernement a prévu d'accompagner les agents publics dans leur transition professionnelle ou l'évolution de leur métier. Un "fonds pour la transformation de l'action publique", au titre du Grand plan d'investissement 2018-2022, a aussi été créé. Il est doté de 700 millions d'euros sur 5 ans. Une offre de services plus large dédiée aux agents publics est en cours de construction, avec notamment des outils collaboratifs et de travail en mobilité issus des appels à projets de l'environnement de travail numérique des agents (ETNA).

- **Améliorer l'efficacité des politiques publiques** grâce aux outils numériques

A titre d'exemple, le Gouvernement a réaffirmé lors du CITP (Comité interministériel de la transformation publique) du 15 novembre 2019 sa volonté de se saisir pleinement du potentiel considérable que représente l'intelligence artificielle^{GI} (IA) pour le service public et l'efficacité des politiques publiques. Un laboratoire – le lab IA – installé au sein de la DINUM soutient des projets visant à expérimenter et développer l'utilisation de l'intelligence artificielle et des datasciences au sein de l'Etat.

Par ailleurs, le cadre juridique sectoriel comprend de plus en plus souvent un volet relatif au numérique. A titre d'exemple, la [loi de programmation pour la justice](#) et la [loi relative à l'organisation et la transformation du système de santé](#) ont mis l'accent sur la transformation numérique de l'action publique dans des domaines ciblés.

Pour en savoir plus

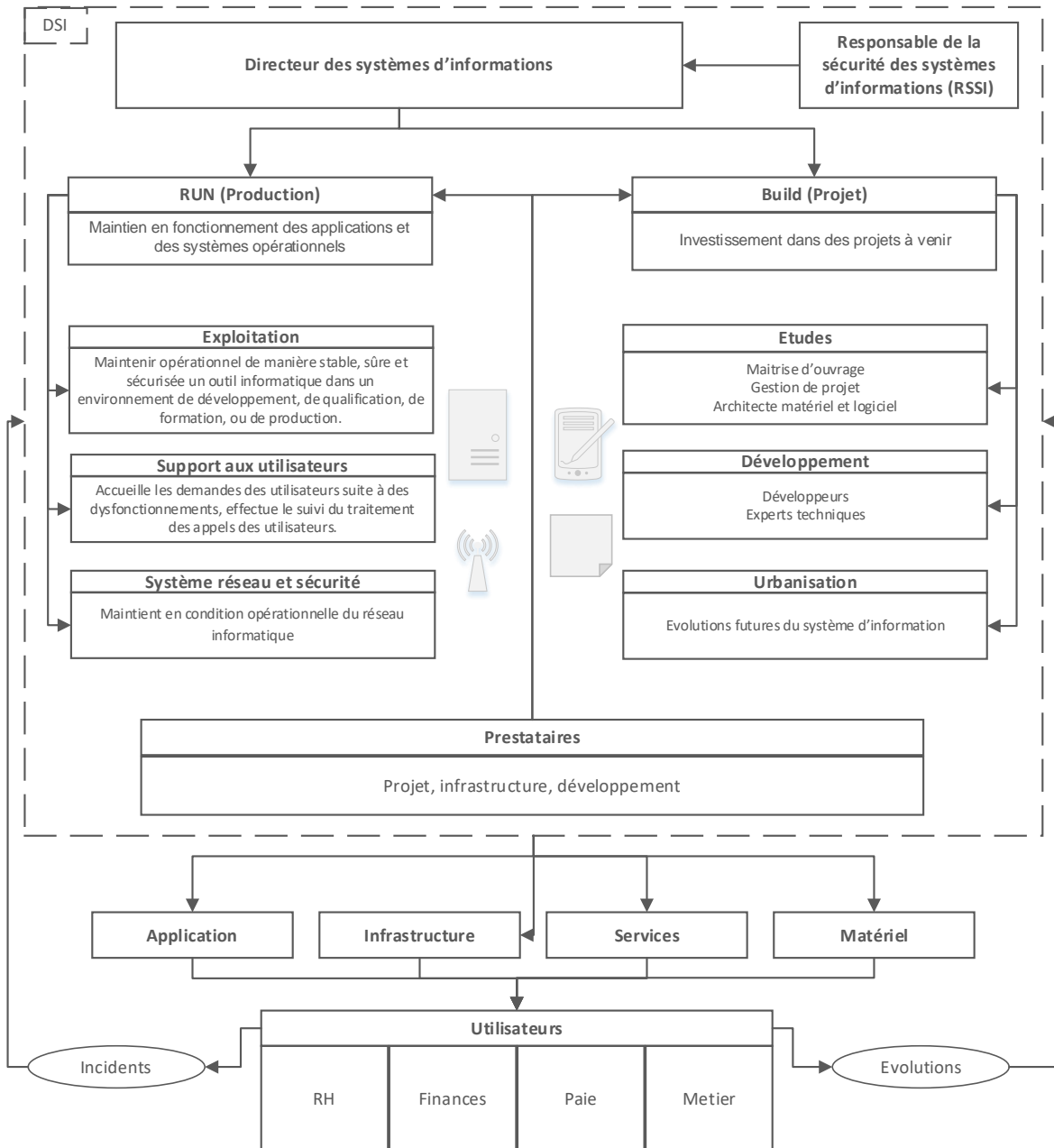
[Plan de transformation numérique de la commande publique 2017-2022](#)

[Histoire du déploiement de l'administration électronique](#)

[Détail des mesures issues du 4^{ème} CITP](#)

[Outils et méthode pour transformer](#)

ANNEXE 2 - LES ACTEURS DU SI



Au sein de la production informatique, on distingue :

- le service d'exploitation qui gère l'infrastructure matérielle (les serveurs, les ordinateurs, le réseau informatique, etc.) et logicielle (les applications informatiques) conformément aux objectifs de disponibilité des applications, d'intégrité et de confidentialité des données, et ainsi répondre aux besoins des utilisateurs finaux.
- Le service de support utilisateur (pour des problèmes de bureautique, des problèmes de connexion, ou pour les problèmes liés à l'utilisation des applications).
- Des services très techniques comprenant les architectes en charge de la conception et des évolutions des systèmes d'exploitation, des bases de données, et des traitements informatiques et les personnes en charge de superviser les systèmes, le réseau informatique et les télécommunications.

ANNEXE 3- ENVIRONNEMENT INFORMATIQUE

Le tableau ci-dessous permet de voir si la DSI a formalisé sa connaissance des applications et du réseau informatique^{G1} (cf. [axe 2](#)).

Nom de l'application	Processus supporté	Système d'exploitation / Base de données	En place depuis	Logiciel du marché ou développement interne	Hébergement	Nombre d'utilisateurs

Quelles applications sont utilisées pour gérer :

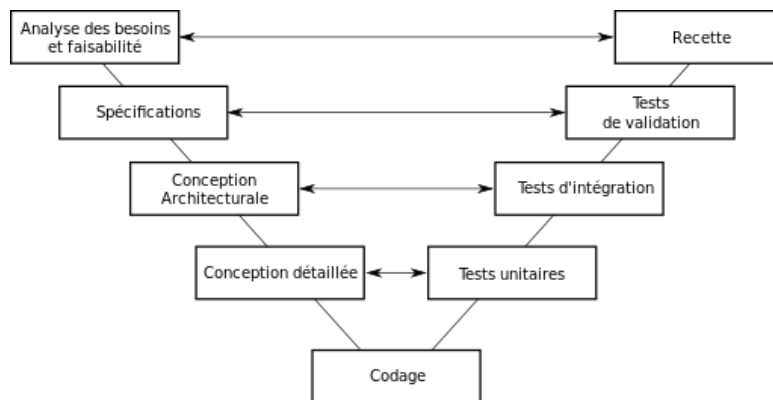
- les stocks
- la dette (les emprunts)
- les ressources humaines (et la paie)
- les immobilisations
- les achats (et la dette fournisseur)
- les recettes (et les créances)
- la trésorerie
- la comptabilité (générale ; analytique, budgétaire)
- la consolidation et le reporting
- les aspects décisionnels (en lien avec la mise en place d'une fonction de contrôle interne)
- autres domaines fonctionnels (à préciser)

ANNEXE 4- LES METHODOLOGIES DE PROJET

Il existe deux méthodes principales de gestion de projet : la méthode « cycle en V » et les méthodes « agiles ».

iv. La méthode « cycle en V »

Cette méthode est apparue dans les années 1980 et tient sa source du monde de l'industrie. Elle est caractérisée par un flux d'activité descendant détaillant le produit jusqu'à sa réalisation (des phases d'analyse des besoins et de faisabilité jusqu'à la phase de codage) ; puis un flux ascendant qui a pour objectif d'assembler le produit en vérifiant sa qualité (de la phase test unitaire à la phase de recette).



Les acteurs du « Cycle en V » :

MOA : (Maîtrise d'Ouvrage)

- ▶ Décide du lancement d'un projet et confie la réalisation à la MOE.
- ▶ Responsable du résultat du projet, assume l'usage du produit et finance sa réalisation.

PMO (Project management office) :

- ▶ Personne en charge de la planification des projets et du suivi de la mise en œuvre.

AMOA : (Assistance à maîtrise d'ouvrage)

- ▶ Assister la MOA en mettant en œuvre tout au long de sa mission des moyens et des compétences pour l'aider à atteindre ses objectifs.

MOE : (Maîtrise d'OEuvre) :

- ▶ Entité ou personne qui développe les logiciels correspondant aux besoins des utilisateurs.

Cette méthode est adaptée quand :	Les risques liés à cette méthode :
<ul style="list-style-type: none">• L'environnement est stable.• Les objectifs et les résultats sont connus à l'avance.• Le périmètre, le budget, et les ressources sont définis.• Le cadrage est clair et l'objectif est défini.	<ul style="list-style-type: none">• Les besoins ont changé entre l'analyse des besoins et la fin du projet et l'adaptation est difficile.• Chaque phase peut être longue, ce qui peut mener à des dérapages temporels et financiers.• Les rôles entre l'AMOA, la MOA et la MOE doivent être clairement définis.

v. « Les méthodes agiles »

Les méthodes agiles datent des années 2000 et proviennent du Manifeste Agile qui référence plusieurs méthodes existantes. Ces méthodes se veulent plus adaptatives et réactives que les méthodes traditionnelles. Elles reposent sur un cycle de développement itératif et collaboratif.

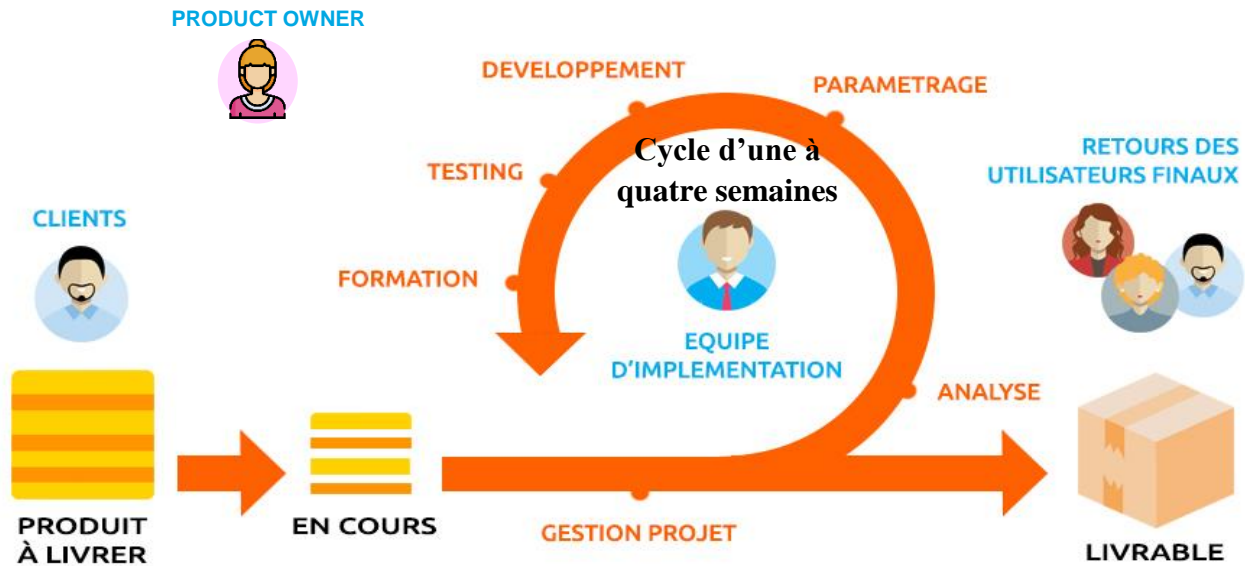






Figure 1: <https://www.mercator.eu/fr/la-methode-agile-comme-methode-de-travail-chez-mercator-explications.shtml>

- 

RETOURS DES UTILISATEURS FINAUX Les personnes qui utilisent le nouvel outil avec les nouveaux processus mis en place. Ils sont impliqués dans les test finaux des nouveaux outils.
- 

CLIENTS Fournit le cahier des charges détaillé correspondant à ses besoins.
- 

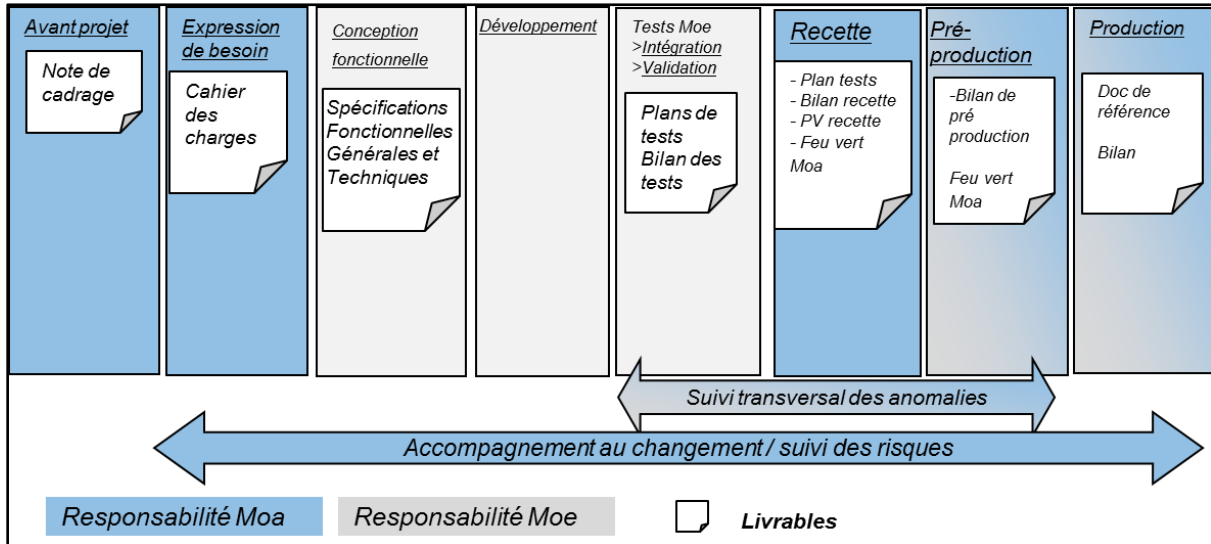
PRODUCT OWNER Représente les clients et les utilisateurs finaux dans le cadre du projet. Le product owner définit la roadmap à suivre pour que le produit s'adapte le mieux aux besoins des clients.
- 

EQUIPE D'IMPLEMENTATION Cette équipe est chargée de transformer les besoins exprimés par le client et/ou le product owner en fonctionnalités utilisables. Elle est pluridisciplinaire et peut faire appel à des rôles tels que développeurs, architectes logiciels, DBA, analystes fonctionnels, ingénieurs systèmes...

Cette méthode est adaptée quand :	Les risques liés à cette méthode :
<ul style="list-style-type: none">• L'objectif du projet est simple.• La communication au sein de l'équipe est efficace et simple.• L'ensemble des acteurs du projet sont pleinement impliqués sur le long terme.	<ul style="list-style-type: none">• Un rythme dense qui nécessite un suivi rigoureux de la méthode.• La définition du besoin n'est pas claire et le client n'a pas de besoin défini. Ceci peut engendrer des dérapages financiers et temporels importants.

ANNEXE 5- SCHEMA D'UN PROJET INFORMATIQUE

Représentation simplifiée des responsabilités et livrables dans le cycle de vie d'un projet informatique



ANNEXE 6- L'ARCHIVAGE DES DONNEES

Les productions des organismes publics entrent dans le cadre juridique des archives publiques qui prévoit des règles spécifiques de collecte, de traitement, de conservation et d'accès à l'information (Code du patrimoine, livre II).

A. Repères

Que sont les archives ?

Il s'agit des informations originales et fiables produites et reçues par une personne physique ou morale à l'appui d'une activité donnée (ce qui exclut les doublons, les éléments préparatoires et la simple documentation). Il est à noter que les archives revêtent ce statut dès leur création, quel que soit le lieu de stockage (bureaux, serveurs informatiques, magasins, etc.). De plus, la notion d'archives n'est pas attachée à un support en particulier.

Références :

- [Code du patrimoine, article L 211-1.](#)
- Norme ISO 15489-1, *Records management* : Partie 1: Principes directeurs.

Que sont les archives publiques ?

Il s'agit des archives relevant :

- de l'activité de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public,
- de la gestion d'un service public,
- ou de l'exercice d'une mission de service public par des personnes de droit privé.

Référence :

- [Code du patrimoine, article L 211-4.](#)

Pourquoi constituer des archives ?

Il y a trois enjeux :

- la gestion courante d'un service (disposer en permanence d'informations authentiques, fiables, intègres et exploitables nécessaires au bon fonctionnement d'un service),
- la justification des droits et des obligations (conserver les preuves en cas de contestation),
- la sauvegarde de la mémoire (constituer les matériaux de l'histoire).

Référence :

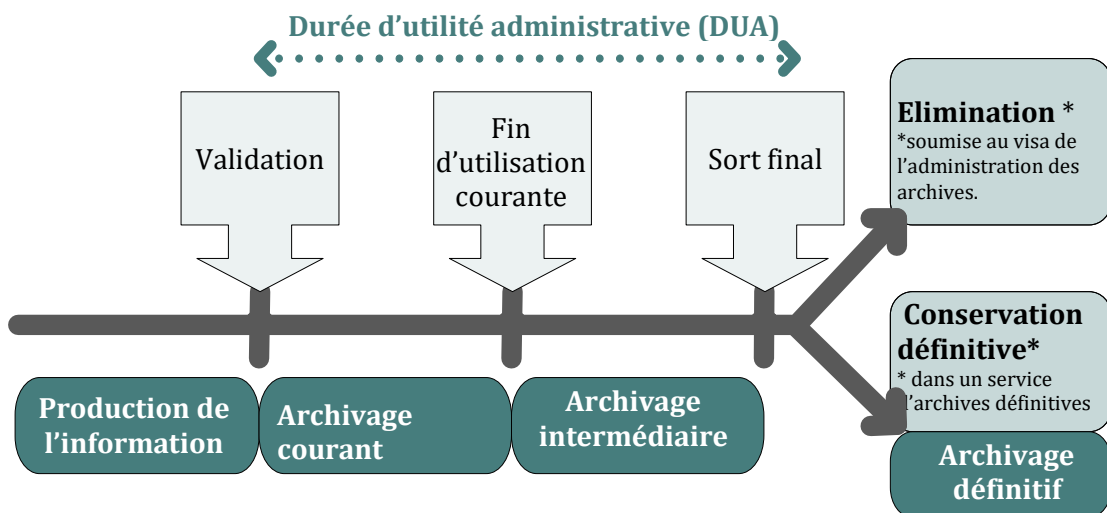
- [Code du patrimoine, article L 211-2.](#)

B. Le régime des archives publiques (papier et numériques)

i. [Le cycle de vie des archives](#)

La gestion des archives publiques repose sur un modèle uniforme de gestion de l'information qualifié de « cycle de vie ». Ce dernier articule trois âges successifs (correspondant aux enjeux précités) :

- **l'âge courant**, période pendant laquelle les archives sont conservées à proximité immédiate du producteur pour la conduite des affaires en cours,
- **l'âge intermédiaire** pendant lequel les archives sont conservées dans un environnement plus distant (« base archives » ou local de pré-archivage) pour répondre à des besoins d'ordres juridique (délais de prescription) ou fonctionnel (accès à l'antériorité des informations).
- **l'âge définitif** qui voit le transfert des archives présentant un intérêt historique dans un service historique d'archives. Les archives dénuées d'un tel intérêt sont quant à elles éliminées à l'issue de l'âge intermédiaire avec l'autorisation préalable de l'administration des archives.



La mise en œuvre de ce schéma suppose en amont, la définition de règles d'archivage soient :

- un sort final, l'élimination ou la conservation définitive,
- et une « durée d'utilité administrative » (DUA) qui est le délai de conservation par le service producteur avant l'application du sort final. La DUA est établie suivant le cadre juridique en vigueur (délais de prescription, protection des données à caractère personnel) et les besoins fonctionnels propres aux services (accès à l'antériorité des informations)

Notons que le respect du cycle de vie des archives favorise par là même la bonne gestion des données à caractère personnel (cf. [fiche 7](#))

ii. Le contrôle scientifique et technique de l'Etat (CST)

Les producteurs d'archives publiques sont placés sous le contrôle scientifique et technique de l'Etat qui est « le moyen juridique dont l'État dispose pour garantir, au nom de l'intérêt général, la constitution d'un patrimoine informationnel national de qualité »⁸.

⁸ [Comité interministériel aux Archives de France, Référentiel général de gestion des archives \(R2GA\)](#), 2013, p.42

Ce contrôle porte sur les conditions de gestion, de collecte, de sélection et d'élimination ainsi que sur le traitement, le classement, la conservation et la communication des archives.

Il est exercé par :

- les ministères des armées et des affaires étrangères, chacun pour leur périmètre (Code du patrimoine, articles [R212-6](#) et [74](#))
- et par le ministère de la Culture (Service interministériel des archives de France) pour le reste des producteurs d'archives publiques [Code du patrimoine, article [R 212-2](#)]

Ce contrôle se traduit notamment par l'obligation pour le service producteur d'obtenir une autorisation écrite de l'administration des archives pour toute élimination d'archives (bordereau d'élimination).

Pour en savoir plus :

- [Comité interministériel aux Archives de France, Référentiel général de gestion des archives \(R2GA\), 2013, 67 p.](#)

C. La spécificité des archives numériques

La dématérialisation des procédures administratives entraîne la production d'originaux numériques dont l'archivage met en œuvre des outils spécifiques.

En effet, si l'article 1366 du Code civil confère à l'écrit numérique la « même force probante » que le support papier, ce principe est soumis à double condition d'authenticité et d'intégrité. Il faut ainsi que « puisse être dûment identifiée la personne dont [l'écrit] émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. ».

Le respect de ces conditions nécessite le recours à une signature électronique pour les actes juridiques (Code civil, article 1367) et l'emploi d'un « système d'archivage électronique », garant de l'intégrité, de la fiabilité et de la pérennité des documents dans le temps.

Pour en savoir plus :

- Site internet « France Archives » (Service interministériel des archives de France), Cadre réglementaire et normatif des archives numériques : <https://francearchives.fr/fr/section/88482500>.
- Lorène Béchar, Lourdes Fuentes Hashimoto, Edouard Vasseur, *Les Archives électroniques*, Paris, Association des archivistes français (AAF), 2020, 96 p.

Exemples de DUA réglementaires

- Pièces justificatives comptables

Pour les ordonnateurs : DUA de 10 ans.

- Le Code des juridictions financières dispose d'un délai de prescription de dix ans pour les actes constitutifs de gestion de fait ([article L 131-2](#)).
- Les différentes instructions du Ministère de la culture (SIAF) préconisent d'aligner sur ce délai la durée de conservation des pièces comptables détenues par les ordonnateurs.
 - o [Instruction n°DAF/DPACI/RES/2008/008 relative à la durée d'utilité administrative des documents comptables détenus par les ordonnateurs.](#)
 - o [Note d'information DGP/SIAF/2018/003 relative à la durée d'utilité administrative des pièces justificatives des comptes et des dossiers de marchés publics.](#)
- Le Ministère de l'action et des comptes publics a rappelé cette règle des dix ans dans son [guide sur l'archivage applicable aux ordonnateurs et aux comptables publics dans le cadre de la dématérialisation](#) (2019).

Pour les comptables : DUA d'un an après le jugement définitif des comptes ou 5 ans à compter du 31 décembre de l'année de production du compte

- L'article 60 de la loi n°63-156 modifiée fixe à 5 ans le délai de prescription des comptes au profit du comptable public.
- La circulaire n°DGP/SIAF/2012/009 du 10/07/2012 relative au traitement et à la conservation des archives des chambres régionales et territoriales des comptes préconise d'aligner sur ce délai la durée de conservation des pièces financières détenues par les comptables.

- Dossiers de marchés publics

Dans le cas des marchés publics, il convient de distinguer le dossier de passation et le dossier d'exécution du marché :

Pour la procédure de passation (offres, avis de publicité), les DUA sont prescrites par le décret 2016-360 du 25 mars 2016 relatif aux marchés publics :

- 5 ans pour les marchés publics de fournitures ou de services ;
- 10 ans pour les marchés de travaux, de maîtrise d'œuvre ou de contrôle technique à compter de la fin de l'exécution du marché public ;
- 5 ans à compter de la date de signature du marché pour les candidatures et offres non retenues ainsi que les documents relatifs à la procédure de passation pendant une période minimale.

Pour le dossier d'exécution, les DUA sont les suivantes :

- 10 ans à compter de la fin du marché (paiement du solde) pour l'ordonnateur (prescription de la gestion de fait, art. L131-2 et L231-3 du code des juridictions financières) ;
- 3 ans à compter du 31 décembre suivant la présentation des comptes dans le cas de marché cofinancé sur des fonds structurels européens (art. 140 du règlement (UE) n° 1303/2013) ;
- 30 ans pour les marchés de travaux à compter de la réception des travaux dans le cas de risques environnementaux (art. L152-1 du code de l'environnement) ;
- 70 ans après la mort de l'auteur pour les pièces d'un marché portant cessions des droits patrimoniaux sur une œuvre de l'esprit (art. L123-1 sqq. du code de la propriété intellectuelle.).

- Dossier individuels des agents publics

Suite à l'arrêté du 21 décembre 2012, La durée d'utilité administrative (DUA) du dossier individuel des agents publics est désormais fixée à 80 ans à compter de la date de naissance de l'agent. Cette nouvelle DUA est applicable à l'ensemble des dossiers individuels des agents publics qu'ils soient gérés sur support électronique ou sur support papier. Le tableau de la [note d'information DGP/SIAF/2014/001](#) contient les durées de conservation pour gestion courante de certains documents à l'intérieur du dossier.

Pour en savoir plus : <https://www.cnil.fr/fr/limiter-la-conservation-des-donnees>

ANNEXE 7 - BONNES PRATIQUES SUR LES MOTS DE PASSE

Contrainte	Valeur préconisée
Le premier mot de passe, par défaut, doit être défini aléatoirement par le système.	Oui
Obligation de changer le mot de passe lors de la première connexion.	Oui
Durée de vie maximale d'un mot de passe.	90 jours
Longueur minimale du mot de passe.	8 caractères
Obligation de recourir à des caractères alphanumériques et/ou caractère spéciaux.	Oui
Historisation des derniers mots de passe.	5
Nombre maximal de tentatives infructueuses de connexion avant blocage du compte.	3
Durée de vie minimale.	1 jour

ANNEXE 8 - LES FORMATIONS

Le pôle formation du centre d'appui métier propose de nombreuses formations d'une durée variable permettant de se familiariser avec l'environnement numérique, la culture de la donnée ou le contrôle des systèmes d'information.

Enjeux du numérique - volet contrôle des systèmes d'information

[Module de deux jours et demi](#) permettant d'acquérir une démarche simple et pragmatique :

- de l'audit des systèmes d'information d'un organisme, sur la base du guide de contrôle proposé par la direction des méthodes et des données du Centre appui métier,
- d'analyses rapides des données obtenues par un organisme contrôlé.

Des formations plus spécifiques peuvent également être organisées en amont d'un contrôle.

Enjeux du numérique - volet données

[Module de deux jours et demi](#) permettant de :

- rechercher et s'appropriier des sources données,
- dialoguer avec les data-scientists et comprendre leurs conclusions,
- s'appropriier des traitements et des indicateurs statistiques, de leur construction à leur bonne utilisation, afin de les intégrer dans des communications,
- maîtriser les concepts de la statistique descriptive afin de comprendre l'information statistique et d'éviter les pièges d'interprétation,
- réaliser des traitements simples sur des données unidimensionnelles et présenter les résultats obtenus à l'aide de tableaux, de graphiques et d'indicateurs numériques.

Le diplôme universitaire de contrôle en environnement numérique

La première édition de ce [nouveau diplôme universitaire](#), comprenant 25 jours de formation, se déroule à l'université Paris-Dauphine d'octobre à avril. Réparti en quatre blocs d'enseignement de six jours chacun (plus un jour d'accompagnement au mémoire), il implique la soutenance obligatoire d'un mémoire individuel ou de travaux collectifs en rapport avec la question du numérique dans la gestion publique. Comme pour le DU « Audit de la gestion des organisations publiques », ce diplôme spécialisé est proposé à des magistrats, rapporteurs ou vérificateurs des juridictions financières, chaque promotion comprenant 12 à 18 auditeurs.

Conditions à la candidature

Avoir déjà suivi les deux modules internes « enjeux du numérique » (volet « données » et volet « audit SI »). En sont toutefois exemptés ceux pouvant justifier d'un niveau de compétence antérieure sur le numérique qui sera vérifié par la commission de sélection des candidatures.

Power Query - Module d'informatique décisionnelle intégré à Excel

[Module d'une journée](#) destiné aux personnels de CRTC et permettant :

- d'aborder progressivement la réalisation de requêtes Power Query à partir de différentes sources,
- d'apprécier les différents types de chargement de données,
- et de s'appropriier les principales fonctionnalités de l'éditeur de requête.

De même les modalités de comparaison de requête (ajout, fusion, différentes liaisons) sont abordées. S'agissant d'une découverte progressive des potentialités de Power Query dans l'environnement professionnel, les apprentissages se font à partir d'exemples liés au contrôle.

ANNEXE 9 - REFERENCES

A. Les éléments stratégiques et règlementaires sur la transformation numérique

- **Sur le cloud**

Stratégie gouvernementale en 3 cercles

<https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-en-matiere-de-cloud/>

Projet européen Gaia-X

<https://www.lesnumeriques.com/vie-du-net/qu-est-ce-que-gaia-x-le-meta-cloud-europeen-n151195.html>

- **Sur les projets innovants**

Les entrepreneurs d'intérêt général

<https://entrepreneur-interet-general.etalab.gouv.fr/>

Les hackatons

https://www.modernisation.gouv.fr/sites/default/files/fiche_des_projets_numeriques_montez_un_hackathon_2.pdf

Les start-ups d'Etat

<https://beta.gouv.fr/startups/>

Les laboratoires d'innovation publique

<https://www.modernisation.gouv.fr/etudes-et-referentiels/etudes/les-laboratoires-dinnovation-publique-bilan-et-referentiel-devaluation>

- **Sur les données**

Tableau classifiant la sensibilité des données et la réglementation applicable par type d'entité, ANSSI

<https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/>

Plateforme ouverte des données publiques françaises

<https://www.data.gouv.fr/fr/>

Règles de sauvegarde des Systèmes d'Information de Santé (SIS)

https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi_guide_regles_sauvegarde_v1.0.pdf

Règlement général sur la protection des données- CNIL

<https://www.cnil.fr/fr/designation-dpo>

<https://www.cnil.fr/fr/les-violations-de-donnees-personnelles>

<https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail>

- **Sur la sécurité numérique**

Sécurité numérique des collectivités territoriales, L'essentiel de la réglementation, ANSSI

<https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite-numerique-collectivites-territoriales-reglementation.pdf>

Politique de sécurité des systèmes d'information de l'Etat

<https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/>

Référentiel général de sécurité

<https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>

Politique de sécurité des activités d'importance vitale

<http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf>

B. Les guides thématiques

- Guide d'audit de la **gouvernance** du SI d'une entreprise numérique par le CIGREF, l'AFAI et l'IFACI

<https://www.cigref.fr/mise-a-jour-2019-guide-audit-gouvernance-systeme-information-entreprise-numerique-cigref-afai-ifaci-2019>

- Guides relatifs au **contrôle interne des SI**

GTAG1-2^{ème} édition, Les contrôles et le risque des systèmes d'information, CRIPP Institute of Internal Auditors

https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%201%20-%20Les%20contrôles%20des%20systèmes%20de%20l%27information_2e%20éd.pdf

Les résultats de l'étude « Risk in Focus »

https://chapters.theiia.org/montreal/ChapterDocuments/Risk%20in%20Focus_2019.pdf

Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne, CIGREF et IFACI - février 2009

https://chapters.theiia.org/montreal/ChapterDocuments/Le%20contrôle%20interne%20du%20système%20d'information%20des%20organisations_IFACI-CIGREF%20%28février%202009%29.pdf

- Guide des **contrôles applicatifs**

GTAG8- Audits des contrôles applicatifs, CRIPP Institute of Internal Auditors

<https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%208%20-%20Audit%20des%20contrôles%20applicatifs.pdf>

- Guide sur la **cartographie des systèmes d'information**

Guide d'élaboration en 5 étapes, ANSSI

<https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf>

- Guide sur la **gestion des données**

Guide des mécanismes de protection de l'intégrité des données stockées

https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi-s_guide-integrite-des-donnees-1.0_0.pdf

Etude sur le cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales

https://www.territoire-numerique.org/wp-content/uploads/2019/04/FNCCR-Etude-cycle-de-la-donn%C3%A9e-v29032019_version-d%C3%A9finitive.pdf

Guide de la CNIL sur la sécurité des données personnelles

<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>

- Méthode interministérielle d'**analyse de la valeur des projets** - MAREVA 2

<http://references.modernisation.gouv.fr/mareva2-cest-quoi>

- Méthode de conduite de projets informatiques

<https://hal.archives-ouvertes.fr/cel-02004689/document>

C. Sur les prestataires informatiques

- Référentiel ISA 3402

<https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isaie-3402.pdf>

- Référentiel SECNUM CLOUD pour les prestataires de Cloud

<https://www.ssi.gouv.fr/actualite/secnumcloud-evolue-et-passe-a-lheure-du-rgpd/>

- Risques liées aux marchés informatiques

Article L8231-1 et Article L8241-1 du code du travail

<https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006904839&cidTexte=LEGITEXT000006072050&dateTexte=20080501>

<https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072050&idArticle=LEGIARTI000006904846&dateTexte=&categorieLien=cid>



Réalisé par la
**Direction des méthodes et des
données**
Centre d'appui métier