Guide Technique d'Accréditation – Systèmes d'information dématérialisés

GEN GTA 02 - Révision 01

SOMMAIRE

1 OBJET

Quel que soit son domaine d'activité, tout organisme est concerné par la maîtrise des informations inhérentes aux prestations d'évaluation de la conformité qu'il réalise. Actuellement, de nombreuses données et informations sont gérées de manière informatisée (dématérialisée), aussi bien pour rendre compte des résultats des prestations d'évaluation de la conformité que pour en assurer la traçabilité requise. Ainsi, la question de la gestion du système d'information dématérialisé est centrale pour bon nombre d'organismes. L'enjeu pour les organismes est notamment de savoir quelles politiques et quelles pratiques mettre en œuvre pour satisfaire aux différentes exigences qui s'imposent à lui (légales ou liées à l'accréditation) tout en tirant le meilleur parti de l'informatisation pour concourir à la performance de l'organisme.

Ce document vise à apporter des éléments d'information et des pistes de réflexion concernant la gestion des systèmes d'information dématérialisés. L'objectif est également de mettre en exergue les points clefs à maîtriser au regard des exigences introduites par les référentiels d'accréditation. Plus largement, ce guide a vocation à constituer une base de réflexion commune pour les organismes et les évaluateurs autour du sujet de la maîtrise des données relatives aux prestations d'évaluation de la conformité dans un contexte de gestion informatisée. S'agissant d'un guide transversal, celui-ci se focalise sur les items communs aux différents référentiels d'accréditation.

L'approche choisie pour ce guide consiste à :

- Partie I : Aborder des généralités relatives aux systèmes d'information : définition et architecture du système d'information, notions de sécurité de l'information,
- Partie II : Présenter des éléments relatifs à la gestion du système d'information : gouvernance, gestion des ressources, pilotage et gestion de projets,
- Partie III : Se concentrer sur les exigences communes aux différents référentiels d'accréditation en présentant notamment des exemples de moyens pour y répondre et des points pouvant être abordés lors des évaluations. Ces derniers peuvent également constituer une base de réflexion pour identifier les points clefs à maîtriser par les organismes ou encore pour développer des outils d'auto-évaluation ou d'audit interne.

Les éléments indiqués dans ce guide, en particulier dans les pistes de réflexion, sont donnés à titre informatif et n'ont pas valeur d'exigence opposable aux organismes dans le cadre de l'accréditation.

Ce document ne se substitue pas aux exigences et/ou normes applicables au sein des organismes. En effet, chaque organisme est libre de prendre en compte et d'appliquer ou non les recommandations contenues dans ce guide. Par ailleurs, il appartient toujours aux organismes de démontrer que les dispositions prises leur permettent de satisfaire pleinement aux exigences d'accréditation qui leur sont opposables.

2 REFERENCES ET DEFINITIONS

2.1 Références

ISO 10007 : Systèmes de management de la qualité – Lignes directrices pour la gestion de la configuration.

NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences

NF EN ISO/CEI 27002 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les mesures de sécurité de l'information

NF ISO 31000 : Management du risque – lignes directrices

Cartographie du système d'information – Guide d'élaboration en 5 étapes (Version 1.0) – ANSSI[1]

Charte d'utilisation des moyens informatiques et des outils numériques - Guide d'élaboration en 8 points clés pour les PME et ETI (Version 1.0) – ANSSI[1]

Guide d'Hygiène Informatique – Renforcer la sécurité de son système d'information en 42 mesures (version 2.0) – ANSSI[1]

Maîtriser les risques de l'Infogérance – Guide de l'externalisation des systèmes d'information (Décembre 2010) – ANSSI[1]

Le risque informatique – document de réflexion de janvier 2019 – Autorité de Contrôle Prudentiel et de Résolution ACPR – Banque de France[2]

GAMP 5 - Une approche de la conformité des systèmes informatisés BPx basée sur les risques[3]

OECD Series on principles of good laboratory practice and compliance monitoring – number 17 – Application of GLP Principles of Computerised Systems[4]

2.2 Abréviations et définitions

⇨ **Abréviations :**

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ESN : Entreprise de Service du Numérique (anciennement SSII : Société de Service et d'Ingénierie Informatique)

GED : Gestion Electronique des Documents

GTC : Gestion Technique Centralisée (pour le suivi des températures par exemple)

MCO : Maintien en Condition Opérationnelle

MOA : Maîtrise d'Ouvrage

MOE : Maîtrise d'Œuvre

NAS : Serveur de stockage en réseau (Network Attached Stockage)

PCA : Plan de Continuité d'Activité

PRA : Plan de Reprise d'Activité

PGI : Progiciel de Gestion Intégrée (en anglais **ERP** / Enterprise Ressource Planning)

SIL (ou SGL) : Système de gestion de l'Information de Laboratoire (en anglais **LIMS /** Laboratory Information Management System)

TMA : Tierce Maintenance Applicative

VPN : réseau privé virtuel (Virtual Private Network)

⇨ **Définitions :**

La plupart des définitions sont extraites du site Internet de l'ANSSI - https://www.ssi.gouv.fr/.

Big data : Le concept de « big data » traduit le fait que les organismes sont amenés à traiter des volumes de données (data) considérables, quasi en temps réel. Le cerveau humain peine à analyser un nombre aussi important d'informations complexes. Il devient ainsi nécessaire de s'appuyer sur des logiciels de traitement des données pour sécuriser les prises de décision.

[1] Disponible sur https://www.ssi.gouv.fr/
[2] Disponible sur https://acpr.banque-france.fr/
[3] Disponible sur https://ispe.org/
[4] Disponible sur http://www.oecd.org/

Commutateur ou switch : composant gérant les connexions entre les différents serveurs au sein d'un réseau.

Confidentialité : propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

Cloud computing : mode de traitement des données, dont l'exploitation s'effectue par internet, sous la forme de services fournis par un prestataire. Le Cloud computing est ainsi une forme d'infogérance, qui consiste à utiliser des serveurs informatiques par l'intermédiaire d'un réseau, généralement Internet, pour stocker des données ou les exploiter. En règle générale, le fonctionnement du Cloud computing et la localisation des serveurs, donc des données, ne sont pas portés à la connaissance des clients.

Donnée primaire : donnée observée.

Donnée secondaire : donnée calculée à partir des données primaires.

Faille : vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Firmware : programme intégré dans un matériel pour qu'il puisse fonctionner. On parle aussi de logiciel interne ou logiciel embarqué.

Hameçonnage (phishing, filoutage) : vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Remarque : les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.

Logiciel espion (espiogiciel, spyware) : logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

Logiciel malveillant (malicious software, malware) : tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau. Remarques : Les virus ou les vers sont deux types de codes malveillants connus. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante.

Logiciel pare-feu (firewall) : outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

Métadonnée : donnée qui permet de décrire les attributs d'une autre donnée ou d'apporter des informations complémentaires (par exemple : personne qui a généré la donnée, date à laquelle la donnée a été produite, unités…).

Middleware : logiciel tiers permettant l'échange d'information entre différentes applications informatiques.

Organisme (dans ce document) : organisme accrédité ou candidat à l'accréditation.

Plan de Continuité d'Activité : Organisation / procédure permettant la continuité de l'activité en général ou de certaines activités essentielles, quel que soit le dysfonctionnement ou problème rencontré.

Plan de Reprise d'Activité : Organisation / procédure permettant la reprise de l'activité sous un délai préalablement défini, en fonction de la criticité des activités impactées.

Qualification de la Conception (QC) : phase de tests qui permet de s'assurer que chacun des éléments du système informatique est conçu conformément au cahier des charges, aux réglementations et normes en vigueur.

Qualification d'Installation (QI) : phase de tests qui permet de s'assurer que chacun des éléments du système informatique est installé conformément au cahier des charges, aux recommandations du fournisseur et aux réglementations en vigueur.

Qualification Opérationnelle (QO) : phase de tests qui permet de s'assurer que le système informatique est capable de fonctionnements conformes répétés dans les limites déterminées par le cahier des charges et les spécifications. Elle permet de vérifier la conformité de toute fonctionnalité critique du système, prise séparément.

Qualification de Performance (QP) : phase de tests qui permet de s'assurer que le système informatique fonctionne correctement dans des conditions réelles d'utilisation, conformément au cahier des charges et que tous les éléments nécessaires à l'utilisation en production du système sont disponibles.

Rançongiciel (ransomware) : forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon. Lorsqu'un rançongiciel infecte un poste de travail, le plus souvent (mais pas nécessairement) par l'envoi d'un courrier électronique piégé, l'infection est dès lors susceptible de s'étendre au reste du système d'information (serveurs, ordinateurs, téléphonie, systèmes industriels…).

Résilience : en informatique, capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident.

Réversibilité : dans les contrats informatiques, faculté pour le client (utilisateur du logiciel ou du système objet du contrat) de récupérer ses données lors de la cessation du contrat, ou plus généralement la faculté de reprendre, au terme du contrat, l'exploitation des données ou d'un logiciel ou même d'un système d'information complet, dans le cadre d'une migration chez un autre éditeur de progiciel, un autre infogérant, une autre infrastructure informatique (data center).

Routeur : composant gérant les connexions entre différents réseaux.

Schéma directeur : plan stratégique pluriannuel qui permet de prévoir et d'anticiper l'évolution du système d'information.

Test fonctionnel : test qui permet de tester une fonctionnalité (la connexion d'un utilisateur par exemple). Ces fonctionnalités sont testées via des parcours en simulant les actions de l'utilisateur (clics, saisies claviers, mouvement de souris, …). Les tests fonctionnels sont faits tout au long de la vie du projet informatique, et ce dès le développement de la première fonctionnalité.

Test Grandeur Nature : test qui permet de s'assurer du bon fonctionnement du logiciel dans un environnement identique à celui de production.

Test d'intégration : test qui permet de s'assurer que le logiciel s'intègre bien dans son environnement informatique et communique avec les autres logiciels du système d'information (par exemple : SIL ↔ Middleware ↔ logiciel embarqué d'un automate…).

Test de non-régression : test qui permet de s'assurer que les modifications et évolutions apportées par les développeurs n'ont pas entrainé d'effet de bord (c'est-à-dire altération de parties du code non modifiées). Ils ne sont réalisés que lorsqu'une nouvelle version logicielle est livrée.

Test unitaire : test qui permet de s'assurer du fonctionnement correct d'une partie déterminée d'une application ou d'une partie d'un programme. Il a pour objectif d'isoler le comportement de la partie de code à tester de tout facteur extérieur et de vérifier qu'il est conforme à ce qui est attendu. Le test unitaire va donc être écrit pour tester une toute petite partie du code source, indépendamment de l'environnement qui l'entoure. Il doit être déterministe, c'est-à-dire qu'exécuté plusieurs fois, il devra toujours donner le même résultat.

Validation : vérification où les exigences spécifiées sont adéquates pour un usage déterminé [Source : Guide ISO/IEC 99:2007, 2.45].

Vérification : fourniture de preuves tangibles qu'une entité donnée satisfait à des exigences spécifiées [Source : Guide ISO/IEC 99:2007, 2.44].

Ver (ou Worm) : logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. Remarques : Les deux termes ver et virus sont relativement proches. Un ver est un virus qui se propage de manière quasi autonome (sans intervention humaine directe) via le réseau. Les vers sont donc une sous-catégorie de virus, dont le vecteur primaire de propagation reste le réseau.

Virtualisation : mécanisme informatique qui consiste à faire fonctionner plusieurs systèmes, serveurs ou applications, sur un même serveur physique. La virtualisation est un composant technique clé dans le Cloud Computing.

Virus : programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB…

Vulnérabilité : faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Remarques : une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

3 DOMAINE D'APPLICATION

Ce document s'adresse aux organismes utilisant un ou des systèmes d'information dématérialisés dans le cadre des prestations de leur portée d'accréditation (actuelle ou demandée).

Il s'adresse également aux évaluateurs du Cofrac, à ses membres d'instances et à son personnel.

4 MODALITES D'APPLICATION

Ce guide est applicable à compter du 01/06/2024.

5 MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

La révision du document porte uniquement sur la révision de l'Annexe 4 - Récapitulatif des exigences communes aux différents référentiels, pour y intégrer la révision 2022 de la norme NF EN ISO 15189 et la norme NF EN ISO/IEC 17029, et ne plus y traiter les normes NF X 50-091 et ISO 14065:2013 obsolètes.

6 PARTIE *I : GENERALITES RELATIVES AUX SYSTEMES D'INFORMATION*

Rappel : Comme indiqué dans le § 1. Objet, les éléments indiqués dans ce guide sont donnés à titre informatif et n'ont pas valeur d'exigence opposable.

6.1 Définition d'un système d'information

Le système d'information, peut être entendu comme l'ensemble des ressources (moyens matériels et moyens humains) destinées à collecter, classifier, traiter, stocker, gérer et diffuser les informations au sein d'un organisme.

Le système d'information comprend la gestion des données et informations contenues dans les systèmes informatiques et non informatisés. Ce guide porte uniquement sur les éléments informatisés du système d'information.

Pistes de réflexion

Les moyens matériels constitutifs du système d'information peuvent être, à titre d'exemple :

- ***Les logiciels :*** *PGI, SIL, Middleware, GED, GTC, outil de gestion des équipements, logiciel embarqué pilotant un équipement (firmware), logiciel pour la saisie des données hors-site (via une tablette ou un smartphone, pour un prélèvement, une inspection, une évaluation, un étalonnage…), logiciel pare-feu, logiciel anti-virus, logiciel de calcul, système d'exploitation, outil permettant la diffusion d'un résultat…*
- ***L'infrastructure physique :*** *câbles, routeurs, serveurs, commutateurs… Cette infrastructure peut être hébergée au sein de l'organisme ou située hors des locaux de l'organisme (Cloud…). Pour cela, il peut être nécessaire de créer une version virtuelle d'équipements physiques comme des serveurs, des systèmes de stockage ou des réseaux virtuels (on parle alors de virtualisation).*
- ***Les équipements bureautiques :*** *station de travail, ordinateur portable, smartphone, tablette, imprimante, scanner…*
- ***Les locaux :*** *salle des serveurs, moyens de maîtrise des conditions d'accès aux locaux de l'organisme…*

En pratique

Connaître son système d'information, c'est connaître les éléments qui le composent, son architecture, ses interrelations. Dans un contexte numérique, la cartographie est un outil permettant de représenter le système d'information ainsi que ses connexions avec l'extérieur – cf. § 6.2 « Architecture du système d'information ».

6.2 Architecture du système d'information

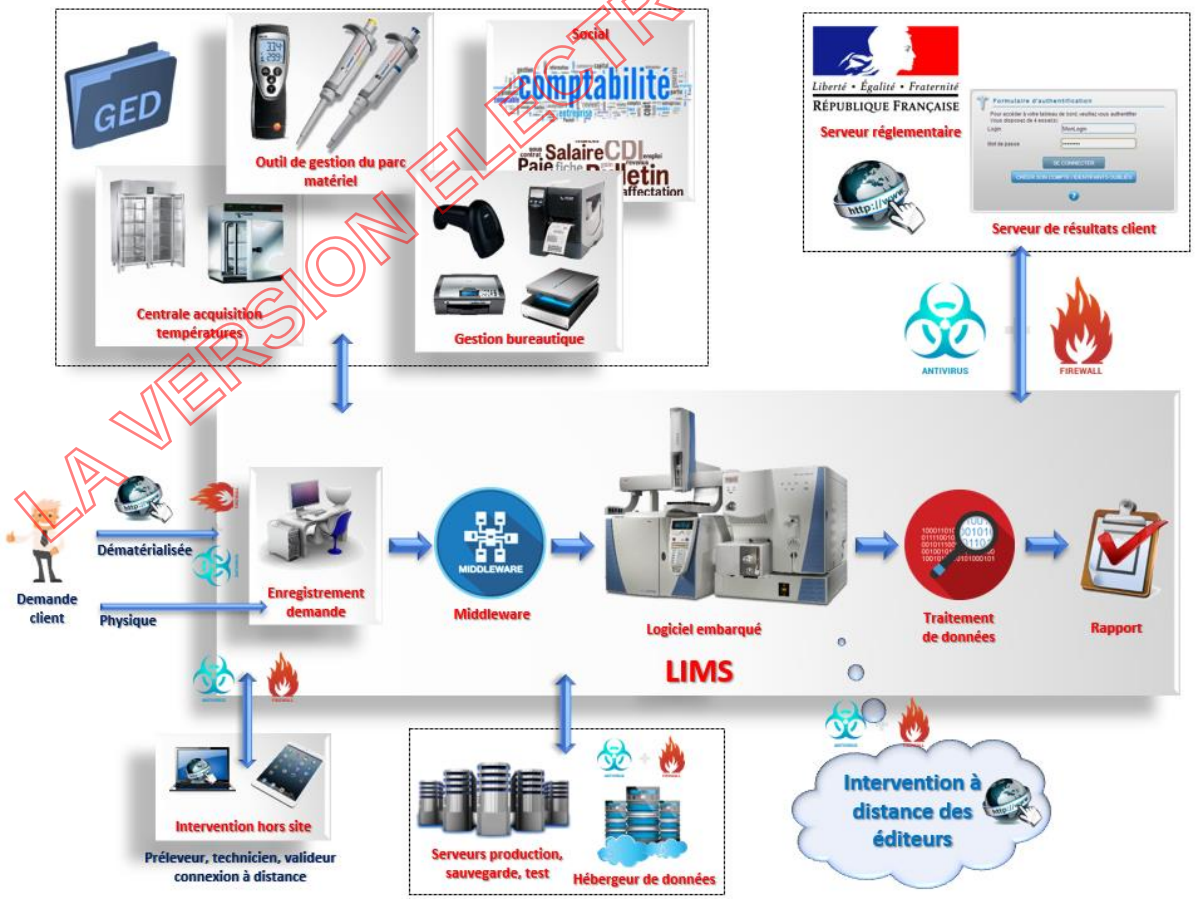
Connaître l'architecture de son système d'information est une condition essentielle pour en assurer la maîtrise et la protection. Mais comment avoir une vision claire d'un système d'information qui apparaît complexe, multiple, ouvert sur l'extérieur ?

Pistes de réflexion

Dans un contexte numérique, la cartographie permet de représenter le système d'information 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.

L'élaboration d'une cartographie du système d'information s'intègre dans une démarche générale de gestion des risques et répond à trois enjeux :

- ***La maîtrise du système d'information** : la cartographie permet de disposer d'une vision commune et partagée du système d'information au sein de l'organisme. C'est un outil indispensable au pilotage de l'évolution du système d'information. Elle facilite également la capitalisation d'expérience et la prise de décision grâce à un langage simple et visuel ;*
- ***La protection et défense du système d'information** : la cartographie permet d'identifier les systèmes les plus critiques et les plus exposés, d'anticiper les chemins d'attaque possibles sur ces systèmes et de mettre en place des mesures adéquates pour assurer leur protection. Elle permet de réagir plus efficacement en cas d'incident ou d'attaque numérique ;*
- ***La disponibilité du système d'information** : la cartographie permet d'identifier les activités clefs de l'organisme afin d'en assurer la disponibilité (via par exemple un Plan de Continuité d'Activité - PCA ou un Plan de Reprise d'Activité - PRA) et s'impose comme un outil indispensable à la gestion de crise, qu'elle soit numérique ou non.*



Exemple d'une cartographie simplifiée du système d'information d'un laboratoire

En pratique

Pour établir sa cartographie, l'organisme peut suivre les étapes suivantes :

- ***Etape 1 – initier la démarche de cartographie :*** *définir les enjeux de la cartographie, les acteurs à mobiliser, le périmètre du système d'information à représenter, le niveau de détail de l'inventaire et les types de vues à réaliser, les différentes itérations et le calendrier associé ;*
- ***Etape 2 – définir le modèle de cartographie :*** *recenser toutes les informations disponibles en rassemblant les inventaires et schémas de représentation du système d'information déjà constitués. Définir le modèle de représentation de la cartographie et des différentes vues ainsi qu'une nomenclature pour les différents objets ;*
- ***Etape 3 – construire sa cartographie :*** *en mettant à jour, le cas échéant, les informations recensées. Représenter les différentes vues de la cartographie selon le modèle choisi ;*
- ***Etape 4 – pérenniser sa cartographie :*** *diffuser et promouvoir la cartographie au sein de l'organisme. Mettre en place un processus de mise à jour de la cartographie et la gouvernance associée.*

En savoir plus

Cartographie du système d'information – Guide d'élaboration en 5 étapes de novembre 2018 (Version 1.0) – ANSSI

6.3 Concepts de sécurité de l'information

Dans un environnement de plus en plus connecté, les cybermenaces qui pèsent sur le système d'information d'un organisme prolifèrent : logiciel espion, logiciel malveillant, virus, hameçonnage, rançongiciel, intrusion… Ces menaces augmentent lorsque le système d'information s'ouvre sur l'extérieur, par exemple dans le cas des connexions à distance (télétravail, prise de contrôle d'un logiciel par un éditeur en cas de panne ou de maintenance…), dans le cas de diffusion d'informations sur des serveurs externes (serveur de résultats dans le domaine de la Santé…), ou plus simplement lorsque le personnel de l'organisme ouvre une pièce jointe annexée à un e-mail.

Tout organisme est amené à s'interroger sur la manière de définir le niveau de sécurité de son système d'information, d'évaluer si son système d'information est correctement sécurisé. Globalement, la question qui se pose est : Comment identifier les failles relatives à la sécurité ?

L'objet de ce chapitre n'est pas d'indiquer une conduite à tenir à ce sujet mais plutôt de délivrer des éléments de réflexion concernant des éléments clefs à prendre en compte pour mettre en œuvre un dispositif de maîtrise de la sécurité de l'information. Par ailleurs, de nombreux aspects de la sécurité de l'information sont en cohérence complète avec les exigences d'accréditation (traçabilité, confidentialité, etc.).

Pistes de réflexion

*Pour répondre à la problématique de sécurité de l'information, l'organisme peut conduire une analyse de la sécurité de son système d'information en fonction de quatre critères (**DICP**) :*

- ***D - Disponibilité :*** *il s'agit de garantir le bon fonctionnement des outils informatiques pour assurer la continuité des services aux utilisateurs. Pour assurer cette continuité, l'organisme peut mettre en place un Plan de Continuité d'Activité (**PCA** – continuité de l'activité quel que soit le*

*dysfonctionnement ou problème rencontré) ou un Plan de Reprise d'Activité (**PRA** – reprise de l'activité sous un délai préalablement défini, en fonction de la criticité de l'activité impactée) ;*

- ***I - Intégrité :** mise à disposition de données de qualité, dans les temps et espaces prévus. Pour assurer cette intégrité, il convient de vérifier que les données sont :*
  - ✓ ***Exactes** : Aucune erreur ou correction sans modifications documentées,*
  - ✓ ***Lisibles :** Données lisibles tout au long de leur cycle de vie (y compris les données archivées),*
  - ✓ ***Contemporaines :** Documentées en même temps que l'activité se déroule,*
  - ✓ ***Originales :** Enregistrement original ou copie certifiée conforme,*
  - ✓ ***Attribuables :** Savoir qui génère la donnée ou effectue une action sur celle-ci et quand,*
  - ✓ ***Complètes :** Toutes les données sont présentes et disponibles,*
  - ✓ ***Cohérentes :** Tous les éléments de l'enregistrement, tels que la chronologie des événements, se suivent et sont horodatés dans l'ordre attendu,*
  - ✓ ***Durables :** Conservées sur média de stockage approuvés et pérennes,*
  - ✓ ***Disponibles :** Accessibles pour revue, audit, évaluation ou inspection durant la durée de vie de la donnée,*
  - ✓ ***Non corrompues :** Données et enregistrements non altérés ;*
- ***C - Confidentialité :** offrir un niveau satisfaisant d'accès et de préservation des données sensibles. La confidentialité est assurée lorsqu'une information ou une donnée n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés ;*
- ***P - Preuve** : garantir la traçabilité suffisante pour tout contrôle et administration de la preuve. La preuve englobe la traçabilité des actions menées, l'authentification des utilisateurs, l'imputabilité du responsable de l'action effectuée.*

Chacun de ces quatre critères représente les fondamentaux de la sécurité du système d'information d'un organisme et correspond à des exigences d'accréditation à satisfaire (voir § 8 du présent guide).

En pratique

Pour évaluer la sécurité de son système d'information, l'organisme peut suivre les étapes suivantes :

- **Etape 1** – identifier les failles du système d'information, par exemple en s'appuyant sur la cartographie ;
- **Etape 2** – recenser les informations traitées par l'organisme, via son système d'information. Identifier, parmi les informations recensées, celles qui doivent être sécurisées, par exemple, *via* une analyse de risques (voir § 7.3.1 item « Apprécier et gérer les risques inhérents au système d'information ») ;
- **Etape 3** – analyser, selon les critères DICP, chaque information qui doit être sécurisée ;
- **Etape 4** – si nécessaire, mettre en place les actions de sécurisation des informations.

En savoir plus

- NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences

- NF EN ISO/CEI 27002 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les mesures de sécurité de l'information

7 PARTIE II : GESTION DU SYSTEME D'INFORMATION

Rappel : Comme indiqué dans le § 1. Objet, les éléments indiqués dans ce guide sont donnés à titre informatif et n'ont pas valeur d'exigence opposable.

Cette 2ème partie traite de la gestion du système d'information au travers des thématiques suivantes :

- Les responsabilités au sein de l'organisme (§7.1),
- La gestion des ressources, en particulier quand elles sont externalisées (§ 7.2),
- Le pilotage du système d'information en prenant l'exemple d'une approche PDCA (§ 7.3),
- La gestion de projet dans le cadre de changements au sein du système d'information (§ 7.4).

7.1 Gouvernance, rôles et responsabilités au sein de l'organisme

Seule une gouvernance avisée est à même de relever le défi du bon fonctionnement et de la sécurité du système d'information. La gouvernance est un élément essentiel de la gestion du système d'information.

Les pistes de réflexion ci-dessous ont pour objet de définir les acteurs de la gouvernance ainsi que les rôles et responsabilités au sein de l'organisme.

Pistes de réflexion

- ***Les acteurs de la gouvernance*** *(Direction) sont fonction de la structure de l'organisme, de sa taille, de son domaine d'activité. Toutefois, quel que soit son positionnement et sa nature, la Direction de l'organisme définit une stratégie informatique via un schéma directeur (plan stratégique pluriannuel permettant de prévoir et d'anticiper l'évolution du système d'information), via une politique du système d'information, des objectifs, des indicateurs de suivi, des exigences et instructions à respecter.*

  La direction alloue les ressources (financières, humaines, matérielles) et définit les responsabilités et autorités en charge de la gestion du système d'information. Ainsi, elle choisit d'externaliser ou non, tout ou partie de son système d'information et de sa gestion.

  Elle est tenue informée des résultats de cette stratégie via les rapports de l'encadrement, les résultats des objectifs, les conclusions des évaluations (audit interne, évaluation Cofrac, inspection réglementaire…), les incidents, les réclamations… La revue de direction est un moment propice pour définir, revoir, adapter la stratégie de l'organisme.

  Note : la politique du système d'information peut prendre différentes formes. Ainsi, un organisme peut choisir de mettre en place une politique (au sens de la NF EN ISO 9000), mais aussi une Charte (par exemple une charte d'utilisation du système d'information), un règlement…

- ***Les fonctions informatiques*** *dépendent, là aussi, de la structure et de la taille de l'organisme : Direction du système d'information (DSI), Responsable de l'Infrastructure, Responsable des solutions logicielles, Responsable Informatique, Correspondant Informatique….*

  Leur mission est de mettre en œuvre les axes stratégiques définis par la gouvernance.

  Les fonctions informatiques se donnent les moyens de mesurer l'efficacité du système d'information via des audits, des indicateurs, des tableaux de bord.

  Elles assurent une veille technologique et réglementaire pour anticiper les éventuelles évolutions du système d'information.

  Elles s'assurent, par un suivi régulier, que les prestataires informatiques fournissent un niveau de service conforme aux besoins de l'organisme et au cadre contractuel.

- ***Les utilisateurs*** *du système d'information respectent les politiques définies (par exemple une politique de Sécurité), les procédures et instructions.*

En savoir plus

- NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences
- Charte d'utilisation des moyens informatiques et des outils numériques - guide d'élaboration en 8 points clés pour les PME et ETI (Version 1.0 de juin 2017) – ANSSI

7.2 Ressources et infogérance

La gestion du système d'information fait appel à des ressources diverses : ressources humaines, locaux, logiciels, infrastructures physiques ou encore équipements bureautiques. En fonction de la stratégie adoptée par l'organisme, ces ressources pourront être internes ou externes.

En effet, la gestion du système d'information fait appel à des compétences que l'organisme ne possède pas systématiquement. C'est pourquoi le recours à des prestataires informatiques est chose courante. On parle alors d'infogérance. Parmi ces prestataires, peuvent être cités (liste non exhaustive) :

- **Les éditeurs de logiciel** : l'éditeur conçoit et développe le logiciel ;
- **Les intégrateurs :** l'intégrateur (qui peut être l'éditeur ou une ESN), accompagne les utilisateurs dans le déploiement d'une solution logicielle et la personnalise en fonction des attentes et des besoins du client ;
- **Les fournisseurs d'accès à Internet** et plus globalement les opérateurs Telecom ;
- **Les opérateurs techniques :** ils gèrent les infrastructures (câblage informatique, gestion de la climatisation de la salle du serveur, détection incendie de la salle du serveur, contrôle d'accès…) ;
- **Les fournisseurs de matériel :** serveur, matériel bureautique…
- **Les Entreprises de Service du Numérique (ESN) :** ces sociétés peuvent intervenir ponctuellement au sein de l'organisme (par exemple pour gérer un projet informatique). Elles peuvent aussi gérer tout ou partie du système d'information de l'organisme – on parle alors de Tierce Maintenance Applicative (TMA) ;
- **Les Data Center :** prestataire proposant l'hébergement de données.

Pistes de réflexion

L'organisme peut s'interroger sur les éléments à prendre en considération pour la maîtrise de l'infogérance. Pour la gestion des moyens internes, Il peut s'appuyer sur les exigences définies dans ses référentiels d'accréditation, sur la norme ISO/CEI 27001 ou encore sur tout autre document de référence.

L'infogérance peut être classée en trois grandes catégories :

- ***Gestion d'infrastructures*** *: maintenance du parc informatique, hébergement et/ou administration de serveurs, gestion des stockages et sauvegardes, supervision du réseau et de sa sécurité…*
- ***Gestion des applications logicielles*** *: support fonctionnel, support aux utilisateurs, maintenance préventive ou corrective, gestion des évolutions (projet)…*

- ***Hébergement de service*** *: le prestataire héberge pour le compte de l'organisme une application utilisée comme un service, accessible le plus souvent par le biais d'un navigateur web ou d'une application spécifique.*

Même si elle offre de nombreux avantages, notamment lorsque les compétences internes à l'organisme sont absentes ou insuffisantes, l'infogérance est aussi une source de risques pour le système d'information : perte de maîtrise du système d'information, confidentialité des données, hébergements mutualisés, sécurité du réseau avec les interventions à distance…C'est pourquoi toute décision d'infogérance devrait s'accompagner d'une étude visant à apprécier les risques qui devront être traités dans le cahier des charges soumis aux prestataires. Les prestataires devraient s'engager, au moins sur :

- *La réversibilité du contrat (cf. § 2.2 définitions),*
- *La possibilité de réalisation d'audits par l'organisme,*
- *La validation de certains choix techniques,*
- *La sauvegarde et la restitution des données dans un format exploitable par l'organisme,*
- *Le maintien à un niveau de sécurité dans le temps.*

En savoir plus

- NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences
- Maîtriser les risques de l'Infogérance – Guide de l'externalisation des systèmes d'information de décembre 2010 – ANSSI

7.3 Pilotage du système d'information : exemple d'une approche PDCA

Le pilotage du système d'information peut suivre une méthodologie de type PDCA, en cohérence avec les démarches d'amélioration continue introduites dans les différents référentiels d'accréditation.

La démarche proposée est résumée ci-dessous puis développée point par point dans la suite du guide :

⇨ PLAN : Identifier les actions à mener (§7.3.1)
⇨ DO : Mettre en œuvre les dispositifs de maîtrise (§7.3.2)
⇨ CHECK : Surveiller le système d'information (§7.3.3)
⇨ ACT : Mettre à jour et améliorer le système d'information (§7.3.4)

7.3.1 PLAN : Identifier les actions à mener

Dans la démarche présentée ici, l'étape de « planification » de la gestion du système d'information consiste à identifier les actions à mener en fonction des enjeux internes et externes de l'organisme. Ainsi, les sources possibles d'identification des actions à mener sont :

- Les besoins de l'organisme et de ses clients,
- Les exigences normatives et règlementaires,
- La gestion des risques inhérents au système d'information.

Les éléments qui suivent présentent des pistes de réflexion pour identifier les actions à mener pour chacun de ces 3 items. Cette approche n'est pas exhaustive. En effet, d'autres sources d'information

peuvent permettre à l'organisme d'identifier les actions à mener (des résultats d'audits de sécurité du système d'information par exemple).

Cette étape de planification est généralement l'occasion de définir les indicateurs de suivi associés aux actions déterminées, si approprié (voir § 7.3.3 Check : surveiller le système d'information).

7.3.1.1 Identifier les besoins de l'organisme et de ses clients

L'identification des besoins de l'organisme et de ses clients peut revenir à s'interroger plus largement sur :

- Qu'est ce qui définit l'efficacité d'un système d'information ?
- Quels sont les critères de qualité du système d'information ?

Cette démarche peut être mise en œuvre lors de changements majeurs (changements structurels ou organisationnels, développement ou déploiement d'un nouveau logiciel, etc.). Elle peut également être utilisée par l'organisme pour se questionner sur l'adéquation du système d'information déjà en place ou sur sa gestion.

Pistes de réflexion

Un système d'information peut être qualifié d'efficace lorsqu'il répond aux besoins des utilisateurs, des clients et parties prenantes et respecte la stratégie définie par la Direction (schéma directeur). Ainsi, pour définir cette stratégie, concevoir ou faire évoluer son système d'information, l'organisme est amené à identifier les besoins des utilisateurs en termes de fonctionnalités, d'ergonomie, de performance (temps de réponse, nombre d'utilisateurs, nombre de licences…).

Les besoins des clients doivent être pris en compte, notamment lorsque le système d'information permet la diffusion des résultats de la prestation accréditée (par exemple : rapport d'essai ou d'analyse, certificat d'étalonnage, rapport d'inspection, certificats…) ou la prise en compte d'une demande (demande de prestation, réclamation…).

Le système d'information tient nécessairement compte des exigences des parties prenantes, principalement dans un contexte réglementaire (les parties prenantes peuvent être des administrations, des certificateurs, le Cofrac…).

En savoir plus

NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences

7.3.1.2 Identifier les exigences normatives et règlementaires

Un système d'information efficace répond aux besoins des utilisateurs et des clients. Il doit aussi permettre à l'organisme de respecter les normes, qu'elles soient de management ou techniques, mais aussi lui permettre de respecter la réglementation en vigueur.

Pistes de réflexion

L'organisme doit connaître la réglementation qui s'applique à lui, réglementation qui dépend directement de son statut (public ou privé) et de son domaine d'activité. Ainsi, plus les informations gérées par l'organisme sont sensibles, plus les règles de protection des systèmes d'information sont contraignantes. Pour cela, il convient qu'une veille réglementaire intégrant les activités du système d'information soit mise en place.

Certaines réglementations s'appliquent à tout organisme. C'est par exemple le cas de la loi « Informatique et Libertés » n° 78-17 du 6 janvier 1978 et de son décret d'application n° 2019-536 du 29 mai 2019. C'est aussi le cas du règlement général sur la protection des données (RGPD), entré en application le 25 mai 2018.

Remarque : La vérification du respect des textes règlementaires nationaux et internationaux relatifs à la gestion des données personnelles (exigences de la CNIL ou du RGPD par exemple) ne relève pas des attributions des évaluateurs du Cofrac.

En savoir plus

- Le site Legifrance, le Service Public de la diffusion du droit : https://www.legifrance.gouv.fr/
- Le site Internet de la CNIL, Commission Nationale de l'Informatique et des Libertés : https://www.cnil.fr/professionnel
- Le site Internet de l'ANSSI : https://www.ssi.gouv.fr/
- Le site de l'AFNOR https://www.afnor.org/

7.3.1.3 *Apprécier et gérer les risques inhérents au système d'information*

Pour apprécier et gérer les risques inhérents, il est essentiel pour l'organisme de comprendre et de décrire la façon dont le système d'information (processus informatique) est géré. Ensuite, les risques peuvent être identifiés, analysés et gérés.

Pistes de réflexion

L'identification des risques liés au système d'information peut être appréhendée selon différentes approches. L'organisme peut par exemple avoir une approche « organisationnelle » en étudiant chacun des macro-processus représentatifs du fonctionnement de son système d'information ; ou encore avoir recours à une approche selon les 5 M.

- *Approche « organisationnelle » (macro-processus)*

Le fonctionnement du système d'information peut se décomposer en trois étapes (macro-processus) :

I. ***Organiser le système d'information** : ceci englobe les notions de gouvernance, de pilotage, de définition des responsabilités et d'allocation des ressources…*
II. ***Faire fonctionner le système d'information au quotidien** : utiliser et exploiter le système d'information, le faire évoluer (nouvelles fonctionnalités, nouveau service, changement de matériel), gérer les corrections.*
III. ***Sécuriser le système d'information** : protéger physiquement les installations, protéger le système d'information, détecter et réagir contre les attaques…*

Le risque inhérent au système d'information correspond au risque de perte résultant d'une inadéquation ou d'une défaillance d'un ou de plusieurs de ces trois macro-processus. La perte peut être de différentes natures : perte d'accès au système d'information, perte de données, perte financière, perte de temps, perte de confidentialité, perte d'intégrité des données…

- *Approche selon la méthode des 5M*

Outre la méthode présentée précédemment, l'analyse des risques inhérents au système d'information peut être conduite selon la méthode des 5M (ou diagramme des causes et effets ou diagramme d'ishikawa).

En pratique

A titre d'exemples, des listes non exhaustives des risques inhérents aux systèmes d'information sont données en annexe :

- Annexe 1 : Analyse de risque par l'approche organisationnelle
- Annexe 2 : Analyse de risque par une approche 5M

Les éléments proposés peuvent constituer une base de réflexion pour l'organisme qui souhaiterait conduire une analyse de risques. L'étape d'identification des risques étant ensuite suivie de leur analyse afin d'identifier les failles à maîtriser et donc les actions à mener en priorité.

En savoir plus

- NF ISO 31000 : Management du risque – lignes directrices
- NF EN ISO/CEI 27002 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les mesures de sécurité de l'information
- Le risque informatique – document de réflexion de janvier 2019 – Autorité de Contrôle Prudentiel et de Résolution ACPR – Banque de France.

7.3.2 DO : Sélectionner et mettre en œuvre les dispositifs de maîtrise

Suite à l'identification des actions issues de l'analyse des besoins, des exigences et des risques liés au système d'information, l'organisme priorise et mène les actions nécessaires pour assurer la maîtrise de son système d'information.

Pistes de réflexion

Cette priorisation est à réaliser en fonction des enjeux internes et externes à l'organisme. Les choix peuvent être faits en fonction des politiques et des objectifs de l'organisme, en fonction des risques majeurs identifiés, en fonction d'exigences légales à respecter, etc.

Les informations recueillies lors de la phase précédente peuvent constituer des éléments d'entrée d'une analyse de risque visant à prioriser les actions à mener.

En savoir plus

- NF ISO 31000 : Management du risque – lignes directrices
- NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences

7.3.3 CHECK : Surveiller le système d'information

L'étape de surveillance du système d'information revient à en mesurer l'efficacité *via* trois concepts : superviser, auditer, réagir. Les objectifs de cette surveillance peuvent être multiples : suivre la conduite d'un projet, évaluer l'efficacité d'actions mises en place, vérifier l'atteinte d'objectifs spécifiques, détecter des menaces, dysfonctionnements, etc.

Pistes de réflexion

Pour assurer la surveillance, l'organisme peut tout d'abord utiliser les outils prescrits dans les normes d'accréditation :

- *Réalisation d'audits intégrant la gestion du système d'information,*

- *Suivi d'indicateurs et de tableaux de bord,*
- *Enregistrement et traitement (via des actions correctives) de tous les incidents liés au système d'information (connexion impossible, multiples alertes de l'antivirus, fichiers créés, modifiés ou supprimés sans autorisation…),*
- *Veille technologique et réglementaire pour anticiper les éventuelles évolutions du système d'information et ainsi accompagner une nouvelle stratégie,*
- *Suivi régulier des prestataires informatiques, afin de s'assurer qu'ils fournissent un niveau de service conforme aux besoins de l'organisme.*

Parallèlement, l'organisme met en place des actions de contrôle spécifiques :

- *Supervision du système d'information via les journaux des applications (permet de détecter d'éventuels dysfonctionnements, tentatives d'accès illicites aux composants du système d'information),*
- *Contrôle systématique de la bonne réalisation des sauvegardes,*
- *Organisation de tests périodiques liés à la continuité d'activité (simulation d'un incident avec mise en place du PCA ou du PRA), de tests liés à l'intégrité des données (reprise de données archivées pour s'assurer qu'elles sont toujours lisibles et exploitables – restauration des données). Ces tests périodiques permettent d'évaluer la résilience du système d'information.*

En savoir plus

- NF EN ISO/CEI 27001 : Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences
- Guide d'Hygiène Informatique – renforcer la sécurité de son système d'information en 42 mesures (version 2.0 de septembre 2017) – ANSSI

7.3.4 ACT : Mettre à jour et améliorer le système d'information

En cohérence avec la démarche d'amélioration continue, les résultats de la surveillance du système d'information conduisent l'organisme à identifier et mettre en place de nouvelles actions et, si approprié, de nouveaux objectifs (actions correctives, actions préventives, actions d'amélioration, mise en place de nouveaux projets, etc.).

Ces décisions peuvent être prises à diverses occasions ; par exemple suite aux audits internes et évaluations Cofrac, au traitement des dysfonctionnements (actions correctives), actions préventives, actions d'amélioration, à la revue de politiques internes, à l'évolution d'un projet, à la revue des risques et opportunités.

Dans le cadre de la gestion du système d'information, cette démarche d'amélioration continue est nécessairement couplée au Maintien en Condition Opérationnelle (MCO) dont l'objectif principal est d'assurer la pérennité du système.

Pistes de réflexion

Le Maintien en Condition Opérationnelle (MCO) du système d'information est une condition sine qua non au respect des engagements pris auprès des utilisateurs, des clients et des parties prenantes (par exemple le Cofrac). Les objectifs de la phase de MCO sont de :

- *Maintenir efficacement l'usage du système d'information pour qu'il fournisse le service attendu par les utilisateurs tel que déterminé en phase projet (cahier des charges, expression des besoins fonctionnels…) ;*

- *Préparer et faire évoluer le système d'information pour préparer l'avenir, tout en maîtrisant les coûts, les délais et la qualité d'exécution du résultat.*

Les grandes activités du Maintien en Condition Opérationnelle sont :

- *La formation en continue des utilisateurs,*
- *La gestion des accès au système d'information,*
- *La gestion des changements,*
- *La maintenance corrective et évolutive incluant la Gestion de Configuration Logicielle* (GCL),*
- *La gestion du paramétrage lié au cœur du système (données statiques),*
- *L'exploitation quotidienne des traitements,*
- *Le support fourni aux utilisateurs.*

** La Gestion de Configuration Logicielle (GCL) englobe quatre principes :*

- *Identification de la configuration (d'un système d'information ou d'un logiciel),*
- *Maîtrise de la configuration : maîtrise des évolutions d'un système d'information ou d'un logiciel en identifiant clairement chaque nouvelle version. C'est généralement réalisé via l'indice de version, la date de mise en production, les paramètres de la version, les évolutions apportées…*
- *Enregistrement de l'état de la configuration (via des formulaires, fiches de vie, dossier de version…),*
- *Audit de la configuration (la traçabilité des configurations successives est assurée).*

Pour résumer, ce sont les actions menées par l'organisme pour maîtriser ses versions du système d'information, leurs évolutions et en assurer la traçabilité via une piste d'audit.

En savoir plus

- NF EN ISO/CEI 27002 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les mesures de sécurité de l'information
- Norme ISO 10007 : Systèmes de management de la qualité – Lignes directrices pour la gestion de la configuration.

7.4 Gestion de projet

Pour un organisme souhaitant mettre en place un système d'information dématérialisé ou lors d'une évolution importante de son système d'information, il peut être nécessaire de mettre en place une gestion de projet. Cette gestion de projet doit lui permettre de gérer au mieux la mise en production d'un nouvel outil (SIL, GED, Centrale d'acquisition des températures), ou la mise en production d'une nouvelle version majeure d'un logiciel.

En pratique

Un développement présentant les étapes d'une conduite de projet et la traçabilité associée est disponible en Annexe 3.

En savoir plus

- GAMP 5 - Une approche de la conformité des systèmes informatisés BPx basée sur les risques.
- OECD Series on principles of good laboratory practice and compliance monitoring – number 17 – Application of GLP Principles of Computerised Systems.

8 PARTIE III : SYSTEME D'INFORMATION ET ACCREDITATION

Cette 3ème partie aborde sept thématiques qui sont communes aux différents référentiels d'accréditation. L'objectif est, pour chaque thématique :

- ⇨ de mettre en lumière les objectifs et bienfondés des exigences,
- ⇨ de présenter quelques exemples de moyens permettant de répondre aux exigences,
- ⇨ d'indiquer des points pouvant être abordés en évaluation pour apprécier le niveau de maîtrise des exigences correspondantes.

Les éléments présentés dans cette partie III sont à exploiter en prenant en considération les remarques suivantes :

- S'agissant d'un guide transversal pour l'ensemble des activités accréditées par le Cofrac, cette partie III se limite aux items qui sont communs aux différents référentiels d'accréditation. Ainsi, pour un référentiel donné, l'ensemble des exigences relatives à la gestion du système d'information et à la maîtrise des données ne sont pas reprises dans cette partie III. Il appartient aux organismes de s'assurer qu'ils respectent l'ensemble des exigences de leurs référentiels d'accréditation et de la réglementation en vigueur ;
- Les exigences relatives aux données (§ 8.1 à 8.4) concernent, si approprié, les données générées, utilisées et/ou transmises dans le cadre de la réalisation des prestations accréditées. Ces exigences ne concernent donc pas l'ensemble des données de l'organisme. Il en va de même pour ce qui concerne la validation du système d'information (§ 8.5) : elle concerne les éléments du système d'information qui peuvent avoir un impact sur la mise en œuvre et/ou le résultat des prestations accréditées. L'organisme est cependant libre d'appliquer les mêmes dispositions pour l'ensemble de son système d'information ;
- Les exemples de moyens présentés ne sont pas exhaustifs. Ils constituent des illustrations de stratégies et actions pouvant être mis en œuvre et ils n'ont pas de caractère prescriptif ;
- Concernant les points pouvant être abordés en évaluation : il ne s'agit pas d'une approche exhaustive et l'évaluation de l'ensemble des points cités n'est pas forcément nécessaire pour considérer que l'organisme satisfait aux exigences d'accréditation. Les points cités ont vocation à indiquer quels aspects peuvent être abordés en évaluation pour apprécier le niveau de satisfaction de l'exigence considérée. En fonction du contexte de chaque organisme, certaines questions peuvent ne pas s'appliquer ou ne pas être pertinentes. Par ailleurs, les éléments présentés peuvent également constituer une base de réflexion pour identifier les points clefs à maîtriser par les organismes ou encore développer des outils d'auto-évaluation.

Dans tous les cas, il est admis que les moyens mis en œuvre par les organismes pour assurer la maîtrise des exigences d'accréditation en lien avec les items qui suivent peuvent être très divers et que ceux-ci doivent rester proportionnés aux risques identifiés.

En pratique

L'annexe 4 récapitule les paragraphes introduisant les exigences relatives à chaque item pour chacun des référentiels d'accréditation.

8.1 Confidentialité des données

Voir aussi le § 6.3 du présent guide.

La confidentialité des informations gérées par les organismes accrédités est une exigence forte dans tous les référentiels d'accréditation. Dans le cadre de la gestion d'un système d'information

dématérialisé, les risques de rupture de confidentialité peuvent survenir à diverses occasions, par négligence, par malveillance ou lors de l'utilisation d'un logiciel inadapté. Il est donc primordial pour les organismes d'identifier précisément les sources de risque possibles afin de mettre en place les moyens appropriés pour assurer la confidentialité des données qu'il détient.

⇨ *Objectifs de l'exigence*

- Assurer que seules les personnes autorisées ont accès aux informations/données qui leur sont destinées.

Par « personnes » il faut entendre toute personne ou entité interagissant avec l'organisme, que ce soit en interne (personnel de l'organisme) ou en externe (destinataires des résultats des prestations, prestataires externes intervenant au sein de l'organisme et ayant accès au système d'information, etc.)

- Empêcher tout accès frauduleux dans le but de voler, corrompre ou crypter des données.

⇨ *Quelques exemples de moyens pouvant être mis en place*

- Définition, par la direction de l'organisme, d'une stratégie de sécurité de l'information (Politique, Charte, Règlement…). Sensibilisation du personnel intervenant au sein de l'organisme (interne, prestataire,…).
- Mise en place de systèmes de protection du réseau informatique (firewall, logiciel antivirus, anti malware, anti phishing…) - supervision du système d'information via les journaux des applications (permet de détecter d'éventuels dysfonctionnements, tentatives d'accès illicites aux composants du système d'information).
- Mise en place d'une politique de gestion des mots de passe pour l'accès au système informatisé (niveau de complexité, fréquence de changement, modalités de déconnexion automatique à partir d'un certain temps, …).
- Pour le personnel de l'organisme :
  - Définition des droits d'accès en fonction des tâches qui lui sont confiées,
  - Engagement au respect de la confidentialité et de la stratégie de sécurité informatique de l'organisme,
  - Sécurisation des accès distants (VPN…).
- Pour les prestataires de l'organisme (notamment dans le cas d'accès distant aux équipements pour maintenance, dépannage ou réparation) :
  - Définition des droits d'accès en fonction des tâches qui leurs sont confiées,
  - Engagement au respect de la confidentialité,
  - Cryptage / anonymisation des données accessibles par les fournisseurs,
  - Sécurisation des accès distants (VPN…),
  - Mise en place d'un système de traçabilité permettant de formaliser les opérations réalisées par le prestataire.
- Pour les clients de l'organisme :
  - Définition des droits d'accès à leurs informations clients, à leurs résultats,…
  - Sécurisation des accès (site internet, serveur de résultats…),
  - Mise en place de clauses de confidentialité dans les contrats, les conditions générales de ventes, dans les conventions de preuves…

⇨ *Points pouvant être abordés au cours des évaluations*

- Une stratégie de la direction de l'organisme vis-à-vis de la confidentialité du système d'information est-elle formulée (Politique, Charte, Règlement…) ?

- Le personnel de l'organisme est-il sensibilisé à la notion de confidentialité ? Des engagements de confidentialité sont-ils signés ?
- L'accès au système d'information de l'organisme se fait-il au moyen d'une authentification sécurisée ? (Gestion de l'accès au poste informatique, système d'identifiant + mot de passe ou information connue seulement de l'utilisateur concerné).
- Les droits d'accès sont-ils en phase avec les autorisations du personnel (au sein des logiciels, dans les dossiers disponibles en réseau, etc.) ?
- Quelles sont les mesures prises pour préserver la confidentialité dans le cadre de l'intervention de prestataires externes sur le système d'information de l'organisme ? (incluant la gestion des accès à distance le cas échéant)
- Quelles sont les mesures prises pour assurer la confidentialité des informations/données lors de leur transmission au client, aux autorités ?
- Quelles sont les mesures prises pour assurer la confidentialité des sauvegardes et des archives ? (en particulier en cas d'externalisation)

8.2 Intégrité des données

Voir aussi le § 6.3 du présent guide.

⇨ *Objectifs de l'exigence*

- Assurer que les données sont intègres, c'est-à-dire : exactes, lisibles, contemporaines, originales, attribuables, complètes, cohérentes, durables, disponibles, non-corrompues.
- Assurer que si des données ont été modifiées, elles l'ont été par une action volontaire et légitime.

Remarque : L'exigence d'intégrité des données suggère que l'organisme conserve la trace et la justification de toutes les modifications apportées aux données.

⇨ *Quelques exemples de moyens pouvant être mis en place*

- Formation/sensibilisation des utilisateurs concernant la sécurité/l'intégrité des données (incluant la réalisation de modifications de données).
- Définition des droits informatiques en lien avec le niveau de responsabilité/qualification du personnel.
- Mise en place d'historiques dans les logiciels pour le suivi des modifications (activation de filière d'audit).
- Mise en place de protections contre les logiciels malveillants (antivirus…).
- Mise en place de systèmes de chiffrement des données (par exemple pour les données transmises à l'extérieur de l'organisme).
- Réalisation des tests d'intégrité des données : comparaison des données archivées (sous différents médias) avec les données stockées dans le système d'information.
- Réalisation de tests de récupération de données en s'assurant que les données récupérées des archives sont exploitables.

⇨ *Points pouvant être abordés au cours des évaluations*

- Les responsabilités liées à la gestion de l'intégrité des données sont-elles définies au sein de l'organisme ?

- Les droits informatiques sont-ils en phase avec le niveau de responsabilité/qualification du personnel (profils au sein du réseau, des logiciels, etc.) ? c'est-à-dire les droits de modification et suppression des données sont-ils affectés uniquement aux personnes autorisées ?
- La traçabilité des modifications / suppressions de données est-elle assurée ?
- L'organisme utilise-t-il des techniques de chiffrement des données lorsque nécessaire (en particulier pour les données transmises et stockées) ?
- Les outils utilisés pour garantir l'intégrité des données (horodatage, chiffrement, signature électronique…) bénéficient-ils d'une qualification par l'ANSSI ?
- L'organisme vérifie-t-il l'intégrité des données collectées, traitées, enregistrées, transmises et stockées ? c'est-à-dire est-il en mesure de détecter toute dérive dans le temps alors qu'a priori aucune modification n'a été apportée au système (par exemple en audit interne ou encore lors de tests d'intégrité des données sauvegardées ou archivées).
- Si oui, fait-il une vérification initiale puis des vérifications périodiques ?
- Les outils de protection (antivirus, firewall…) sont-ils installés, tenus à jour ? Les droits de gestion de ces outils de protection sont-ils attribués aux fonctions pertinentes ? (un utilisateur Lambda ne doit pas pouvoir désactiver ou modifier les paramétrages de ces outils)

8.3 Disponibilité des données (continuité d'activité et sauvegardes)

Voir aussi les § 6.2, 6.3 et 7.3.3 du présent guide.

⇨ *Objectifs de l'exigence*

- Assurer la sauvegarde du système d'information de l'organisme, c'est-à-dire assurer que l'organisme est en mesure de restaurer et redémarrer le système d'information en cas de « sinistre ».
- Assurer la continuité des activités qui le nécessitent en cas de « sinistre » touchant le système d'information.
- Eviter toute perte ou dégradation/altération de données en cas de problème sur le système d'information.

Remarque : la sauvegarde correspond à un dispositif de protection des informations contenues dans un système informatique, par copie de ces informations sur un support physique ou virtuel (disque, bande magnétique, serveur en cloud, etc.).

⇨ *Quelques exemples de moyens pouvant être mis en place*

- Mise en place d'une stratégie de sauvegarde (données à sauvegarder, fréquence des sauvegardes, sauvegarde complète ou incrémentielle ou différentielle, choix des supports de sauvegarde à utiliser, le cas échéant modalités de stockage des supports de sauvegardes physiques).
- Suivi du planning de sauvegarde – contrôle de la bonne réalisation des sauvegardes.
- Mise en place de moyens pour éviter que les données sauvegardées soient inexploitables (tests de restaurations de sauvegardes, réalisations de plusieurs sauvegardes sur des supports différents, virtualisation des données sur plusieurs machines physiques…).
- Mise en place de conduites à tenir en cas de panne de certains éléments du système d'information, par exemple en fonction d'une analyse bénéfice/risque (en cas de panne du serveur, des connexions réseau, du SIL dans un laboratoire, etc.).
- Détermination de Plans de Reprise d'Activité (PRA) et / ou de Plans de Continuité d'Activité (PCA).

⇨ *Points pouvant être abordés au cours des évaluations*

- L'organisme a-t-il défini une stratégie pour assurer la disponibilité des données ?
- L'organisme a-t-il défini les modalités de sauvegarde : Que sauvegarder ? A quelle fréquence, pour quelle durée ? Qui réalise les sauvegardes ? Comment et où ? (Support physique ou virtuel / internalisée ou externalisée)
- L'organisme met-il en œuvre des tests réguliers de ses sauvegardes, si pertinent ? Met-il également en œuvre des tests aléatoires ?
- Les conduites à tenir en cas de panne relative au système d'information sont-elles définies et accessibles pour le personnel ?
- Si approprié, l'organisme a-t-il défini un plan de continuité d'activité (PCA) ou un plan de reprise d'activité (PRA) en cas de sinistre impactant son système d'information ?
- Les responsabilités liées à la continuité d'activité (PCA) ou à la reprise d'activité (PRA) sont-elles définies au sein de l'organisme ?
- Si oui, ces PCA ou PRA sont-ils périodiquement revus et, si approprié, testés ?

8.4 Archivage électronique

Voir aussi le § 6.3 du présent guide.

⇨ *Objectifs de l'exigence*

- Assurer que les données numériques sont conservées durant les durées définies, que leur intégrité est alors préservée et qu'elles restent accessibles aux utilisateurs autorisés.
- Assurer la traçabilité des données générées tout au long de la réalisation des prestations pendant une durée préétablie.

Remarque : L'archivage correspond au stockage à long terme de données et informations qui ne sont plus utilisées dans l'activité courante de l'organisme mais qui doivent néanmoins être conservées. On parle parfois de « données mortes ».

⇨ *Quelques exemples de moyens pouvant être mis en place*

- Définition des supports d'archivage en fonction de leur pérennité dans le temps (disque dur, serveur de stockage réseau NAS, serveur de stockage externalisé, serveur de stockage virtuel, etc.).
- Définition et sécurisation (protection contre les risques d'incendie, inondation, rongeurs, etc.) des conditions d'entreposage/de conservation de ces supports.
- Mise en place de modalités pour s'assurer que les données archivées vont rester lisibles même après l'arrêt d'un logiciel (archivage des fichiers dans un format lisible par la plupart des logiciels, ou encore conservation sur un poste d'un accès aux anciens logiciels afin de permettre la lecture des fichiers qui sont dans des formats non lisibles par la plupart des logiciels, etc.).
- Définition des durées d'archivage des données en s'appuyant sur les besoins des clients, la réglementation en vigueur dans le domaine et les exigences d'accréditation le cas échéant.
- Définitions des droits d'accès aux données archivées électroniquement (notamment pour assurer le respect de la confidentialité).
- Vérification de l'intégrité des archives.

⇨ *Points pouvant être abordés au cours des évaluations*

- L'organisme a-t-il défini les modalités d'archivage électronique : Quelles données sont archivées ? A quelle fréquence, pour quelle durée ? Qui réalise l'archivage ? Comment et où ? (Support physique ou virtuel / internalisée ou externalisée)
- Les durées d'archivage définies sont-elles en phase avec les exigences légales applicables à l'organisme ?
- En pratique, les données archivées demeurent-elles accessibles, lisibles et intègres ?
- L'accès aux données archivées est-il limité aux seuls utilisateurs autorisés ?
- L'organisme vérifie-t-il son niveau de maîtrise des archives ? (Par exemple en audit interne ou *via* des tests planifiés)

8.5 Validation du système d'information

Voir aussi le § 7.4 et l'annexe 3 du présent guide.

La nécessité de validation du système d'information (terme pris au sens large incluant les outils du système d'information tels que les logiciels commerciaux ou développés en interne, les fichiers de calcul créés par l'organisme) est introduite par de nombreux référentiels d'accréditation (voir annexe 4 du présent guide).

⇨ *Objectifs de l'exigence*

La validation consiste, pour les organismes, à vérifier que leur système d'information (ou outils du système d'information) répond aux exigences spécifiées en termes de fonctionnalité et de performance. Les avantages d'une validation sont nombreux :

- Satisfaire les clients et utilisateurs en vérifiant que leurs besoins sont pris en compte ;
- Satisfaire le législateur en vérifiant que les exigences réglementaires sont prises en compte ;
- Limiter les risques d'arrêt d'une activité à cause d'une défaillance du système d'information ou d'un de ses éléments ; limiter la nécessité de mettre en place des procédures alternatives ;
- Limiter le risque de perte ou d'altération de données.

⇨ *Quelques exemples de moyens pouvant être mis en place*

- La validation peut consister à vérifier les éléments suivants (si pertinent) :
  - La qualité des données primaires (données observées, données en sortie d'équipement analytique, etc.) ;
  - La qualité des données secondaires (vérification des calculs, des règles d'arrondi, etc.) ;
  - La qualité des métadonnées (vérification des unités, de l'horodatage, etc.) ;
  - L'intégrité des données (protection effective des accès en fonction des droits attribués aux utilisateurs, traçabilité des modifications…) ;
  - La confidentialité des données (envoi d'informations vers les bons destinataires…).
- La vérification que les exigences spécifiées sont effectivement atteintes lors de la mise en place et/ou de la mise à jour d'un logiciel peut être réalisée par la :
  - Réalisation de dossiers tests avec des résultats attendus (vérification des fonctionnalités) ;
  - Réalisation de tests de connexions (comparaison des données brutes avec toutes les données dans les différents logiciels) ;
  - Validation des calculs par comparaison à des résultats attendus ou des résultats calculés par un autre moyen ;
  - Vérification des droits d'accès par profil.

- La vérification que les exigences spécifiées sont effectivement maintenues tout au long de l'utilisation du logiciel peut être réalisée par la planification d'opérations ponctuelles, par exemple telles que :
  - Réalisation de dossiers tests avec des résultats attendus ;
  - Réalisation de tests de connexions (par comparaison des données brutes avec les données correspondantes dans les différents logiciels) ;
  - Vérification des calculs par échantillonnage ;
  - Vérification des droits d'accès par profil, par échantillonnage ;
  - Tests de restauration de données (stockées ou archivées).

Remarque : Il n'est pas nécessaire de valider les fonctionnalités pour lesquelles un logiciel est commercialisé. En revanche, l'usage qui est fait de ce logiciel, dans l'environnement de l'utilisateur doit être validé. A titre d'exemple, l'objectif de la validation d'un outil de calcul utilisant le logiciel Excel® n'est pas de vérifier que le logiciel Excel® réalise correctement un calcul (par exemple, il est admis que le logiciel Excel® exécute correctement le calcul d'une somme ou d'un écart-type quand la formule correspondante est utilisée). En revanche, il s'agit pour l'organisme de valider l'usage qu'il fait du logiciel en vérifiant que l'outil de calcul qu'il a créé atteint les objectifs prévus. Cela peut passer par la vérification que les formules de calcul définies par l'organisme sont correctes (la bonne formule de calcul est-elle utilisée ? les bonnes cellules sont-elles sélectionnées ?) ou encore par l'utilisation de jeux de données tests dont les résultats sont connus. La protection des cellules contenant les formules de calcul paramétrées est également à vérifier afin d'éviter les risques de modification inopinée de l'outil de calcul lors de son utilisation.

⇨ *Points pouvant être abordés au cours des évaluations*

- L'organisme a-t-il défini une organisation, des responsabilités liées à la validation du système d'information ?
- Si oui, le personnel en charge de la validation du système d'information est-il compétent ?
- Les méthodes de validation sont-elles définies ? Si nécessaire, une planification du projet de validation est-elle établie et tenue à jour ?
- L'organisme a-t-il défini les éléments de son système d'information à valider ? C'est-à-dire a-t-il :
  - Identifié les briques logicielles (composants logiciels) à valider ?
  - Identifié les fonctions/fonctionnalités du système d'information à valider (en fonction d'une analyse de risque par exemple) ?
  - Etabli sa stratégie de tests, décrit les tests à réaliser ?
- Les interfaces du système d'information sont-elles prises en compte dans le cadre de la validation (connexion avec des automates, des Middleware, des serveurs de résultats…) ?
- Les enregistrements des tests réalisés sont-ils conservés ? (Scenarii, résultats, conclusions)
- Les éventuelles corrections apportées au logiciel dans le cadre de la validation sont-elles documentées, tracées ?
- Les dossiers de validation comportent-ils une conclusion relative à l'aptitude du système testé à satisfaire aux exigences définies, c'est-à-dire à mener correctement les fonctions définies ?
- L'organisme met-il en œuvre cette démarche de validation avant mise en service puis en cas de modification d'une brique logicielle ou encore en cas de modification du paramétrage initial ?

8.6 Prestataires externes / services supports

Voir aussi le § 7.2 du présent guide.

⇨ *Objectifs de l'exigence*

- Assurer que les prestataires externes/services supports sollicités pour gérer ou entretenir le système d'information répondent aux besoins identifiés par l'organisme (notamment besoins des utilisateurs, des clients de l'organisme, aux exigences réglementaires).

Des prestataires externes peuvent par exemple être sollicités pour le maintien de l'infrastructure réseau, de la fourniture de matériel informatique ou de solutions logicielles, de la fourniture de solutions d'hébergement, de sauvegardes.

⇨ *Quelques exemples de moyens pouvant être mis en place*

- Définition des besoins de l'organisme et des exigences applicables au prestataire externe (ou service support), par exemple au moyen d'un contrat, d'une convention de fonctionnement, d'un cahier des charges, de procédures rédigées et validées par les 2 parties. Ce « contrat » peut notamment aborder les points suivants :
  - Clauses relatives à la confidentialité et, si approprié, à l'impartialité (notamment définition des données accessibles au prestataire) ;
  - Définitions des tâches confiées au prestataire et expression des besoins de l'organisme. Par exemple :
    - en termes de durée d'archivage et de délai d'accès aux archives pour une prestation d'archivage,
    - en termes de délai de reprise d'activité en cas de panne quand la gestion du système d'information est déléguée à un service support,
    - modifications du système que le prestataire est autorisé à effectuer sans accord préalable,
  - Définition des outils de communication entre l'organisme et le prestataire (en particulier en conduite à tenir en cas de dysfonctionnement) ;
  - Définition des modalités de connexion du prestataire au système d'information et de traçabilité associée ;
  - Traces des tâches réalisées par le prestataire.
- Réalisation d'une évaluation par l'organisme des prestataires sollicités, selon des critères adaptés à la prestation fournie.

⇨ *Points pouvant être abordés au cours des évaluations*

- L'organisme a-t-il identifié l'ensemble des prestataires externes (ou services supports) impliqués dans la gestion ou l'entretien du/des système(s) d'information ?
- L'organisme a-t-il défini les besoins/exigences relatives aux tâches confiées aux prestataires externes/services supports ?
- Comment l'organisme s'assure-t-il que ses besoins (incluant les exigences d'accréditation applicables si pertinent) sont respectés par le prestataire externe (ou service support) ?

8.7 Compte rendu des prestations accréditées

Les « comptes rendus » des prestations accréditées correspondent notamment :

- Aux comptes rendus d'examens médicaux produits par les laboratoires de biologie médicale ou les cabinets d'anatomo-cytopathologie,

- Aux rapports d'inspection produits par les organismes d'inspection,
- Aux rapports d'essai, d'analyse, d'échantillonnage ou d'étalonnage produits par les laboratoires,
- Aux certificats délivrés par les organismes de certification.

Les clients de l'organisme et les autorités souhaitent souvent pouvoir disposer rapidement des résultats de la prestation accréditée, par un moyen qui facilite leur prise en compte. Ainsi, la dématérialisation des résultats s'impose progressivement aux organismes : utilisation de serveurs de résultats, de messageries et signatures électroniques, etc.

Toutefois, l'utilisation de ces nouvelles technologies ne doit pas détourner les organismes de leurs devoirs : fournir des résultats intègres, exploitables par leurs clients, tout en assurant la confidentialité des données et la sécurité de leur système d'information. Pour y parvenir, les moyens mis en œuvre peuvent être très divers d'un organisme à un autre, notamment en fonction de son contexte d'activité et des risques qu'il aura pu identifier en lien avec la phase d'émission et de transmission des comptes rendus de ses prestations accréditées.

⇨ *Objectifs de l'exigence*

- Assurer la transmission des rapports dématérialisés aux destinataires identifiés par les clients, en utilisant des moyens de communication assurant un niveau de confidentialité adéquat.
- Utiliser un format garantissant l'intégrité, la lisibilité et la protection de toutes les informations constituant le rapport sur les résultats (dont l'authentification de l'identité du signataire).

⇨ *Quelques exemples de moyens pouvant être mis en place*

- Authentification de la personne autorisant le compte rendu de la prestation par l'utilisation :
    - d'un système de signature électronique (ou numérique),
    - d'un PGI ou SIL permettant de gérer les droits de chaque utilisation en fonction des niveaux d'autorisation/responsabilité de chacun,
    - d'une carte professionnelle connectée au système d'information (exemple Carte de Professionnel de Santé),
    - tout autre système permettant de garantir que la personne autorisant le compte rendu de la prestation est bien celle revendiquée.

Remarque : Les moyens mis en œuvre pour assurer l'authentification de la personne autorisant les comptes rendus des prestations peuvent être plus ou moins complexes en fonction du contexte d'activité du laboratoire, des risques identifiés, des besoins des clients, etc.

- Protection du contenu du compte rendu en utilisant une format possédant une clef de chiffrement.
- Transmission des comptes rendus par messagerie électronique sécurisée (existe en santé) ou non, *via* un coffre-fort numérique, *via* un serveur de résultats sécurisé, *via* un réseau en utilisant un protocole qui garantit la confidentialité et l'authentification du serveur distant (type : SFTP ou HTTPS), par fax.
- Transmission des comptes rendus *via* l'intégration directe des résultats dans le système d'information du client ou de l'autorité.
- Lorsque les modalités de diffusion ne sont pas réputées sécurisées par une tierce partie (par exemple, l'ANSSI), une convention de preuve peut être signée avec les clients. Cette convention de preuve formalise généralement :
    - le mode de transmission,
    - la liste des adresses mails, des adresses serveurs, des numéros de Fax (etc.),
    - les rôles et responsabilités de chacun vis-à-vis de la confidentialité,

- les modalités de réalisation des dossiers tests pour vérifier l'intégrité des données et la bonne réception par les destinataires identifiés par le client,
- le cas échéant, les modalités de signature électronique des documents.

⇨ *Points pouvant être abordés au cours des évaluations*

- Comment l'authentification des émetteurs des rapports est-elle assurée ?
- Quels sont les moyens utilisés par l'organisme pour diffuser ses résultats ?
- L'organisme a-t-il identifié les risques liés aux moyens de diffusion des résultats (intégrité, lisibilité, confidentialité, sécurité du système d'information…) ?
- Les outils utilisés pour diffuser des résultats sont-ils validés, régulièrement testés si besoin ?
- Les modalités de diffusion des résultats font-ils l'objet d'un accord avec le client (contrat, engagement, conditions générales de vente, convention de preuve…) ?
- Les outils utilisés pour la diffusion dématérialisée des résultats (horodatage, chiffrement, signature électronique…) sont-ils qualifiés par l'ANSSI (si pertinent) ?
- Lorsque les modalités de diffusion ne sont pas réputées sécurisées par une tierce partie (par exemple, l'ANSSI), une convention de preuve est-elle signée avec les clients ?
- L'organisme met-il en place, dans la mesure du possible, des procédures pour limiter (voire interdire) la modification malveillante des résultats par un tiers (client, client du client…) ?

ANNEXE 1 : Analyse de risques par une approche organisationnelle

Comme indiqué au § 7.3.1, le fonctionnement du système d'information peut se décomposer en trois étapes (macro-processus) :

- ✓ Organiser le système d'information
- ✓ Faire fonctionner le système d'information au quotidien
- ✓ Sécuriser le système d'information

Le risque inhérent au système d'information correspond au risque de perte résultant d'une inadéquation ou d'une défaillance d'un ou plusieurs de ces trois macro-processus. La perte peut être de différente nature : perte d'accès au système d'information, perte de données, perte financière, perte de temps, perte de confidentialité, perte d'intégrité des données…

A titre d'exemple, une liste non exhaustive des risques liés à chacun de ces trois macro-processus (causes et effets potentiels) est donnée ci-dessous.

Macro-processus : Organiser le système d'information

Implication insuffisante des instances dirigeantes :

- *Mauvaise perception des enjeux du système d'information,*
- *Décisions inappropriées,*
- *Pilotage insuffisant.*

Stratégie insuffisamment définie, stratégie n'étant pas en adéquation avec la stratégie métier :

- *Manque d'anticipation des besoins métier et des évolutions/enjeux/usage technologiques,*
- *Outils et niveaux de service inadéquats.*

Pilotage budgétaire défaillant :

- *Alignement insuffisant du budget avec la stratégie informatique,*
- *Allocation budgétaire absente ou insuffisamment claire,*
- *Suivi insuffisant des dépenses.*

Rôles et responsabilités de la fonction informatique et de la fonction de sécurité informatique inadéquats :

- *Rôles et responsabilités mal définis, mal répartis ou mal communiqués,*
- *Profils inadaptés ou insuffisants.*

Rationalisation insuffisante du système d'information :

- *Manque de maîtrise de l'architecture du système d'information (urbanisation/cartographie),*
- *Incohérence des normes informatiques suivies,*
- *Défaut de maîtrise de l'obsolescence.*

Maîtrise insuffisante de l'externalisation (prestataires informatiques) :

- *Cadre contractuel inadapté,*
- *Dépendance forte,*
- *Suivi insuffisant du respect des niveaux de service offerts par les prestataires informatiques,*
- *Dispositif de réversibilité insuffisant.*

Non-conformité du système d'information avec les lois, règlements, normes…

Gestion des risques insuffisante :

- *Cartographie des risques inexistante ou partielle,*
- *Défaut dans l'analyse de risque,*
- *Dispositif de contrôle permanent/périodique insuffisant,*
- *Recensement et gestion insuffisants des incidents de risque opérationnel.*

Macro-processus : Faire fonctionner le système d'information au quotidien

Mauvaise gestion de l'exploitation (systèmes et réseaux) :

- *Insuffisance des moyens de production,*
- *Insuffisance dans la détection des erreurs ou anomalies,*
- *Insuffisance dans la gestion des incidents et des problèmes,*
- *Non-respect des niveaux de service.*

Mauvaise gestion de la continuité informatique :

- *Mauvaise organisation de la continuité informatique (PRA, PCA),*
- *Insuffisance dans l'identification des scénarios d'indisponibilité,*
- *Non-alignement de la continuité informatique avec la continuité métier,*
- *Protection insuffisante des moyens de production et de secours contre les accidents,*
- *Tests insuffisants.*

Mauvaise gestion des changements (projets, évolutions, corrections) :

- *Insuffisance dans la définition ou l'application des normes relatives à la gestion des changements,*
- *Mauvaise organisation dans la conduite de projets,*
- *Mauvaise prise en compte des exigences fonctionnelles et techniques,*
- *Défaut dans les logiciels,*
- *Insuffisance des tests.*

Mauvaise qualité des données :

- *Utilisation ou production par le système d'information de données erronées,*
- *Défaut de contrôle de qualité des données.*

Macro-processus : Sécuriser le système d'information

Insuffisance dans la protection physique des installations :

- *Protection insuffisante contre l'intrusion dans les bâtiments,*
- *Protection insuffisante des équipements informatiques.*

Insuffisance dans la protection du système d'information :

- *Défaillance du dispositif de protection contre les logiciels malveillants,*
- *Défaillance du dispositif de gestion des identités et des droits d'accès,*
- *Défaillance du dispositif d'authentification des collaborateurs,*
- *Défaillance du dispositif de protection de l'intégrité des systèmes et des données,*
- *Défaillance du dispositif de protection de la confidentialité des données,*
- *Défaillance du dispositif de protection de la disponibilité,*
- *Défaillance du dispositif de gestion des correctifs de sécurité,*
- *Défaillance du dispositif de revues de sécurité,*
- *Défaillance du dispositif de sécurité des solutions externalisées,*
- *Défaillance du dispositif de sensibilisation à la sécurité des systèmes d'information.*

Insuffisance dans la détection des attaques :

- *Défaillance du dispositif de recueil et d'analyse des traces,*
- *Défaillance du dispositif de surveillance des comportements anormaux des utilisateurs.*

Insuffisance du dispositif de réaction aux attaques :

- *Défaillance du dispositif de gestion de crise,*
- *Défaillance du dispositif de contingentement des attaques,*
- *Défaillance du dispositif de reprise des opérations.*

ANNEXE 2 : Analyse de risques par une approche 5M

Outre la méthode présentée précédemment, l'analyse des risques inhérents au système d'information peut être conduite selon une approche par la méthode des 5M.

L'objectif de cette partie est de lister les risques les plus couramment rencontrés dans le cadre de la gestion des systèmes d'information.

Remarque : Du fait des évolutions très rapides dans ce domaine, les risques présentés ci-dessus ne peuvent pas être considérés comme exhaustifs.

MATIERE

Risque de dégradation ou de pertes des données lors :

- ✓ d'un changement de logiciel,
- ✓ d'un changement de version de logiciel,
- ✓ des modifications des tables d'une base de données,
- ✓ d'un transfert de données entre deux ou plusieurs logiciels,
- ✓ d'un changement d'unité de mesure,
- ✓ d'un changement de mesurande,
- ✓ de la traduction / transfert d'une alarme entre deux logiciels,
- ✓ de la modification de liens entre les tables d'une base de données,
- ✓ du traitement des données :
  - Erreur de calcul,
  - Erreur lors de l'application de règles d'arrondissage,
  - Erreur de règles d'expertise (logiciel qui réalise automatiquement des déclarations de conformité, donne des avis ou des interprétations, sélectionne automatiquement la réalisation de prestations complémentaires…),
  - Erreur de tâche informatique automatisée,
- ✓ de l'archivage des données,
- ✓ de la restauration des données à partir d'une copie de sauvegarde,

MATERIEL

- Risque de ne pas avoir le matériel nécessaire au bon fonctionnement du système d'information,
- Risque de panne sur le matériel (smartphone, tablette, ordinateur, serveur, périphérique, routeur, réseau…) du fait de son obsolescence pouvant entrainer des pertes de données, des retards dans l'exécution voire l'arrêt des travaux,
- Risque de panne sur le matériel pouvant entrainer des pertes de données, des retards dans l'exécution voire l'arrêt des travaux,
- Risque d'accès frauduleux aux données ou de détérioration de celles-ci du fait :
  - ✓ d'une protection insuffisante du réseau informatique (droits d'accès, anti-virus, Firewall, anti-spam ou phishing…),
  - ✓ de la non mise à jour des systèmes de protection des données.
- Risque de panne et/ou de failles de sécurité sur les logiciels métiers et les systèmes d'exploitation de l'organisme du fait :
  - ✓ De leurs obsolescences,
  - ✓ De l'absence de mises à jour.
- Risque de perte de traçabilité sur les opérations réalisées sur le système d'information.

METHODE

- Risque d'insatisfaction des clients qui ne seraient pas informés de la politique de l'organisme en matière de protection des données et qui ne pourraient pas avoir accès à leurs données,
- Risque réglementaire relatif à l'absence de prise en compte des exigences opposables, par exemple le règlement général sur la protection des données,
- Risque de rupture de confidentialité : accès aux données par des personnes non autorisées du fait d'un défaut de définition des responsabilités et des droits d'accès au système d'information (peut concerner les collaborateurs, les fournisseurs et les clients),
- Documentation du système insuffisante (infrastructure matérielle du réseau, interactions de tous les logiciels composant le système d'information de l'organisme, description des opérations réalisés par des prestataires externes) pouvant entrainer une perte de connaissance du système en cas de départ ou d'indisponibilité des personnes en charge du système d'information,
- Risque d'utilisation de documents obsolètes du fait d'une revue documentaire ou d'une gestion de la documentation externe n'incluant pas le système d'information,
- Produits et services fournis par des prestataires externes :
  - ✓ Risque de faire appel à un prestataire de service ou un fournisseur informatique qui ne répond pas aux besoins du laboratoire,
  - ✓ Risque qu'un fournisseur de service, de logiciel ou de matériel informatique ne soit plus en mesure d'assurer la continuité de ses activités,
  - ✓ Risque qu'un fournisseur délivre un équipement ou un logiciel informatique qui ne soit pas totalement opérationnel et qui génère des informations erronées,
  - ✓ Risque qu'un fournisseur de service, de logiciel ou de matériel informatique ou d'équipement connecté ait accès à des données confidentielles lors de ses interventions dans les locaux de l'organisme ou à distance,
  - ✓ Dans le cadre de la mise en place d'une sous-traitance entre des organismes :
    - risque d'erreurs si des données informatiques sont échangées par exemple lors de l'envoi des demandes, la réception des résultats, l'amendement d'informations sur les résultats, les rapports d'analyses ou les comptes rendus…,
    - risque de perte des connexions informatiques (surtout lors des changements sur l'un ou l'autre des systèmes d'information des organismes),
    - risque que l'un ou l'autre des organismes ait accès à des données confidentielles qui ne lui sont pas indispensables pour la réalisation de ses prestations.
- Risque de ne pas détecter la défaillance d'un équipement informatique ou d'un logiciel,
- Risque de ne pas enregistrer les défaillances des équipements informatiques ou d'un logiciel et de ne pas mettre œuvre les éventuelles actions correctives nécessaires,
- Risque de ne pas avoir identifié tous les risques inhérents au système d'information et de ne pas avoir mis en place les moyens de maîtrise appropriés de ces risques,
- Risque de ne pas détecter qu'un moyen de maîtrise n'est plus adapté pour maîtriser efficacement un risque effectivement identifié par l'organisme,
- Risque de ne pas planifier et maîtriser correctement toutes les opérations sur le système d'information permettant d'améliorer son efficacité, sa sécurité…,
- Risque de ne pas identifier qu'une action d'amélioration ou corrective en lien avec le système d'information n'est pas efficace,
- Risque de ne pas détecter que les dispositions en lien avec le système d'information ne sont plus ou pas pertinentes vis-à-vis des besoins et des attentes des clients de l'organisme,
- Risque de ne pas avoir identifié que la politique liée au système d'information n'est plus en adéquation avec les besoins et les attentes des clients de l'organisme.

MAIN D'OEUVRE

- Risque d'avoir du personnel en nombre insuffisant pour gérer le système d'information,
- Risque d'erreur du fait d'une formation insuffisante sur les tâches qui sont confiées au personnel (en fonction des profils : utilisateur, paramétreur, administrateur, etc.),
- Risque de laisser un tiers accéder à des données, risque d'importer un virus ou un logiciel malveillant dans le système par méconnaissance des risques liés au système d'information et de la politique de l'organisme en matière de protection des données,
- Risque de réaliser volontairement des actes malveillants induisant la perte de données, la rupture de la confidentialité, la transmission erronée d'informations aux clients…,
- Risque d'avoir du personnel (interne ou externe) ne travaillant pas en toute impartialité,
- Risque d'erreur ponctuelle et involontaire induisant la perte de données, la rupture de la confidentialité, la transmission erronée d'informations aux clients…,
- Risque de ne pas savoir comment agir en cas de panne/problème informatique.

MILIEU

- Risque de ne pas pouvoir se rendre dans les locaux hébergeant le système d'information,
- Risque que l'infrastructure ne permette pas le télétravail à grande échelle, par exemple dans le cas d'un confinement sanitaire,
- Risque de perte de confidentialité du fait de l'ergonomie des postes de travail et des accès aux locaux non protégés permettant à une personne non autorisée d'accéder, de crypter ou de voler des donner,
- Risque de vol de matériel contenant des données (smartphone, tablette, ordinateur, disque dur…),
- Risque de destruction du matériel et de pertes de données du fait d'un incendie ou d'un évènement climatique majeur,
- Risque de panne du matériel, d'endommagement des supports de sauvegardes et plus largement de pertes des données du fait de conditions ambiantes non maitrisées (température, hygrométrie…) ou de réalisation d'activités incompatibles à proximité du matériel informatique (eau, poussières, ondes électromagnétiques…).

ANNEXE 3 : Gestion de projet

Il peut être nécessaire, pour un organisme confronté à une évolution importante de son système d'information, de mettre en place une gestion de projet. Cette gestion de projet doit lui permettre de gérer au mieux la mise en production d'un nouvel outil (SIL, GED, Centrale d'acquisition des températures), ou la mise en production d'une nouvelle version majeure d'un logiciel.

Les éléments relatifs à la définition des besoins, à la sélection du prestataire et à la phase de développement de l'outil ne sont pas traités dans cette annexe. Pour les 2 premiers items, l'organisme peut s'appuyer sur ses propres dispositions, en lien avec les exigences d'accréditation correspondantes. Pour la phase de développement informatique, le choix de la stratégie adoptée (Cycle en V, méthode Agile, etc.) relève de choix techniques et stratégiques adoptés par l'éditeur du logiciel, éventuellement en concertation avec l'organisme dans le cas d'outils développés spécifiquement.

Les éléments qui suivent traitent du déploiement et de la mise en production, au sein de l'organisme, du nouvel outil ou de la nouvelle version de l'outil considéré.

Rappel : Il s'agit d'une proposition de méthodologie qui ne constitue pas des exigences à satisfaire par les organismes.

1. Conduite du projet

La gestion du projet se décompose en plusieurs étapes décrites ci-dessous.

1.1. Constitution de l'équipe projet

L'organisme constitue une équipe pluridisciplinaire à même de gérer toutes les phases du projet. Les compétences du personnel choisi devraient couvrir un large spectre, à la fois informatique, métier et qualité. A titre d'exemple, les fonctions suivantes peuvent être représentées pour la mise en production d'un SIL : responsable du processus informatique, équipe informatique (y compris la partie infrastructure), responsable Technique, techniciens, responsable Qualité… Un chef de projet est nommé.

Dans le cadre d'un projet informatique important, les acteurs suivants peuvent intervenir :

- **La Maîtrise d'Ouvrage (MOA)** : elle représente l'utilisateur final. Elle est responsable de la qualité fonctionnelle de la solution. Elle définit les besoins fonctionnels de la solution (en concertation avec les utilisateurs – cahier des charges fonctionnel) et pilote le projet en concertation avec la MOE (Comité de Pilotage, planification…). Elle gère la phase de tests fonctionnels ;
- **La Maîtrise d'Œuvre (MOE)** : elle est responsable de la qualité technique de la solution. Elle assure le suivi de la réalisation technique des solutions, en général du développement, et participe à l'élaboration des jeux d'essai et à la réception des applications. Elle procède, avant toute réception contractuelle, aux vérifications nécessaires (la MOE réalise les tests techniques).

1.2. Formation du personnel du projet

Dans le cas d'un nouvel outil ou d'une évolution importante d'un outil déjà utilisé (par exemple le SIL), le personnel retenu pour constituer l'équipe projet connaît les fonctionnalités du logiciel et son mode de fonctionnement. Cette connaissance lui permettra de paramétrer et de tester le nouveau logiciel. Cette formation est le plus souvent réalisée par l'éditeur du logiciel, mais ce n'est

pas une obligation. Cette formation est tracée (programme de la formation, attestation de présence) et, si possible, fait l'objet d'une validation des acquis de la formation.

1.3. Phase de recueil des besoins et façons de faire

La réussite du projet repose, en grande partie, sur la qualité du paramétrage du logiciel. Et pour bien paramétrer, il est nécessaire de recenser, connaître, comprendre les pratiques de l'organisme et les besoins des utilisateurs. Cette étape repose sur des entretiens, des audits des pratiques. Des guides et formulaires de paramétrage pourront être mis en place par l'équipe projet pour assurer la traçabilité de cette étape.

1.4. Paramétrages

Cette étape de paramétrage est souvent la plus longue du projet, la plus fastidieuse, mais aussi la plus critique. Outre le paramétrage du logiciel à mettre en production, il est souvent nécessaire de revoir le paramétrage des outils périphériques. A titre d'exemple, dans le cas d'un nouveau SIL ou d'une évolution importante du SIL, il peut être nécessaire de revoir le paramétrage des équipements suivants : logiciels embarqués des automates, Middleware, outil d'aide à la validation, outil utilisé pour la diffusion des résultats (serveurs de résultat…), outil de traitement de données, équipements périphériques (imprimante, scanner, douchette code-barre, fax…)…

1.5. Phases de tests

De la qualité de la phase de tests dépend la réussite de la mise en production. L'exhaustivité des tests, c'est-à-dire réaliser des tests pour toutes les fonctionnalités du logiciel, est le plus souvent impossible, voire inutile. Il est en effet plus pertinent de concentrer les efforts de l'équipe projet sur des tests identifiés comme à risque. Pour identifier la liste des tests à réaliser, l'équipe projet établit, pour chaque fonctionnalité, une analyse des risques. En fonction de la criticité du risque, l'équipe projet testera, ou non, la fonctionnalité. Les tests seront de différentes natures : tests fonctionnels, tests d'intégration, tests de bout en bout (ou grandeur nature), tests de non-régression…

L'organisme pourra aussi choisir de réaliser des Qualifications d'Installation, Qualification Opérationnelles et Qualifications de Performance. A chaque anomalie identifiée pendant la phase de tests est associée une criticité, ou un impact (par exemple, mineur, majeur, bloquant…). En fonction de l'impact, l'équipe projet décidera, ou non, de mettre en place un correctif qui sera, lui aussi, testé.

Remarque : la Qualification de la Conception (QC) est de la responsabilité de l'éditeur du logiciel. Elle est de la responsabilité de l'organisme lorsqu'il est amené à développer son propre système d'information.

1.6. Formation du personnel et mise à jour de la documentation

Parallèlement à la phase de tests, il est nécessaire de former le personnel de l'organisme à l'utilisation du nouveau logiciel. Cette formation est tracée (programme de la formation, attestation de présence) et, si possible, fait l'objet d'une validation des acquis. La documentation, elle aussi, est mise à jour.

1.7. Information des clients de l'organisme

Lorsque le nouveau logiciel impacte les clients de l'organisme, une information, voire une formation, est réalisée.

1.8. GO – NO GO

A l'issu de la phase de tests, l'organisme prend la décision de mettre ou non en production le logiciel. C'est l'étape du GO – NO GO. Cette décision est collégiale, basée sur les résultats de la phase de tests, et notamment le nombre et la nature des anomalies identifiées lors des tests et qui

n'ont pas été corrigées. Le fait que des anomalies ne soient pas corrigées n'est pas, en soit, un frein à la mise en production. En fonction de leur nature, l'organisme peut choisir de mettre en place une solution dégradée pour la fonctionnalité non opérationnelle. La décision prise (GO ou NO GO) est tracée. Cet enregistrement, signé par une personne habilitée à autoriser la mise en production (par exemple, Directeur de l'organisme, responsable du processus informatique…) acte la décision prise et dresse un état de la phase de tests (par exemple, nombre et nature des anomalies non corrigées…). En cas de GO, une procédure dite de « retour arrière » est mise en place. Cette procédure consiste à remettre en production l'ancien logiciel, dans le cas où la mise en production du nouveau logiciel ne se passerait pas correctement.

1.9. Mise en production

Le grand jour arrive. Le personnel est formé, la documentation est revue, les fonctionnalités critiques sont testées, des solutions dégradées sont mises en place si nécessaire, les clients sont informés, tout est prêt pour la mise en production. La première journée post-mise en production est mise sous surveillance, pour identifier les éventuelles anomalies ou dysfonctionnements. En fonction des résultats obtenus, un « retour arrière » peut être décidé.

1.10. Outils de contrôle post mise en production

A l'instar de la première journée post-mise en production, l'organisme met en place un système de contrôle pour identifier et tracer les anomalies ou dysfonctionnements. En fonction de leur nature, l'organisme peut choisir de corriger le problème. La solution apportée sera testée et validée, avant mise en production.

2. Traçabilité associée à la conduite du projet

Dans le cadre de la gestion de projets ayant un impact sur les activités accréditées, il est nécessaire que l'organisme puisse démontrer comment les exigences d'accréditation qui lui sont opposables ont été respectées. Aussi, il assure la traçabilité des actions menées. La liste ci-dessous propose les enregistrements à conserver par étape clef (liste non exhaustive).

2.1. Cahier des charges

C'est le point d'ancrage de la validation. *Via* ce document, l'organisme exprime ses besoins : fonctionnalités du système, performances du système, exigences réglementaires, sécurité, ergonomie (Interface Homme/Machine – IHM), aspects Qualité…

2.2. Liste des fonctionnalités / évolutions

Etablir cette liste relève de la responsabilité de l'éditeur du logiciel (l'organisme s'assure qu'une telle liste existe). Cette liste, élément clef du projet, présente de nombreux intérêts. Elle permet de s'assurer que les besoins des utilisateurs sont couverts par les fonctionnalités de l'outil, d'établir la liste des fonctionnalités à tester…

2.3. Plan/protocole de validation (incluant l'analyse de risque)

La clef de voute du processus de validation du logiciel. Via ce document, l'organisme aborde les thèmes suivants :

- Les objectifs et le contexte du projet,
- Les documents de référence (décrets, normes, bonnes pratiques…),
- Une description du système à valider (fonctionnalités, architecture technique, environnement mis en place),
- L'organisation mise en place pour la validation (périmètre de la validation, phasage du projet et planning général, acteurs et signataires…),

- Le déroulement de la validation (analyse des risques, différentes phases de qualification, organisation et gestion documentaire…),
- Les procédures attendues pour garantir le maintien du statut validé (gestion des changements, sécurité, sauvegarde / restauration…).

2.4. Fiches de test (avec preuve de réalisation des tests)

Cette fiche décrit le test à réaliser, avec une précision qui dépendra de la complexité du logiciel, de sa connaissance par les recetteurs… Cette fiche de test peut traiter des points suivants (cf. exemple ci-dessous) :

- Instruction à suivre pour réaliser le test,
- Résultats attendus / Critères d'acceptation,
- Succès du test (O/N),
- Référence des fiches d'anomalie ouvertes,
- Commentaires.

	Fiche de tests PROJET SH GTA 02	
Référence du plan de validation : Plan-Validation-V02	Titre : Module Paramétrage	Page : 12/37

Instructions	Résultats attendus / Critères d'acceptation	Succès (O/N)	Réf. Fiche d'anomalie
12. (RF-31) : vérifier le renouvellement du mot de passe. • Se connecter sous un profil Biologiste • Réaliser la modification du mot de passe • Se déconnecter puis tenter de se reconnecter avec l'ancien mot de passe • Se connecter avec le nouveau mot de passe	La modification du mot de passe est correctement prise en compte : impossible de se connecter avec l'ancien mot de passe et connexion possible avec le nouveau mot de passe.		
Commentaire / Résultats obtenus / Conditions opératoires :			
13. (RF-40) : vérifier l'impossibilité de réutiliser les 3 anciens mots de passe selon le paramétrage effectué. • Se connecter sous un profil Technicien • Réaliser la modification du mot de passe 3+1 fois • Tenter de modifier à nouveau le mot de passe en utilisant chacun des 3 mots de passe utilisés précédemment • Se connecter avec le dernier (3+1) mot de passe	Le système ne permet pas la réutilisation des x anciens mots de passe lors de la modification du mot de passe.		
Commentaire / Résultats obtenus / Conditions opératoires :			

- **Fiches d'anomalie :** Cette fiche d'anomalie permet de tracer et traiter les anomalies/dysfonctionnements relevés lors de la phase de test.
- **Rapport de validation :** C'est un document de synthèse reprenant les fiches de test renseignées, le Procès-Verbal de recette, les preuves de réalisation des tests (en annexe).

Outre ces documents directement liés au projet et à sa phase de tests, d'autres documents sont conservés. A titre d'exemple, nous pouvons citer (liste non exhaustive) :

- Les documents liés aux formations, au processus d'habilitation du personnel…
- Les comptes rendus de réunion (Comité de Pilotage, réunion avec les clients de l'organisme, réunion avec les éditeurs des logiciels…),
- Un planning du projet,
- Un document de suivi des risques du projet,
- Un descriptif du paramétrage initial.

ANNEXE 4 : Récapitulatif des exigences communes aux différents référentiels

Attention : les § mentionnés sont ceux des versions en vigueur au moment de la parution du présent guide. En cas d'évolution d'une norme, il appartient aux utilisateurs de ce tableau d'effectuer leur analyse d'impact dans l'attente d'une version ultérieure du guide.

Norme	Confidentialité des données	Intégrité des données	Disponibilité des données	Archivage électronique	Validation des SI	Rapport sur les résultats	Prestataire externes
NF EN ISO 15189	§ 4.2 § 6.3.2.a § 7.4.1.4.e § 7.6.3.c § 8.4.3.a	§ 4.3.g §7.6.3 § 8.4	§ 4.3.g § 6.2.3.c § 7.6.1 et 7.6.4 § 8.4.3	§ 4.3.g § 8.4.3	§ 7.4.1.5 § 7.6.3	§ 7.4.1.1 § 7.4.1.4 à 7.4.1.7	§ 6.8 § 7.6.5
NF EN ISO/CEI 17025	§ 4.2 § 7.11.3.a et 7.11.4 § 8.4.2	§ 7.5.1 et 7.5.2 § 7.11.3 et 7.11.6 § 8.4.1 et 8.4.2	§ 7.11.1 et 7.11.3.b § 8.4.1 et 8.4.2	§ 7.11.1 § 8.4.1 et 8.4.2	§ 6.4.13.c § 7.11.2 et 7.11.6	§ 7.8.1.2	§ 4.2.4 § 6.6 § 7.11.4
NF EN ISO 17034	§ 4.3 § 7.8.2.d § 7.16.5 et 7.16.6 § 8.5.2	§ 7.8.1 et 7.8.2.b, c et d § 7.16.3 à 7.16.6	§ 7.8.2.d § 7.16.6	§ 7.16.3, 7.16.5 à 7.16.7 § 8.5.2	§ 7.8.2.a	§ 7.14	§ 6.3
NF EN ISO/CEI 17043	§ 4.2 § 7.1.2 § 7.4.3.2.f § 8.4.3	§ 7.4.1.1 § 7.5.1 et 7.5.2.3 § 8.4	§ 7.5.2.1 § 8.4.2 et 8.4.3	§ 8.4.2 et 8.4.3	§ 7.5.2.2 et 7.5.2.6	§ 7.4.3.1	§ 6.4 § 7.5.2.4
NF EN ISO/CEI 17020	§ 4.2 § 6.1.13 § 8.4.2	§ 6.2.13.b § 7.1.7 et 7.1.8	§ 6.2.13.b	§ 6.2.13.b § 8.4.1 et 8.4.2	§ 6.2.13.a	§7.1.8 § 7.4	§ 6.2.11 et 6.2.13

Norme	Confidentialité des données	Intégrité des données	Disponibilité des données	Archivage électronique	Validation des SI	Rapport sur les résultats	Prestataire externes
NF EN ISO/IEC 17029	§ 4.3.3 § 7.2.6 § 9.11.2 § 10.4	§ 9.5.4 § 9.11.2 § 11.6.1, 11.6.2 et 11.6.4	§ 9.6.5 § 9.11 § 10.1 et 10.2 § 11.6.1 et 11.6.2	§ 9.11.1 et 9.11.3 § 11.1.1 § 11.6.2 et 11.6.3	∅	§ 9.7	§ 7.2.6 § 7.4
NF EN ISO/CEI 17021-1	§ 8.4 § 9.9.3 § 9.8.5 § 10.2.4	§ 9.9.4 § 10.2.4	§ 9.9.4 § 10.2.4	§ 9.9.4 § 10.2.4	∅	§ 8.2 § 9.4.8 § 9.9.2	§ 7.5
NF EN ISO/CEI 17024	§ 6.1.6 § 6.2.2.3 et 6.2.3.2 § 6.3.1 § 7.1.2 § 7.3 § 9.9.9 § 10.2.4	§ 7.1.2 § 10.2.3 et 10.2.4	§ 7.1.2 § 10.2.3 et 10.2.4	§ 7.1.2 § 10.2.3 et 10.2.4	∅	§ 7.1.1 § 9.2.3 § 9.4.7 et 9.4.8 § 10.2.4	§ 6.3
NF EN ISO/CEI 17065	§ 4.5.1 § 6.1.1.3 et 6.1.3 § 6.2.2.3 § 7.12.2 § 8.4.2	§ 8.4.1	§ 8.3.2 § 8.4.1	§ 7.12.3 § 8.3.2 § 8.4.1 et 8.4.2	∅	§ 7.7 § 7.12	§ 6.2.2 § 7.4.4 et 7.4.5

∅ : *point non abordé explicitement dans la norme considérée*