SANTÉ

ETABLISSEMENTS DE SANTÉ

Gestion

MINISTÈRE DES AFFAIRES SOCIALES
ET DE LA SANTÉ

Direction générale de l'offre de soins

Sous-direction du pilotage de la performance
des acteurs de l'offre de soins

Mission systèmes d'information des acteurs
de l'offre de soins (MSIOS)

Instruction DGOS/MSIOS n° 2013-62 du 21 février 2013 relative au Guide méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé

NOR : *AFSH1304975J*

Validée par le CNP le 1er février 2013. – Visa CNP 2013-22.

Catégorie : directives adressées par le ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.

Résumé : présentation du Guide méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé.

Référence : circulaire interministérielle DGOS/DGFIP/PF/PF1/CL1B n° 2011-391 du 10 octobre 2011 relative au lancement du projet de fiabilisation des comptes de l'ensemble des établissements publics de santé.

Mots clés : systèmes d'information, auditabilité, accompagnement à l'atteinte des prérequis, boîte à outils.

Annexe : Guide méthodologique pour l'auditabilité des SI.

La ministre des affaires sociales et de la santé à Mesdames et Messieurs les directeurs des agences régionales de santé ; Mesdames et Messieurs les directeurs des établissements publics de santé (pour mise en œuvre).

Cette instruction a pour objet de présenter le Guide méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé.

1. **Contexte et enjeux**

Le projet de fiabilisation et de certification des comptes

L'article 17 de la loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires du 21 juillet 2009 (loi HPST) a inscrit dans le code de la santé publique, article L. 6145-16, le principe de la certification des comptes de certains établissements publics de santé. Le point II de cet article 17 de la loi du 21 juillet 2009 prévoit l'entrée en vigueur de la certification des comptes au plus tard sur les comptes de l'exercice 2014 pour les établissements concernés. À ce jour, le décret d'application et le calendrier associé sont en cours d'élaboration. Dans l'attente de cette échéance, la priorité est donnée à la fiabilisation des comptes de l'ensemble des établissements publics de santé.

Un espace Internet du ministère chargé de la santé présente la documentation utile à l'amélioration de la qualité des comptes ainsi qu'à la mise en œuvre de cette certification : http://www.sante.gouv.fr/la-fiabilisation-et-la-certification-des-comptes-des-etablissements-

publics-de-sante.html. Cet espace renvoie notamment sur la circulaire interministérielle DGOS/DGFIP/PF/PF1/CL1B nº 2011-391 du 10 octobre 2011 relative au lancement du projet de fiabilisation des comptes de l'ensemble des établissements publics de santé, qui précise les orientations stratégiques et le calendrier général préconisés pour fiabiliser les comptes de l'ensemble des établissements publics de santé et faciliter la préparation de la certification des comptes des établissements soumis à terme à cette obligation.

L'auditabilité des systèmes d'information

Dans le cadre du projet de fiabilisation des comptes et en préparation à la certification des comptes, les établissements publics de santé doivent se préparer à répondre aux exigences de contrôle interne ou d'auditabilité des systèmes d'information (SI). La notion d'auditabilité fait référence à la traçabilité des opérations et des contrôles réalisés et de la documentation produite, les contrôles non documentés étant réputés non réalisés.

Les certificateurs s'appuient sur la qualité du contrôle interne, notamment des systèmes d'information concourant à l'élaboration de l'information comptable et financière des établissements. Ils pourront être amenés, dans ce cadre, à examiner les éléments suivants :

– les éléments d'organisation et de contrôle sur lesquels s'appuie le système d'information des établissements, comme par exemple : l'organisation de la direction des systèmes d'information (DSI), la démarche de conduite des projets SI dans l'établissement, la cartographie des SI, les contrôles généraux informatiques en place au sein de la DSI, les procédures de recette et de test réalisées avant mise en production des applications ;
– la fiabilité des applications informatiques utilisées (couverture fonctionnelle, paramétrage et mise en œuvre de la règlementation).

2. **Le Guide méthodologique pour l'auditabilité des systèmes d'information**

Un groupe de travail dédié

Un groupe de travail dédié, piloté par la DGOS, a été constitué de septembre à décembre 2012 afin d'élaborer le Guide d'auditabilité des systèmes d'information. Le groupe de travail était composé de professionnels de terrain et de représentants institutionnels :

– représentants de DSI(O) (directeurs des systèmes d'information [et de l'organisation]) d'établissements de santé publics (CHU et CH) et ESPIC, suite à un appel à candidatures auprès des collèges de DSIO de CHU et de CH et des fédérations concernées ;
– représentants de la CNCC (Compagnie nationale des commissaires aux comptes) ;
– représentants de la DGFiP (direction générale des finances publiques) ;
– représentants de la DGOS (direction générale de l'offre de soins).

Les objectifs du Guide d'auditabilité des systèmes d'information

Le Guide d'auditabilité des systèmes d'information s'adresse en particulier aux établissements de santé se préparant à la certification des comptes mais les bonnes pratiques mentionnées s'appliquent à l'ensemble des établissements inscrits dans une démarche de fiabilisation des comptes. Il constitue un guide méthodologique pratique à destination des directeurs des systèmes d'information leur permettant de définir :

– les bonnes pratiques relatives au contrôle interne du système d'information ;
– les documents et éléments de preuve qui devront être produits et conservés par les établissements en vue de faciliter la certification (cartographie du SI, guide utilisateur des applications...) ;
– les niveaux de contrôle minimum requis pour les établissements qui développent et maintiennent les applications de leur SIH ;
– les documents et éléments probants produits et conservés par les établissements (cartographie du SI, guide utilisateur des applications...).

Composition du guide

Le guide est composé de trois parties :

Partie 1 : présentation de la démarche globale de certification des comptes, de l'impact des systèmes d'information sur la démarche et des étapes de la revue du SI ;

Partie 2 : préparation des établissements à l'audit de leur SI ;

Partie 3 : fiches pratiques de mise en œuvre. Ces fiches sont disponibles au sein de ce guide et sont également téléchargeables sur l'espace Internet du programme (http://www.sante.gouv.fr/la-fiabilisation-et-la-certification-des-comptes-des-etablissements-publics-de-sante.html) en version tableur, modifiables par les établissements qui peuvent ainsi les remplir et les adapter.

Le Guide méthodologique pour l'auditabilité des systèmes d'information est présenté en annexe de la présente instruction.

Je vous prie de bien vouloir assurer la diffusion de cette instruction et de son annexe à vos services ainsi qu'aux établissements de santé. Je vous invite à me faire part des difficultés éventuelles que vous pourriez rencontrer dans sa mise en œuvre, en prenant contact, le cas échéant, avec la mission systèmes d'information des acteurs de l'offre de soins (dgos-msios@sante.gouv.fr).

Pour la ministre et par délégation :
Le directeur général de l'offre de soins,
J. DEBEAUPUIS

ANNEXE

GUIDE MÉTHODOLOGIQUE POUR L'AUDITABILITÉ DES SI

SOMMAIRE

INTRODUCTION

Le projet de fiabilisation et de certification des comptes

L'article 17 de la loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires du 21 juillet 2009 (loi HPST) a inscrit dans le code de la santé publique (art. L. 6145-16) le principe de la certification des comptes de certains établissements publics de santé. Le point II de cet article 17 de la loi du 21 juillet 2009 prévoit l'entrée en vigueur de la certification des comptes au plus tard sur les comptes de l'exercice 2014 pour les établissements concernés. À ce jour, le décret d'application et le calendrier associé sont en cours d'élaboration. Dans l'attente de cette échéance, la priorité est donnée à la fiabilisation des comptes de l'ensemble des établissements publics de santé.

La direction générale de l'offre de soins (DGOS) et la direction générale des finances publiques (DGFiP), en lien avec la Cour des comptes et la Compagnie nationale des commissaires aux comptes, se sont organisées pour aider les établissements publics de santé à se préparer à la fiabilisation puis à la certification de leurs comptes. Elles assurent depuis 2009 le pilotage de ce projet ainsi que l'animation de différents groupes de travail et sont chargées de préparer le cadre réglementaire et la documentation nécessaire à la mise en œuvre de la certification des comptes des établissements publics de santé. Les agences régionales de santé (ARS), la Fédération hospitalière de France (FHF), les conférences de directeurs et les conférences de présidents de CME d'établissements publics de santé sont également associées au projet.

Un espace Internet du ministère chargé de la santé présente la documentation utile à l'amélioration de la qualité des comptes ainsi qu'à la mise en œuvre de cette certification : http://www.sante.gouv.fr/la-fiabilisation-et-la-certification-des-comptes-des-etablissements-publics-de-sante.html. Cet espace renvoie notamment sur la circulaire interministérielle DGOS/DGFIP/PF/PF1/CL1B n° 2011-391 du 10 octobre 2011 relative au lancement du projet de fiabilisation des comptes de l'ensemble des établissements publics de santé, qui précise les orientations stratégiques et le calendrier général préconisés pour fiabiliser les comptes de l'ensemble des établissements publics de santé et faciliter la préparation de la certification des comptes des établissements soumis à terme à cette obligation.

L'auditabilité des systèmes d'information

Dans le cadre du projet de fiabilisation des comptes et en préparation à la certification des comptes, les établissements publics de santé doivent se préparer à répondre aux exigences de contrôle interne ou d'auditabilité des systèmes d'information (SI). La notion d'auditabilité fait référence à la traçabilité des opérations et des contrôles réalisés et de la documentation produite, les contrôles non documentés étant réputés non réalisés.

Les certificateurs s'appuient sur la qualité du contrôle interne, notamment des systèmes d'information concourant à l'élaboration de l'information comptable et financière des établissements. Ils pourront être amenés, dans ce cadre, à examiner les éléments suivants :

- les éléments d'organisation et de contrôle sur lesquels s'appuie le système d'information des établissements, comme : l'organisation de la direction des systèmes d'information (DSI), la démarche de conduite des projets SI dans l'établissement, la cartographie des SI ;
- les contrôles généraux informatiques en place au sein de la DSI, les procédures de recettes et de tests réalisées avant mise en production des applications ;
- la fiabilité des applications informatiques utilisées (couverture fonctionnelle, paramétrage et mise en œuvre de la réglementation).

Le guide d'auditabilité des SI

Un groupe de travail dédié

Un groupe de travail dédié, piloté par la DGOS (mission systèmes d'information des acteurs de l'offre de soins [MSIOS] et bureau de l'efficience des établissements de santé publics et privés [PF1]), a été constitué de septembre à décembre 2012 afin d'élaborer le guide d'auditabilité des SI. Le groupe de travail était composé de professionnels de terrain et de représentants institutionnels :

- représentants de DSI(O) (directeurs des systèmes d'informations [et de l'organisation]) d'établissements de santé publics (CHU de Tours, CHU de Besançon, hôpitaux de Saint-Maurice, CH de Saint-Denis, CH de Lens, CH de Laon) et ESPIC (fondation Hopale), suite à un appel à candidatures auprès des collèges de DSIO de CHU et de CH et des fédérations concernées ;
- représentants de la CNCC (Compagnie nationale des commissaires aux comptes) ;
- représentants de la DGFiP (direction générale des finances publiques) ;
- représentants de la DGOS (direction générale de l'offre de soins).

Les objectifs du guide d'auditabilité des SI

Le guide d'auditabilité des SI s'adresse en particulier aux établissements de santé se préparant à la certification des comptes, mais les bonnes pratiques mentionnées s'appliquent à l'ensemble des établissements inscrits dans une démarche de fiabilisation des comptes. Il constitue un guide méthodologique pratique à destination des directeurs des systèmes d'information leur permettant de définir :

– les bonnes pratiques relatives au contrôle interne du système d'information ;
– les documents et éléments de preuve qui devront être produits et conservés par les établissements en vue de faciliter la certification (cartographie du SI, guide utilisateur des applications...) ;
– les niveaux de contrôle minimum requis pour les établissements qui développent et maintiennent les applications de leur SIH.

Ce guide a pour périmètre le système d'information de l'établissement : les autres systèmes d'information concourant à la production des états financiers (Helios par exemple) ne sont pas traités dans ce document. Ce guide n'a pas vocation à prévaloir sur les textes, réglementations en vigueur ou à venir, ni sur les normes ou pratiques qui seront adoptées par les certificateurs mais vise essentiellement à apporter un éclairage sur les travaux à engager sur le volet système d'information du projet de fiabilisation et de certification des comptes.

Composition du guide

Le guide est composé de trois parties :

– partie 1 : présentation de la démarche globale de certification des comptes, de l'impact des systèmes d'information sur la démarche et des étapes de la revue du SI ;
– partie 2 : préparation des établissements à l'audit de leur SI ;
– partie 3 : fiches pratiques de mise en œuvre. Ces fiches sont disponibles au sein de ce guide et sont également téléchargeables sur l'espace Internet du programme (http://www.sante.gouv.fr/la-fiabilisation-et-la-certification-des-comptes-des-etablissements-publics-de-sante.html) en version tableur, modifiables par les établissements, qui peuvent ainsi les remplir et les adapter.

PARTIE 1

PRÉSENTATION DE LA DÉMARCHE GLOBALE

1.1. *La démarche d'audit*

1.1.1. La démarche du certificateur

La certification des comptes est une mission d'audit externe des comptes qui consiste à exprimer une assurance que les comptes pris dans leur ensemble ne comportent pas d'anomalie significative.

À l'issue de son audit, le certificateur émet un rapport d'opinion dans lequel :

– il certifie que les comptes annuels sont réguliers et sincères et qu'ils donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de la situation financière et du patrimoine de l'entité à la fin de cet exercice ;
– il assortit la certification de réserves ;
– il refuse la certification des comptes.

Dans ces deux derniers cas, il précise les motifs de sa décision. Le certificateur peut également formuler, dans son rapport d'opinion, des observations afin d'attirer l'attention sur une information fournie dans l'annexe du compte financier.

La régularité et sincérité des comptes ainsi que l'image fidèle que doivent présenter les états financiers sont des exigences prévues par le décret n° 2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique. L'article 53 précise en effet notamment que : « La comptabilité publique est un système d'organisation de l'information financière permettant :

1° De saisir, de classer, d'enregistrer et de contrôler les données des opérations budgétaires, comptables et de trésorerie afin d'établir des comptes réguliers et sincères.
2° De présenter des états financiers reflétant une image fidèle du patrimoine, de la situation financière et du résultat à la date de clôture de l'exercice. »

L'article 57 (1) recense les objectifs qui permettent de répondre à ces exigences.

Pour formuler son opinion, le certificateur recherche l'assurance que les comptes, pris dans leur ensemble, ne comportent pas d'anomalies significatives.

Compte tenu de la masse des opérations, le certificateur ne vérifie pas toutes les opérations comptabilisées. De ce fait, sa mission, telle que prévue par les normes, s'appuie sur l'analyse et l'évaluation des organisations, des méthodes, des systèmes d'information et des processus qui ont permis d'élaborer les informations comptables.

Ainsi, la démarche du certificateur est fondée sur une approche par les risques. Son objectif est d'apprécier comment l'organisation, les processus et les dispositifs de contrôle mis en place assurent un niveau de maîtrise satisfaisant de ces risques et permettent donc de réduire le risque de survenance d'anomalies significatives dans les comptes. Sa démarche couvre les champs de compétences de l'ordonnateur et du comptable.

Les normes d'audit internationales et françaises soulignent l'importance pour le certificateur de bien comprendre l'environnement dans lequel opère l'établissement, d'apprécier les risques inhérents à ses activités, d'évaluer les dispositifs de contrôle mis en œuvre.

Le COSO (Committee of Sponsoring Organizations), auquel se réfèrent habituellement les certificateurs, définit le contrôle interne comme un processus mis en œuvre par les dirigeants à tous les niveaux de l'entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants : l'efficacité et l'efficience des opérations, la fiabilité des informations financières, la conformité aux lois et règlements.

Les termes de « risque d'audit » et de « niveau de risque » sont évoqués dans la définition des différentes normes auxquelles est soumis le certificateur :

Le « risque d'audit » est le risque que le commissaire aux comptes exprime une opinion incorrecte du fait d'anomalies significatives contenues dans les comptes et non détectées. Il se subdivise en trois composants :

– le « risque inhérent » correspond à la possibilité que, sans tenir compte du contrôle interne qui pourrait exister dans l'entité, une anomalie significative se produise dans les comptes ;

(1) « La qualité des comptes des personnes morales mentionnées à l'article 1er est assurée par le respect des principes comptables, tels que définis par les règles arrêtées par le ministre chargé du budget, dans les conditions fixées à l'article 54.
Elle doit répondre aux exigences énoncées aux 1° et 2° de l'article 53 au regard notamment des objectifs suivants :
1° Les comptes doivent être conformes aux règles et procédures en vigueur ;
2° Ils doivent être établis selon des méthodes permanentes, dans le but d'assurer leur comparabilité entre exercices comptables ;
3° Ils doivent appréhender l'ensemble des événements de gestion, en fonction du degré de connaissance de leur réalité et de leur importance relative, dans le respect du principe de prudence ;
4° Ils doivent s'attacher à assurer la cohérence des informations comptables fournies au cours des exercices successifs en veillant à opérer le bon rattachement des opérations à l'exercice auquel elles se rapportent ;
5° Ils doivent être exhaustifs et reposer sur une évaluation séparée et une comptabilisation distincte des éléments d'actif et de passif ainsi que des postes de charges et de produits, sans possibilité de compensation ;
6° Ils doivent s'appuyer sur des écritures comptables fiables, intelligibles et pertinentes visant à refléter une image fidèle du patrimoine et de la situation financière. »

– le « risque lié au contrôle » correspond au risque qu'une anomalie significative ne soit ni prévenue ni détectée par le contrôle interne de l'établissement et donc non corrigée en temps voulu ;
– le « risque de non-détection » est propre à la mission d'audit : il correspond au risque que le certificateur ne parvienne pas à détecter une anomalie significative.

Le niveau de risque peut être accru du fait de l'existence de lois et règlements complexes affectant l'activité. Par ailleurs, certaines situations et évènements constituent des facteurs de risques aggravants comme :
– l'ouverture de nouvelles activités ou de nouveaux services ;
– l'existence d'un plan de restructuration ;
– des changements informatiques importants ;
– des changements de technologie majeurs dans l'activité ;
– l'absence de personnel qualifié en matière comptable et financière ;
– des changements récents de direction financière ;
– la première application de nouvelles règles comptables ;
– etc.

Dans ce contexte, le certificateur va adapter sa démarche aux risques identifiés et non pas uniquement au volume des transactions. Cette méthodologie se fonde sur la compréhension des activités et des enjeux de l'établissement par l'analyse de ses processus opérationnels, ainsi que sur la revue critique des dispositifs de maîtrise et de gestion des risques, c'est-à-dire l'examen du contrôle interne mis en place et des systèmes d'information qui concourent à la qualité de la gestion dans l'établissement.

1.1.2. Les étapes clés de la démarche d'audit

La démarche classique de l'audit s'articule autour de quatre grandes étapes :

1. Planification de la mission

Cette étape comporte notamment l'approche générale des travaux, le niveau de supervision, les ressources nécessaires pour la réalisation de la mission, les besoins d'intervenants externes et d'autres professionnels.

2. Prise de connaissance de l'établissement et de son environnement

Cette étape vise à recueillir les éléments relatifs au secteur d'activité, aux caractéristiques de l'établissement, aux indicateurs de performance financière, aux éléments de contrôle interne pertinents pour l'audit.

3. Évaluation du risque d'anomalies significatives

Cette étape consiste à apprécier l'efficacité du contrôle interne à détecter ou corriger des anomalies significatives dans les comptes.

4. Procédures d'audit mises en œuvre à l'issue de l'évaluation des risques

Les procédures d'audit comprennent les tests de procédures et les contrôles de substance. Dans cette étape, le certificateur détermine l'étendue et le calendrier de la mise en œuvre de ces procédures au regard des risques d'anomalies significatives identifiés.

La démarche d'audit s'accompagne de communications à l'organe collégial chargé de l'administration, à la direction et à l'organe de surveillance, selon les modalités définies par l'article L. 823-16 du code de commerce. D'autres restitutions peuvent être réalisées, et pourront notamment porter sur :
– une restitution détaillée et critique des travaux sur les procédures de contrôle interne de l'établissement en insistant sur les axes d'amélioration ;
– un compte rendu d'intervention sur les comptes de l'exercice qui reprend la synthèse des travaux sur les procédures précédemment détaillées et présente des points clés des travaux sur les comptes ;
– le cas échéant, un rapport détaillé sur l'intervention des spécialistes des systèmes d'information ;
– la participation à la réunion du conseil de surveillance délibérant sur les comptes.

1.1.3. Les risques liés aux systèmes d'information

Au regard des points précédents, le certificateur ne s'intéressera pas seulement aux comptes, mais il examinera les modalités d'acquisition des données, leur gestion et leur traitement, étant précisé que certaines de ces données sont soumises au secret médical, ainsi que la qualité de l'organisation des systèmes informatiques.

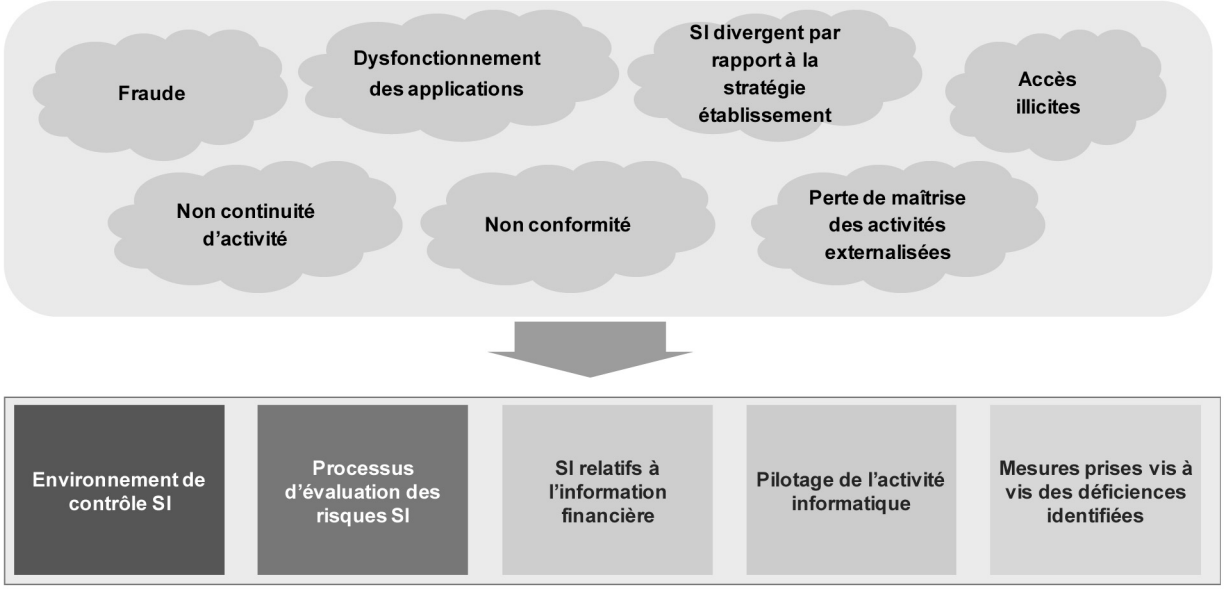
Dès lors, la prise en compte de l'environnement des systèmes d'information hospitalier (SIH) et des applications qui le composent devient une nécessité. La nature des risques, dans un environnement informatique, est liée aux spécificités suivantes :
– le manque de trace matérielle justifiant les opérations, qui entraîne un risque plus important de non-détection des erreurs contenues dans les programmes d'application ou les logiciels d'exploitation ;

– l'uniformité du traitement des opérations, qui permet d'éliminer quasiment toutes les erreurs humaines ; en revanche, les erreurs de programmation peuvent entraîner un traitement incorrect de toutes les opérations ;
– la séparation des tâches intégrée dans le paramétrage du système, qui n'est plus seulement physique (échange de documents), mais également logique avec un risque accru (*cf.* paragraphe 2.3.1 dédié à la séparation des fonctions) ;
– le risque d'erreurs et d'irrégularités, qui peut provenir :
  – d'erreurs humaines dans la conception, la maintenance et la mise en œuvre, plus importantes que dans un système manuel ;
  – d'utilisateurs non autorisés qui accèdent, modifient, suppriment des données sans trace visible.

L'exemple suivant illustre le risque d'impact qu'un changement non maîtrisé peut avoir sur les états financiers et la nécessité pour l'établissement de prendre en compte ces processus : un service disposant d'un logiciel de spécialité a souhaité mettre à jour la version en place afin de disposer des nouvelles fonctionnalités proposées par l'éditeur. Cette mise à jour mineure a été effectuée sans sollicitation de la DSI. Après quelques semaines de fonctionnement, le service contrôle de gestion de l'établissement s'étonne d'une baisse sensible et durable de l'activité. Une première investigation terrain n'apporte pas d'élément probant venant confirmer ou infirmer cette tendance, autre qu'une évolution temporaire des pathologies traitées. Ce n'est qu'une seconde investigation, menée cette fois avec la DSI, quelques semaines après (la tendance baissière étant toujours constatée) qui révélera à la DSI qu'une mise à jour a été réalisée et que celle-ci a impacté les interfaces de remontée d'informations. Le montant des actes en retard de facturation a été évalué à plusieurs centaines de milliers d'euros.

Par ailleurs, la possibilité de détection de ces erreurs et irrégularités est affectée par le fait qu'elles sont souvent intégrées lors de la conception ou de la modification de programmes d'application ou de logiciels d'exploitation, et sont aussi difficilement identifiables dans le temps.

Ci-après sont schématisés des exemples de risques auxquels l'établissement doit faire face et qui doivent être couverts par la prise de connaissance de l'environnement informatique par le certificateur :



Le terme « déficiences » s'entend des faiblesses du contrôle interne de l'établissement de santé.

1.2. *L'audit des systèmes d'information*

1.2.1. Le périmètre des systèmes d'information entrant dans le champ d'action du certificateur

Le champ d'investigation du certificateur, en matière de système d'information, inclut tout ou partie des applications intervenant dans la saisie et le traitement des informations, entre la survenance du fait générateur et la production des états financiers, et ce pour l'ensemble des opérations ayant un impact sur la production des états financiers.

Les applications concernées par l'auditabilité du système d'information sont notamment :
– celles supportant le périmètre des cinq principaux processus du cycle comptable : recettes, personnel, immobilisations, achats d'exploitation, endettement long terme et trésorerie court terme ;

– les progiciels (applications standardisées ou adaptées acquises auprès d'éditeurs ou intégrateurs), développements spécifiques (applications développées en interne par l'établissement) ainsi qu'outils bureautiques de type tableur ou bases de données ;
– pour les établissements de santé publics : le système comptable commun Hélios (hors AP-HP) et les interfaces mises en place avec le SIH de l'établissement (1). Un exemple de cartographie applicative est fourni dans la fiche de prise de connaissance du système d'information : il présente un exemple de périmètre applicatif pouvant être pris en compte dans le cadre d'une démarche de fiabilisation des comptes (*cf.* partie 3, fiche 1).

1.2.2. L'impact des systèmes d'information sur la démarche de certification

La prise en compte de l'environnement informatique lors de l'audit des comptes est indispensable, dans la mesure où les systèmes d'information ont un impact :
– sur l'orientation et la planification de la mission ;
– sur l'évaluation du risque (risque inhérent et risque lié au contrôle) ;
– sur la conception et l'exécution des tests de procédures et des contrôles de substance (*i.e.* contrôles ayant pour but d'obtenir des éléments probants afin de détecter des anomalies significatives dans les comptes).

L'audit réalisé dans un environnement informatique amène le certificateur à adapter son approche, la nature des contrôles à réaliser et l'exploitation des résultats obtenus à l'issue de ces contrôles.

Exemple 1 :

Les utilisateurs sont fortement impliqués dans les choix informatiques majeurs. Des représentants des utilisateurs participent à la validation du plan informatique définissant les objectifs et l'emploi des ressources informatiques (calendrier général, budget).

Le responsable informatique est conscient des enjeux liés aux réglementations en vigueur. Il dispose notamment d'une cartographie précise de son SIH, des interfaces et pilote l'ensemble des traitements.

Exemple 2 :

Un établissement présentant une informatique vieillissante, développée par des informaticiens ayant quitté l'établissement, ne peut plus adapter son système d'information à ses nouvelles contraintes. Si les programmes sont complexes et mal documentés, il est probable que plus personne ne sera en mesure de faire évoluer les systèmes d'information : il faudra donc les refondre totalement.

Les adaptations du système nécessaires à sa maintenance et à la mise en œuvre des évolutions réglementaires (par exemple : facturation individuelle des établissements de santé [FIDES], protocole standard de dématérialisation des titres de recette, des mandats de dépense et des bordereaux récapitulatifs [PES V2]) peuvent s'avérer très difficiles à mettre en œuvre ou très coûteuses.

Dans l'exemple 2, en dehors de toutes autres considérations qui pourraient apparaître lors de l'analyse des contrôles généraux ou applicatifs, le niveau de risque semble plus élevé que dans l'exemple 1. Il pourra conduire le certificateur à adapter sa démarche, par exemple en mettant en œuvre davantage de contrôles de substance (2).

Dans ce contexte, la part croissante des systèmes d'information et leur complexité ont amené le certificateur à apprécier l'incidence de l'environnement informatique sur sa démarche, au travers notamment :
– de la prise de connaissance de l'informatique dans l'établissement et de son incidence sur la production des informations financières et comptables ;
– de l'identification des principales composantes du système d'information et de son niveau de complexité.

Toutefois, la prise en compte de l'environnement informatique lors de l'audit des comptes ne doit pas être confondue avec l'audit informatique d'un système d'information, confié généralement à des experts spécialisés.

Les points d'attention du certificateur, selon les exigences professionnelles dans le cadre d'un environnement informatisé, s'appuieront sur les principes suivants :
– l'existence d'un environnement informatique ne modifie pas l'objectif et l'étendue de la mission du commissaire aux comptes ;
– l'utilisation des moyens informatiques modifie la saisie et le processus de traitement et de conservation des données et en conséquence peut avoir une incidence sur les systèmes comptables et de contrôle interne de l'entité ;
– un environnement informatique peut ainsi avoir une incidence sur la démarche du certificateur lors de :
  – la prise de connaissance des systèmes comptables et de contrôle interne ;
  – la prise en compte du risque inhérent et du risque lié au contrôle ;

(1) Ce guide a pour périmètre le système d'information des établissements : il ne traite pas des contrôles propres au système Hélios, mais uniquement des interfaces entre le système Hélios et le SIH des établissements.

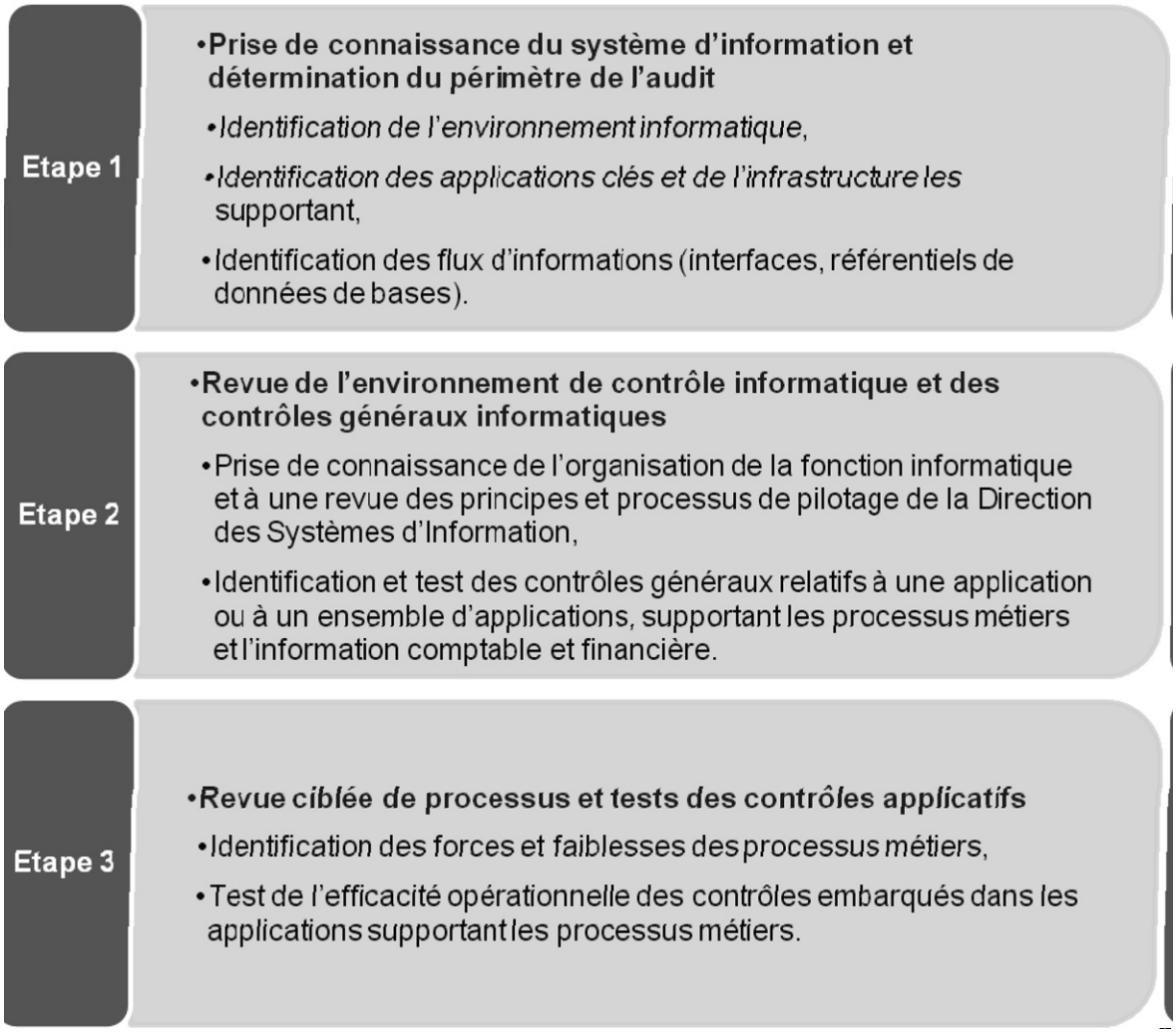
(2) Les contrôles de substance sont des procédures d'audit qui incluent les test de détail visant à contrôler un élément individuel faisant partie d'une catégorie d'opérations ou d'un solde ainsi que les procédures analytiques.

– la mise en œuvre des procédures d'audit.

Les normes en vigueur mettent également l'accent sur certaines spécificités à prendre en considération par le certificateur pour atteindre l'objectif de l'audit, notamment les compétences du certificateur et de son équipe au regard de la complexité de l'environnement informatique de l'entité. Dans ce cadre, le certificateur « détermine si des compétences informatiques particulières sont nécessaires pour réaliser la mission ». Si tel est le cas, il se fait assister par un professionnel possédant ces compétences, qui peut être un collaborateur ou un spécialiste externe.

1.2.3. Les étapes de la revue du SIH dans la démarche d'audit

Les étapes présentées ci-dessous constituent la démarche type du certificateur pour l'audit du système d'information.



Étape 1 : prise de connaissance du système d'information

La prise de connaissance du système d'information consiste, d'une part, à recueillir et formaliser les éléments de contexte généraux relatifs à l'organisation et au pilotage du SIH et, d'autre part, à définir, et formaliser le périmètre des applications informatiques pouvant entrer dans le champ d'action du certificateur. Les éléments recherchés sont les suivants :

– comprendre l'environnement informatique ;
– déterminer les contrôles applicatifs et contrôles généraux informatiques qui les supportent ;
– identifier les applications informatiques pertinentes ;
– identifier les contrôles applicatifs et les rapports générés par le système sur lesquels le certificateur pourra s'appuyer ;
– identifier dans quelles applications sont localisés les contrôles automatisés et les rapports générés par le système ;
– tester la conception et l'implémentation des contrôles applicatifs ;
– tester les contrôles généraux informatiques pour les applications concernées.

Les travaux au cours de cette phase peuvent être réalisés par entretien et par analyse de la documentation existante ; ils permettent notamment d'établir une cartographie applicative du système d'information de l'établissement, afin d'identifier :

– les applications supportant les processus d'élaboration de l'information financière, y compris les applications bureautiques, ainsi que leurs caractéristiques techniques : progiciels/développements spécifiques ; date de mise en production/dernière montée de version ; infrastructure technique/système d'exploitation/base de données, etc. ;
– les principaux flux d'information en amont et en aval de ces applications : type de flux, nature des données, fréquence, etc.

Cette cartographie permettra d'identifier les applications clés (ainsi que leur environnement technique) supportant la production des états financiers pour lesquelles une analyse de l'environnement de contrôle interne et des contrôles généraux informatiques sera réalisée.

Pour se préparer

En s'appuyant sur la fiche 1 « Présentation du système d'information » ou les recueils déjà existants, l'établissement pourra s'assurer qu'il dispose des documents nécessaires à une description la plus complète possible de son système d'information (cartographies), de ses modes de fonctionnement (traitements existants, interfaces) et des grands principes de gouvernance du SIH. Le travail de cartographie peut être complexe, compte tenu du nombre d'applications et d'interfaces au sein du SIH, et doit ainsi être anticipé suffisamment à l'avance.

Étape 2 : revue de l'environnement de contrôle informatique et des contrôles généraux informatiques

À l'issue de l'étape de prise de connaissance du SIH, la revue de l'environnement de contrôle informatique et des contrôles généraux informatiques permet de réaliser une analyse plus approfondie du fonctionnement de la DSI, à travers l'analyse des contrôles généraux.

Les domaines présentés dans cette étape sont issus du référentiel COBIT (référentiel de gouvernance des systèmes d'information et de gestion des risques), qui constitue un cadre de contrôle, fondé sur un ensemble de bonnes pratiques, qui vise à aider les directions à gérer les risques (sécurité, fiabilité, conformité) et les investissements. La dernière version du référentiel COBIT (V5 au moment de la rédaction du présent document) a été conçue pour pouvoir s'intégrer à d'autres référentiels et standards.

La revue des contrôles généraux informatiques permet d'appréhender l'environnement de contrôle interne relatif à une application, ou à un ensemble d'applications, supportant les processus métiers et l'information comptable et financière. Les contrôles clés sont analysés pour les applications qui doivent garantir l'intégrité des données financières et pour l'infrastructure (système d'exploitation et base de données). Les contrôles clés portent sur les quatre principaux domaines suivants :

– l'accès aux programmes et aux données ;
– la gestion des changements (suivi des évolutions des composants du SIH, qu'ils soient applicatifs ou relatifs à l'infrastructure) ;
– la gestion des développements et des acquisitions de nouveaux systèmes ;
– la gestion de l'exploitation (suivi des traitements et tâches relatives au maintien en condition opérationnelle du SIH, y compris l'analyse du traitement et du suivi des incidents relevés et des problèmes),

ainsi que les domaines complémentaires suivants :

– la gestion des applications bureautiques ;
– le plan de reprise d'activité (PRA).

La revue des contrôles généraux informatiques peut permettre :

– d'identifier les axes d'amélioration de l'organisation informatique par rapport aux référentiels de bonnes pratiques (principalement le référentiel COBIT) ;
– d'appréhender le niveau de sécurité et de séparation des tâches au sein des applications et de l'organisation pour couvrir le risque de fraude ;
– d'appréhender les mécanismes en place concourant à assurer la continuité d'activité ;
– d'apprécier l'homogénéité des procédures de contrôle entre les différents environnements techniques audités ;
– d'apprécier la permanence des contrôles d'une année sur l'autre.

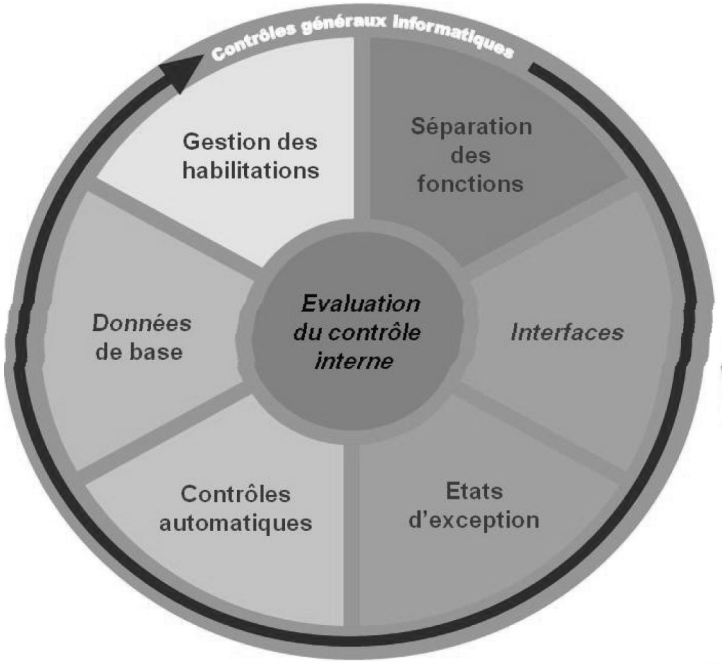
Pour se préparer

En s'appuyant sur les fiches pratiques 2 à 19, l'établissement pourra, dans un premier temps, recenser et rassembler les éléments de contrôle existants relatifs aux différents thèmes abordés.

En fonction du niveau de maturité de cette documentation et des exemples de bonnes pratiques décrits, l'établissement pourra approfondir les thématiques utiles et critiques et, plus largement, identifier le plan d'actions associés.

Étape 3 : revue ciblée de processus et tests des contrôles applicatifs

Les domaines présentés ci-dessous sont issus du référentiel COBIT.



L'amélioration du contrôle interne informatique au sein des processus et des applications qui les supportent repose sur une analyse des contrôles existants, qu'ils soient manuels ou automatisés. Elle permet notamment d'identifier, pour le processus concerné :

- les applications concourant à ce processus ;
- les interfaces existantes (flux entrants et sortants) ;
- les référentiels en place (données, traitements) ;
- les droits d'accès mis en œuvre et la séparation des fonctions ;
- les traitements et contrôles automatiques réalisés au sein des applications ;
- les contrôles portant sur les opérations permettant de fiabiliser l'information (notamment financière). Ces contrôles peuvent s'appuyer sur des états d'exception générés automatiquement par le système et permettant d'identifier les écarts vis-à-vis des règles de gestion (ex. : état des commandes non validées depuis plus de trente jours).

Cette analyse permet de mettre en évidence l'identification des risques potentiels, qui peuvent porter, par exemple, sur l'existence d'interfaces multiples, la gestion de profils utilisateurs inadaptés et qui pourraient nécessiter la mise en place de procédures particulières, de revue périodique, de contrôles supplémentaires (par exemple) afin de sécuriser le flux de traitement de l'information.

Pour se préparer

Dans le chapitre 2.3.2, un exemple de démarche est proposé. Elle implique fortement les acteurs des pôles, des services et de l'informatique et doit permettre une représentation des différents processus de l'établissement. Certains établissements peuvent déjà avoir engagé cette démarche de représentation au travers d'outils spécifiques de modélisation de processus. Il conviendra, sur ces représentations, d'y associer le contexte du SIH, les contrôles existants et leur nature (manuel ou automatisé) ou les instances existantes permettant de garantir la qualité des données présentes dans le système d'information.

1.2.4. Spécificités des établissements publics de santé

Dans le contexte des établissements de santé, la démarche d'auditabilité des systèmes d'information est impactée par :

- le cadre réglementaire ;
- la multiplication et la nature des interlocuteurs concernés au sein de l'établissement ;
- la confidentialité des données médicales ;
- une cartographie complexe des SIH et le rôle du DIM dans l'établissement :
  - les applications supportant les processus d'élaboration de l'information financière, y compris les applications bureautiques, ainsi que leurs caractéristiques techniques sont très hétérogènes et ne présentent généralement pas de réelle intégration ni d'unicité dans le référentiel de données et les traitements de l'information. De nombreuses applications de spécialités médicales sont présentes au sein des SIH, multiplient les nécessités d'interfaces avec le système de facturation et sont autant de points de contrôle à réaliser. Par nature, ces interfaces sont sources de risques, qu'ils soient relatifs aux traitements réalisés ou aux changements de versions des solutions ou plates-formes techniques impactées. Les bonnes pratiques, en termes de contrôles, seront d'autant plus importantes ;

– les processus spécifiques des établissements de santé, dont notamment le processus de recettes lié à l'activité de soins :
  – l'exhaustivité de la facturation des prestations repose sur la création d'un dossier patient à l'entrée du patient et sur la qualité de la documentation de ce dossier. La correcte valorisation de la prestation est liée à un codage précis du séjour. Le codage est complexe et il existe par conséquent des risques d'erreur et des risques de sous-cotation ou de surcotation ;
– des interfaces avec le comptable public et son système d'information HELIOS :
  – les flux budgétaires et comptables des établissements de santé publics sont interfacés avec le système d'information HELIOS. Le certificateur pourra notamment vérifier l'exactitude et l'exhaustivité des flux de données entre l'ordonnateur et le comptable public ;
  – le certificateur pourra étudier la revue des flux de données (sens, contenu, exhaustivité des données, déclencheurs) transitant par cette interface, notamment en cas d'évolution de version du SI des établissements ou suite au changement de protocole d'échange de données (adoption du protocole unique PES V2). Il conviendra de s'assurer, pour chaque évolution des solutions concernées, que les modifications engendrées, sur la structure des données du système ordonnateur ou leur paramétrage, soient correctement retranscrites dans l'interface et n'altèrent pas le contenu des données transmises au système du comptable ;
– des certifications tierces pouvant concourir à l'évaluation du niveau de contrôle de l'établissement par le certificateur :
  – la certification HAS des établissements de santé comprend deux critères de certification dédiés au système d'information (critères 5a et 5b), dont le respect concourt également à l'auditabilité du SI ;
  – les initiatives déjà engagées par certains établissements du type ISO (ou autres) ou la mise en œuvre de bonnes pratiques conformes aux référentiels COBIT ou ITIL, par exemple, contribueront à apprécier le niveau de maturité de l'établissement au regard de la qualité de sa gestion des services informatiques.

PARTIE 2
SE PRÉPARER À L'AUDIT DU SIH

Ce chapitre a pour objectif de décrire de façon opérationnelle les points d'attention relatifs au système d'information. Les points abordés constituent les aspects essentiels et les domaines sensibles susceptibles d'être investigués par le certificateur dans l'exDaans ce cas mission, ils n'ont pas vocation à être exhaustifs.

Pour l'ensemble des thèmes abordés dans ce chapitre, il conviendra, pour l'établissement inscrit dans une démarche de fiabilisation de comptes, de recenser la documentation disponible et d'évaluer l'adéquation des processus internes avec les bonnes pratiques.

Ce chapitre est complété par des fiches pratiques détaillées disponibles en partie 3 du présent document et permettant de guider l'établissement dans son évaluation du niveau de contrôle en place vis-à-vis des thèmes abordés. Les bonnes pratiques données en exemple dans ce document sont principalement extraites du référentiel COBIT.

Il convient également de préciser que si les thèmes abordés relèvent essentiellement du système d'information, objet du présent guide, leur périmètre d'application pourra s'étendre, au-delà d'une direction des systèmes d'information (DSI), aux processus supportés par le SI et aux acteurs métiers concernés.

Les développements sont structurés en trois parties :
– présentation succincte du thème abordé ;
– éléments utiles à la démarche d'auditabilité du SIH, présentant les points clés utiles à la compréhension et à la documentation du thème abordé ;
– le tableau ci-dessous précisant :

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Exemples de situations ou constats rencontrés dans diverses organisations et pouvant présenter un niveau de risque qu'il convient de prendre en considération par l'établissement.	Exemples de bonnes pratiques, dont la mise en œuvre pourra être modulée en fonction de chaque établissement, de son organisation, de la capacité des outils techniques en place et des ressources existantes.	Liste indicative.

2.1. *Étape 1 : préparer la prise de connaissance du système d'information*

Cette étape consiste à préparer la prise de connaissance, par le certificateur, du système d'information de l'établissement dans son ensemble dans le but d'évaluer son niveau de complexité afin notamment de déterminer son incidence sur la production des informations financières et comptables.

La préparation de la prise de connaissance du système d'information consiste à collecter des informations sur les applications et les systèmes informatiques, ainsi que les processus et l'organisation informatiques de l'établissement. Les principaux domaines à prendre en compte sont :

– l'organisation de la fonction SI dans l'établissement ;
– la stratégie informatique matérialisée par le schéma directeur ;
– la documentation générale du SI ;
– la politique de sécurité ;
– les méthodologies mises en œuvre dans la gestion et le suivi des projets ;
– plus largement, les processus d'évaluation des risques au sein du SI et les processus mis en œuvre pour la correction des déficiences.

2.1.1. Organisation de la fonction SI dans l'établissement

La préparation de la prise de connaissance de la fonction informatique dans l'établissement a pour objectif d'aider le certificateur à mesurer :
– son adéquation aux besoins et aux enjeux de l'établissement ;
– les procédures existantes au sein de la DSI ;
– les principes de séparation des tâches entre, par exemple, les fonctions dites d'exploitation et celles dites de développement ;
– le niveau de dépendance de l'établissement vis-à-vis de prestataires externes ;
– les procédures d'évaluation des risques et de correction des déficiences.

Éléments utiles à la démarche d'auditabilité du SIH

Dans le cadre de cette analyse, seront sollicités le responsable informatique et les responsables de la direction financière. La documentation existante, sa précision et sa mise à jour constituent des pièces nécessaires à la démarche. Les informations et documents suivants constituent des éléments clés de compréhension de l'organisation de la fonction SI dans l'établissement :
– la définition et le périmètre de la DSI au sein de l'établissement ainsi que sa représentation dans les instances de direction ;
– l'organigramme détaillé de la DSI, avec la mention des effectifs et de leur localisation ;
– l'organisation de la DSI, les responsabilités des différents acteurs sur les différents sujets que sont la production (exploitation), les études, et la sécurité informatique ;
– les principes de séparation des fonctions et des tâches relatives aux environnements de production et d'études ;
– la définition du poste de responsable de la sécurité des systèmes d'information (RSSI) et son positionnement hiérarchique ;
– le niveau d'externalisation du SI et les contrats de service avec les prestataires clés (TMA, hébergement, exploitation, *hotline*...) ;
– les audits informatiques réalisés en interne, par des tiers, les recommandations formulées, les plans d'actions initiés et leur suivi.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Absence de séparation des fonctions, qui peut impliquer un plus grand risque de fraude (développement et mise en production d'une application ou interface sans contrôle). Absence de maîtrise du système d'information (sous-traitants non encadrés, manque de compétences internes sur certains thèmes), qui peut impliquer un risque sur la fiabilité des applications. Incapacité des équipes informatiques à maintenir une application ou à investiguer ses modes de fonctionnement, qui peut entraîner un risque d'erreur dans les données financières. Dépendance vis-à-vis de personnes clés sur des applications ou des infrastructures, qui peut entraîner un risque en cas de départ de la personne, quelle qu'en soit la raison, sur la capacité à assurer les évolutions sur cette application/infrastructure ou sa maintenance.	Les fonctions, notamment études et production, sont gérées par des services indépendants. La fonction de RSSI est définie dans l'établissement (indépendamment des missions de la DSI). Les fonctions externalisées sont sous contrôle de la DSI et répondent à des bonnes pratiques équivalentes à celles définies en interne. L'organisation est en phase avec les besoins métiers et répond aux attentes de ces derniers (prise en compte, analyse du besoin, validation des livrables...). La DSI a mis en place des procédures décrivant ses modes de fonctionnement, les modalités d'évaluation régulière des risques pouvant porter sur le SI. Un processus d'évaluation des risques informatiques, de traitement des anomalies constatées et des améliorations engagées est mis en œuvre et tracé (processus de correction d'un problème, par exemple). Un plan de formation pour les équipes de la DSI existe, en cohérence avec la stratégie définie et les outils (applications et infrastructures en place).	Formalisation d'un organigramme à jour du service informatique de l'établissement précisant l'ensemble des effectifs concernés. Formalisation des fiches de poste relatives à l'organisation mise en place. Respect des principes de séparation des fonctions au sein de la DSI entre études et exploitation (dans le cas contraire, documenter et justifier les exceptions). Formalisation de la description des modes de fonctionnement de la DSI. Existence d'un RSSI dont le rattachement hiérarchique est en lien avec la direction générale. Mise en œuvre d'un plan de formation répondant aux environnements et solutions en place au sein de l'établissement. Recensement des contrats d'externalisation existants, respect des principes définis par la DSI et activités des prestataires sous contrôle de l'établissement. Définition d'une analyse des risques et d'un processus de traitement des anomalies constatées selon un diagramme des responsabilités définies (RACI). Identification du niveau de dépendance vis-à-vis des prestataires ainsi que des clauses de réversibilité. Vérifier si les compétences en place répondent aux exigences techniques du système et des métiers et permettent de limiter le risque de dépendance.
Fiche pratique liée.	Fiche 1. – Présentation du système d'information.	

2.1.2. Gouvernance des SI

Dans ce paragraphe sont traités les aspects liés à la gouvernance du système d'information, l'objectif étant, pour l'établissement, de démontrer que la direction générale dispose d'une vision claire du SI en place, de ses faiblesses, des risques encourus et des évolutions attendues qui doivent être en accord avec la stratégie globale de l'établissement.

L'établissement devra prioriser les travaux en fonction de son contexte et de ses risques.

Ainsi, les deux situations extrêmes présentées en exemple ci-dessous illustrent les impacts possibles sur la démarche du certificateur et sur son évaluation du niveau de risque plus ou moins élevé :

– dans le premier cas, la DSI dispose d'un espace d'échange avec la direction générale et les acteurs du métier à intervalles réguliers. Elle participe activement, par l'amélioration de la performance de son SI, à accompagner les gains d'efficience souhaités par la direction générale. En ce sens, elle partage son schéma directeur, qui est suivi et revu chaque année. Dans ce cas, le niveau de risque sera relativement faible et la mise en œuvre de contrôles pourra être allégée ;
– dans le second cas, par manque de ressources, la DSI est focalisée sur le support aux utilisateurs, la mise en place des solutions qui lui sont proposées par les acteurs du métier. Un schéma directeur existe, mais il n'est pas actualisé chaque année. Dans ce cas, la direction générale ne dispose pas d'une vision exhaustive du SI, de ses évolutions et le certificateur pourra estimer un niveau de risque plus important, qui exigera, dans son approche, une prise en compte plus importante des contrôles.

Éléments utiles à la démarche d'auditabilité du SIH

L'établissement pourra préparer la documentation permettant au certificateur d'identifier la prise en compte des besoins métiers et l'implication des services ou unités concernés dans la définition de la stratégie informatique. Les informations et documents suivants constituent des éléments clés de compréhension de la gouvernance des SI :

– le niveau d'informatisation des services et leur perception des moyens mis à leur disposition ;
– les modalités de définition du schéma directeur et son processus d'élaboration et de validation par la direction générale et les acteurs métiers ;
– la déclinaison dans le schéma directeur des enjeux stratégiques de l'établissement (amélioration de la prise en charge du patient et de la traçabilité des actes, mise en place d'un GCS...) ;
– l'identification et partage avec la direction générale des risques qui peuvent porter sur le SI et les mesures prises pour les réduire ;
– les processus mis en œuvre pour assurer la satisfaction des utilisateurs, les démarches engagées par la DSI de type ITIL, ISO ou autres ;
– les indicateurs de pilotage mis en œuvre pour s'assurer, par exemple, du suivi budgétaire, de la réactivité du service, de la satisfaction des utilisateurs, de la disponibilité du SI ;
– la capacité du SI à évoluer, à s'adapter à de nouvelles contraintes.

Pour compléter l'analyse, il sera utile de produire les documents suivants :

– le schéma directeur du système d'information et de la sécurité informatique et les révisions qu'il a pu subir ;
– la formalisation du budget informatique et son évolution ;
– les méthodologies de gestion de projet retenues, et notamment la prise en compte des acteurs métiers dans les évolutions les concernant.

L'établissement pourra également se préparer à ce que le certificateur s'entretienne avec un représentant de la direction générale afin de comprendre la stratégie, les enjeux de l'établissement, le niveau d'implication et de compréhension de la direction générale sur le SI. Cet échange pourra permettre à l'établissement :

– de justifier que les orientations stratégiques sont déclinées dans le schéma directeur ;
– d'évaluer les difficultés auxquelles la DSI peut faire face (ressources, compétences...) ;
– de justifier du niveau de contrôle assuré par la direction générale sur le pilotage global du SI.

Ces échanges entre l'établissement et le certificateur pourront être complétés avec d'autres directions (DAF, DIM, services de soins...) afin d'évaluer leur connaissance des projets en cours les concernant et leur implication dans ces derniers, ainsi que leur appréciation du service rendu et de la disponibilité générale du SI.

Enfin, l'établissement pourra préparer la prise de connaissance du certificateur, en recensant :

– les faits majeurs ayant pu altérer le SI ou les services (incidents majeurs : rupture dans la continuité du service/fraudes/actes malveillants) ;
– la réponse faite aux différentes situations évoquées et les plans d'actions mis en œuvre ;
– le budget informatique et son pilotage ;
– le suivi des indicateurs mis en œuvre et partagés avec les services ou la direction générale.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Absence de stratégie informatique partagée et formalisée. Absence de mise à jour d'un schéma directeur existant. Absence de visibilité de la direction générale sur d'éventuels chantiers importants à mener et de leur impact sur les services. Inadéquation entre les moyens mis en œuvre par la DSI et les attentes métiers. Absence de prise en compte par les services du cadre global de cohérence défini par la DSI (exemple : choix d'application informatique sans implication de la DSI).	La stratégie informatique existe et est formalisée. Les besoins utilisateurs sont pris en compte dans les différents projets. Des représentants des utilisateurs appuient la DSI lors de la mise en œuvre des projets. Le schéma directeur existe et décline la stratégie SI à partir de la stratégie de l'établissement et des besoins des services. Le schéma directeur est mis à jour régulièrement en accord avec la direction générale, qui a une vision claire des enjeux du SI et de ses apports sur les processus métiers. L'activité de la DSI est pilotée dans ses différentes dimensions (taux de service, disponibilité, satisfaction des utilisateurs, budgets...). Les risques sont mesurés, analysés et des actions sont mises en œuvre pour les réduire (dépendance, malveillance, sécurité).	Existence d'une stratégie informatique (formalisée ou non) partagée avec la direction et les services. Existence d'un schéma directeur mis à jour *a minima* une fois par an. Identification des risques potentiels sur le SI, au regard de la stratégie et de ce schéma directeur, et d'un plan d'action (décliné en objectifs, moyens nécessaires et planning) visant à les réduire. Traçabilité des incidents majeurs et mise en œuvre d'un traitement particulier. Prise en compte de l'ensemble des projets identifiés par les services et impactant le SI au travers de réunions périodiques avec les acteurs concernés. Identification et diffusion d'indicateurs auprès des acteurs concernés (direction et/ou services), par exemple : – disponibilité du SI ; – délai moyen de traitement des demandes ; – budget ; – taux de satisfaction des utilisateurs sur le suivi des projets, les outils en place.
Fiche pratique liée.	Fiche 1. – Présentation du système d'information.	

2.1.3. Documentation générale du SI

L'établissement pourra préparer la prise de connaissance de l'environnement informatique en documentant la description du système d'information.

La description du système d'information de l'établissement consiste à formaliser la cartographie des applications, à apprécier le degré de complexité du système d'information et identifier les processus à analyser, utiles aux objectifs de l'audit.

Éléments utiles à la démarche d'auditabilité du SIH

Dans cette étape, la prise en compte de la cartographie générale du système d'information constituera un élément clé de la documentation. Elle permet en outre de mettre en évidence les risques potentiels liés à cette architecture. L'établissement de la cartographie du système d'information nécessite l'identification des principales applications et interfaces.

Par « identification des principales applications informatiques », il est entendu un recensement de l'ensemble des applications de l'établissement, avec les éléments caractéristiques suivants :

– le type (progiciel avec indication de l'éditeur/développement spécifique) ;
– l'éditeur ou le prestataire ;
– le besoin fonctionnel couvert ;
– la date de mise en place (date de dernière mise à jour ou évolution) ;
– l'environnement technique qui supporte l'application : Unix, Windows, AS400, web... ;
– le mode de traitement (différé ou temps réel) ;
– la date de la dernière modification ;
– la nature des sorties ;
– une estimation du volume traité (nombre de séjours, nombre d'actes, utilisateurs concernés, par exemple).

Par « identification des principales interfaces », il est entendu un recensement des principaux liens qui existent entre les différentes applications. Ces liens peuvent être automatiques, semi-automatiques ou manuels. Pour chaque interface identifiée, il est nécessaire de préciser :

– le type de flux : automatique, semi-automatique, manuel ;
– les applications (source et destination) ;
– la nature des flux : actes, stocks, séjours, patients... ;
– la périodicité : quotidienne, hebdomadaire, mensuelle... ;
– l'origine et la destination des données ;
– les contrôles existants.

Les informations complémentaires nécessaires pourront être recueillies par le certificateur par voie d'entretiens avec le responsable informatique.

La représentation graphique des différentes applications et des liens existant entre elles constitue la cartographie générale des applications. Elle permet de visualiser de façon synthétique un système d'information complexe et sert en outre de support de communication pluridisciplinaire (culture comptable, culture informatique) dans l'identification des risques potentiels. La cartographie des applications peut être complétée par une description de l'infrastructure technique (matériels et réseaux).

La documentation du SI permet de mieux évaluer le niveau de fiabilité du SI et les risques potentiels.

Parmi les situations présentant un risque moindre, les suivantes peuvent être notées :

– un système intégré avec un partage des référentiels ;
– l'existence de rapports d'anomalies ou de contrôles intégrés dans les systèmes.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Système hétérogène avec absence de partage des référentiels. Multiplication des interfaces, qui sont autant de zones de risques à couvrir. Documentation simpliste se limitant aux applications, sans description précise des flux de données échangées, de leur fréquence. Multiplication de développements spécifiques.	La cartographie des applications du SIH est documentée et à jour. Les principales applications ou fichiers bureautiques impactant les états financiers sont identifiés. Les principales interfaces entre ces systèmes sont décrites de façonexhaustive (nature, données, périodicité). Les applications, qu'elles soient progicielles ou spécifiques, sont documentées. Cette documentation est maintenue à jour des dernières modifications ou évolutions opérées. Les principaux référentiels (du type patients, séjours, agents, marchés) sont décrits ainsi que leurs principes d'alimentation et de modification.	La fiche nº 1 « Présentation du système d'information » fournit un exemple de cartographie ainsi que des tableaux permettant le recensement des applications et interfaces. La constitution de cette documentation fournit un premier élément significatif de compréhension du SI. D'autres initiatives, en fonction des établissements, peuvent être déjà initiées, notamment sur la formalisation des processus opérationnels.
Fiche pratique liée.	Fiche 1. – Présentation du système d'information.	

2.1.4. Politique de sécurité

La politique de sécurité des systèmes d'information (PSSI) doit constituer le document de référence en matière de sécurité de systèmes d'information de l'établissement. Elle en est un élément fondateur, définissant les objectifs à atteindre et les moyens accordés pour y parvenir. La démarche de sécurité des systèmes d'information est basée sur une analyse des risques en matière de sécurité des systèmes d'information.

L'objectif de cette partie n'est pas de revenir sur les enjeux de la sécurité des SI dans le secteur de la santé ni sur le cadre réglementaire qui peut la régir, mais de souligner les principaux points en lien avec la démarche du certificateur et les points d'attention qu'il pourra identifier.

Éléments utiles à la démarche d'auditabilité du SIH

Pour se préparer, l'établissement pourra collecter la documentation justifiant qu'une politique de sécurité a été définie et qu'elle a été communiquée aux responsables de l'établissement.

Les informations et documents suivants constituent des éléments clés de compréhension de la politique de sécurité des SI :

– l'importance de la sécurité dans l'organisation, et plus particulièrement dans le milieu médical ;
– la communication et l'acceptation de la politique de sécurité ;
– l'accès physique aux ressources informatiques ;
– les responsabilités du collaborateur et du prestataire ;
– la gestion des accès (attribution, revue et révocation des droits d'accès) ;
– l'accès aux applications, bases de données, systèmes d'exploitation ;
– la gestion des mots de passe ;
– le *monitoring* du réseau ;
– l'accès à distance ;
– la protection antivirus supervisée par une console centrale ;
– la revue et les modalités de mise en œuvre des correctifs de sécurité des éditeurs ;
– la revue des incidents liés à la sécurité.

L'établissement pourra démontrer que cette politique a été définie en lien avec la direction générale, qu'elle a fait l'objet d'un plan d'action et d'une revue régulière par un acteur (RSSI) indépendant de la DSI. L'établissement collecte la documentation justifiant que des actions de sensibilisation régulières sont menées à destination des utilisateurs et prestataires.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Politique de sécurité définie sans concertation avec les différentes instances de l'établissement. Absence de processus de diffusion, de validation de la politique de sécurité auprès des utilisateurs. Absence d'actions de sensibilisation récurrente des utilisateurs aux problématiques de la sécurité. Absence de prise en compte des prestataires dans la politique de sécurité.	La politique de sécurité est définie en lien avec la direction générale et fait l'objet d'un plan d'actions concerté et d'un partage des responsabilités clairement identifié. Après validation par les différents acteurs de la sécurité de l'information, la PSSI est déclinée dans les procédures opérationnelles et la charte est communiquée à l'ensemble des acteurs du système d'information concernés (charte utilisateurs, charte spécifique à destination des prestataires, etc.). La PSSI constitue un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir. La politique de sécurité traite *a minima* les sujets suivants : – sécurité physique et sécurité de l'environnement ; – exploitation informatique et gestion des réseaux ; – contrôle d'accès logique ; – acquisition, développement et maintenance des applications et systèmes ; – gestion de la continuité ; – respect de la réglementation interne et externe.	Recensement des documents existants. Définition de la politique de sécurité en concertation avec la direction et validation par cette dernière de la politique. Mise en œuvre des principes de séparation des fonctions entre le RSSI et la DSI et documentation. Formalisation d'une procédure concernant la prise de connaissance de la charte d'utilisation du SI par tout nouvel arrivant. Diffusion de la charte d'utilisation du SI (affichage, intranet, etc.) et communication régulière. Formalisation d'une charte de sécurité à destination des intervenants externes (prestataires) et insertion de cette dernière dans les appels d'offres concernés et les contrats de services signés.
Fiche pratique liée.	Fiche 1. – Présentation du système d'information.	

2.1.5. Gestion et suivi des projets

Les projets informatiques peuvent avoir un impact significatif sur l'organisation et le fonctionnement d'un établissement. Selon l'AFNOR, « un projet est une démarche spécifique qui permet de structurer méthodiquement et progressivement une réalité à venir. Un projet est défini et mis en œuvre pour élaborer une réponse au besoin d'un utilisateur, d'un client ou d'une clientèle, et il implique un objectif et des actions à entreprendre avec des ressources données ».

Un projet se doit d'être :
– limité dans le temps : un projet est mené par rapport à un calendrier ;
– unique : s'il existe de nombreux projets analogues ou similaires, les projets ne sont pas identiques, en raison des évolutions technologiques et des spécificités organisationnelles de l'établissement ;
– pluridisciplinaire : la conduite de projet requiert des compétences techniques, administratives, financières, sociales et juridiques.

Les projets structurants qui auraient pu être menés sur l'année en cours ou passée (mise en place d'un dossier patient informatisé [DPI], remplacement de la gestion administrative des patients, etc.) peuvent avoir un impact important sur l'auditabilité du SI et sur le contrôle interne des SI de façon plus générale.

Éléments utiles à la démarche d'auditabilité du SIH

Les informations et documents suivants constituent des éléments clés de compréhension de la gestion et du suivi des projets :
– le cadrage du projet, qui doit intégrer le volet stratégique, les besoins des utilisateurs, l'analyse de l'existant (logiciel, moyens, infrastructure...) ;
– la prise en compte du contrôle interne et de la sécurité (mots de passe, profils, piste d'audit...) ;
– les mesures prises pour assurer l'intégrité des traitements, la disponibilité de l'application ;
– la pertinence des jeux d'essais au regard de l'analyse des phases de test et de déploiement ;
– les dispositifs de gestion de l'exploitation de la solution mise en place ;
– les domaines fondamentaux de la conduite de projet et de la conduite du changement.

Dans le cadre d'opérations de migration, il sera par ailleurs important de s'assurer que les domaines suivants sont correctement documentés et tracés :
– périmètre des données à reprendre ;

– opérations de nettoyage des données ;
– conservation des données historiques ;
– préparation des tests ;
– opération de conversion de données et traçabilité des conversions ;
– préparation de la migration ;
– validation des opérations de bascule et de reprise des données ;
– plan de retour arrière en cas de difficultés majeures.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Absence de cahier des charges et documentation insuffisante. Absence de motivation des parties prenantes au projet (manque de soutien de la direction, manque de compétence de la maîtrise d'œuvre, manque d'implication des utilisateurs aux différentes phases du projet, en particulier à la phase de conception). Faiblesses dans la gestion de projet, principalement la planification des travaux, la gestion des ressources, la communication, les compétences... Délaissement des questions relatives à l'organisation et au contrôle interne, au profit des aspects techniques (la problématique du contrôle interne est souvent traitée *a posteriori*, ce qui implique une période de transition pendant laquelle le niveau de contrôle est plus faible : les états de gestion et les procédures de contrôle sont souvent modifiés avec la mise en place d'un nouveau système d'information).	L'établissement adopte une méthodologie standard de gestion de projet. Il existe une description des enjeux du projet et de son périmètre. Une organisation projet adéquate est mise en place. Un planning détaillé a été défini et est régulièrement mis à jour. Des indicateurs pertinents de suivi sont produits. Sur les principes de migration et de suivi des données, il pourra être porté une attention particulière sur les points suivants : – identification et validation de l'ensemble des données nécessaires à la migration par les responsables métier ; – qualité du processus de nettoyage des données concourant à la cohérence et la pertinence des données migrées ; – modalités de conservations des données historiques ; – modalités de reprise des données et des tests ; – modalités de conversion des données migrées ; – exécution de la conversion de données. – mise en œuvre d'environnements distincts pour les différentes phases du projet (tests, recette, production) ; – correction de l'ensemble des anomalies bloquantes à l'issue de la phase de recette ; – validation de la phase de recette par les responsables appropriés ; – existence d'un plan de retour arrière en cas d'anomalie majeure lors de la mise en production ; – existence d'une validation formelle métier accordant un feu vert pour la migration ; – exactitude et exhaustivité des données reprises dans le nouveau système ; – qualité des données migrées dans le nouveau système ; – adéquation des formations dispensées avec le niveau d'utilisateurs et le périmètre fonctionnel ; – mise à disposition des utilisateurs de dispositifs de support en phase de transition ; – prise en compte et traitement des anomalies rencontrées après le démarrage. Sur le volet du contrôle interne : – étude de la gestion des habilitations mise en place suite à la migration ; – réalisation d'un reporting adapté et fiabilité/opérationnalité des états de contrôle en place avant la migration.	Identification des différentes typologies de projets menés (par exemple : acquisition d'une nouvelle solution, évolution/migration). Pour chaque typologie, définition de principes de gestion de projet : gouvernance, planning, phases de tests, mise en production, principes de suivi et de formalisation... Classement des projets en cours impactant le SI selon les typologies retenues et mise en œuvre des principes de gestion de projet définis. Au regard des bonnes pratiques, identification des éventuels écarts et définition d'un plan d'harmonisation des modes de fonctionnement. Pour les projets en lien avec les principales applications identifiées, documentation et traçabilité (y compris conservation) des actions réalisées (par exemple : dans les phases de reprise de données, transcodification...).
Fiche pratique liée.	Fiche 1. – Présentation du système d'information.	

2.2. *Étape 2 : préparer la revue de l'environnement de contrôle et des contrôles généraux informatiques*

Les contrôles généraux comprennent tous les contrôles de l'environnement informatique nécessaire au fonctionnement des applications, par exemple : la gestion de l'exploitation, la sécurité des accès, le développement et la maintenance des systèmes et des applications ou la gestion des changements. La maîtrise de ces différentes briques ou évolutions du système d'information doit apporter au contrôle interne un socle fiable sur lequel il pourra s'appuyer.

La priorité pourra être donnée aux applications jugées critiques, ce qui s'entend dans le cadre de l'auditabilité des SI par les applications supportant les principaux processus du cycle comptable (recettes, personnel, immobilisations, achats d'exploitation, endettement long terme et trésorerie court terme) et ayant un impact sur les états financiers, par exemple : GAM, GEF, GRH, pharmacie et PMSI.

Sur le volet des contrôles généraux informatiques, les points de vigilance porteront essentiellement sur les thèmes suivants :

– la gestion de la sécurité ;
– le développement et l'acquisition de solutions informatiques ;
– la gestion de l'exploitation ;
– la gestion des sauvegardes et la continuité d'activité.

2.2.1. Accès aux programmes et aux données

La gestion de la sécurité se traduit principalement par l'évaluation de la sécurité, qui permet de contrôler les risques d'accès aux données par des personnes non autorisées (internes ou externes), ainsi que les risques d'altération des données (notamment par des virus) ou d'actes malveillants. L'étude de la sécurité logique a pour objectif de vérifier que l'établissement a mis en place un dispositif adapté à la prévention de ces risques.

Éléments utiles à la démarche d'auditabilité du SIH

La politique de sécurité logique mise en place par l'établissement doit être formalisée, et détaille notamment les modalités et procédures mises en œuvre sur les points suivants :

– antivirus : le fichier de signatures est mis à jour régulièrement et supervisé ;
– des dispositifs de pare-feu existent ;
– des actions de sensibilisation aux pratiques relatives à l'utilisation de la messagerie et d'Internet sont réalisées ;
– des règles sont définies sur l'utilisation des supports physiques par les utilisateurs du SI pour échanger les données (disques externes, clés USB, graveur).

Concernant l'accès aux programmes et aux données, la gestion des habilitations revêt une importance majeure. Elle a pour objectif de s'assurer de la définition de profils utilisateurs en adéquation avec les fonctions occupées. Ces points seront particulièrement importants à préparer, tout comme la gestion des mots de passe et l'authentification au SIH.

Il convient de distinguer les différents niveaux d'accès aux composants informatiques :

– l'accès au SIH : mot de passe de connexion système ;
– l'accès aux applications identifiées comme critiques ;
– l'accès aux bases de données supportant ces applications ;
– ainsi que sur les typologies d'accès comme « utilisateurs », « administrateurs » ou comptes à pouvoir et les comptes génériques.

Ces travaux préparatoires permettront à l'établissement de mieux appréhender les contrôles réalisés par le certificateur relatifs à la qualité de la politique de sécurité logique. Ils pourront notamment permettre la mise en évidence d'une séparation de fonctions insuffisante et de comprendre son incidence sur le contrôle interne au sein du(des) processus concerné(s). L'établissement pourra identifier les risques de fraude et mettre en place des contrôles compensatoires permettant de limiter ces risques.

Une visite physique de la « salle informatique » peut également être réalisée afin de s'assurer que les dispositifs existant en matière de sécurité physique des infrastructures sont opérationnels et que les règles définies sont respectées et suivies d'actions, le cas échéant.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Malgré l'existence d'une politique de sécurité et d'une charte, pas de communication aux nouveaux arrivants ni mise en place d'actions de rappel ou de sensibilisation (des utilisateurs non sensibilisés à la sécurité logique pourraient, par exemple, communiquer leur mot de passe à des collègues ou utiliser des supports externes contenant des virus, mettant ainsi en zone de risque le SIH). Droits attribués erronés, en contradiction avec les principes de séparation des tâches (certains profils peuvent rester actifs alors que les personnes sont parties de l'établissement. Une utilisation malveillante de leurs droits pourrait être faite sans traçabilité possible). Certains utilisateurs disposent de droits étendus à des fonctions dont ils n'ont pas l'usage dans le cadre de leur fonction. Utilisation de profils génériques par plusieurs utilisateurs (la traçabilité des opérations réalisées par un utilisateur ainsi désigné n'est pas assurée). Utilisation de mots de passe génériques ou simples (login : Admin, mdp : Admin) ou mot de passe facilement accessible, y compris pour certains comptes utilisateurs ayant des droits étendus (il pourrait en résulter la possibilité d'acte malveillant par intrusion sur le SIH de l'établissement).	Chaque utilisateur dispose d'un compte nominatif avec les droits nécessaires à l'exercice de ses fonctions. Les autorisations, modifications ou révocations des droits font l'objet d'une procédure et sont revues régulièrement avec les directions métiers. Un travail conjoint est réalisé par la DSI : – avec les directions métiers, pour identifier les profils utilisateurs types, en accord avec une matrice de séparation des tâches définie par le contrôle interne ; – avec la DRH, afin de s'assurer qu'un contrôle régulier puisse être fait entre les droits déclarés sur le SIH et les effectifs présents au sein de l'établissement. Les habilitations sont régulièrement revues afin qu'aucun compte non utilisé ne reste actif dans le système. Le système et les applications proposent, dans la limite des contraintes techniques des solutions, des règles de gestion conformes aux meilleures pratiques, énoncées notamment par la CNIL et la HAS. Les comptes génériques (secrétariat, admin, stagiaire...) sont limités, justifiés et font l'objet d'une revue régulière (*a minima* annuelle). Les comptes administrateurs sont limités à un nombre restreint d'agents et sont créés sur la base d'autorisations décrites dans des procédures formalisées, une revue régulière de l'activité de ces comptes est effectuée par les administrateurs. Concernant la sécurité physique : – des dispositifs de contrôle d'accès sont utilisés pour restreindre l'accès physique aux installations hébergeant les applications clés ; – les autorisations, modifications ou révocations des droits font l'objet d'une procédure et sont revues régulièrement ; – les accès de l'extérieur sont sécurisés (fenêtres protégées) ; – la salle est équipée de dispositifs de détection d'incendie, d'extinction d'incendie, d'une climatisation et d'un système anti-intrusion.	Diffusion de la politique de sécurité par les agents et nouveaux arrivants et conduite d'actions de sensibilisation. Élaboration d'un processus de création, modification et suppression des droits d'accès s'appuyant sur les règles métiers définies par l'établissement et les autorités de tutelle (ce processus peut s'appuyer sur le contrôle interne et sur une matrice de séparation des tâches). Définition de profils dans les applications du SIH (si les applications ne le permettent pas, envisager les contrôles compensatoires pour pallier les défaillances du système). Pour les applications dites critiques, extraction de la liste des comptes existants et classement selon les principes « utilisateurs nommés, administrateurs, comptes génériques » : – contrôle, avec la liste des effectifs présents, que les comptes sont justifiés ; – contrôle des comptes administrateurs pour s'assurer qu'ils sont justifiés ; – investigation des comptes génériques, dénombrement et clarification des droits attribués, pour s'assurer qu'ils sont limités et justifiés. Respect des bonnes pratiques en termes de gestion des mots de passe ainsi que celles relatives à la sécurité physique des moyens informatiques. Formalisation des procédures et revues. Pour ces étapes, au-delà des contrôles qui sont certainement déjà réalisés dans les établissements, une importance toute particulière est à porter à la traçabilité des contrôles, des revues qui sont réalisées et des actions correctives qui sont mises en œuvre. Par traçabilité des contrôles, on entend la nécessité de formaliser et de conserver les contrôles réalisés, ces derniers pouvant être demandés par le certificateur. Les plans d'action définis par l'établissement pourront être formalisés et communiqués au certificateur.
Fiches pratiques liées.	Fiche 2. – Mécanismes d'identification. Fiche 3. – Comptes génériques. Fiche 4. – Configuration des mots de passe – Applications. Fiche 5. – Accès administrateur. Fiche 6. – Gestion des droits d'accès. Fiche 7. – Matrice de séparation des tâches. Fiche 8. – Gestion des accès aux applications, bases de données et systèmes d'exploitation – Création, modification et suppression des accès. Fiche 9. – Revue périodique des accès aux applications. Fiche 10. – Restriction des accès physiques.	

2.2.2. Gestion des changements

Un changement consiste à modifier, créer ou supprimer un des composants de l'infrastructure du système d'information (logiciel, application, équipement, matériel, configuration, documentation, procédure, etc.) donc d'un ou plusieurs éléments de configuration.

Les changements peuvent avoir des origines diverses et comme élément déclencheur, par exemple :

– dysfonctionnement du système existant ;
– utilisateurs insatisfaits ;
– montée de version de certains composants de l'infrastructure ;
– évolution réglementaire.

La gestion des changements constitue donc un processus central qui permet d'évaluer la façon dont les changements sont opérés, tracés et historisés et s'appuie sur les principales composantes suivantes :

– le cycle de décision ;
– l'implémentation du changement ;
– les procédures d'urgence.

Avant toute réalisation, un changement devra être catégorisé par un comité de gestion des changements, composé de représentants des fonctions informatiques et du personnel métier (personnel de soins, technique, administratif...), en fonction des applicatifs impactés par la demande de changement. Le critère principal de sélection d'une catégorie est les ressources requises pour implémenter le changement.

Selon le référentiel ITIL, les changements peuvent ainsi être répartis en deux catégories principales :

– les changements mineurs : pour ces changements, l'impact sur le système d'information est négligeable et celui-ci peut généralement être délégué au support informatique (exemple : changement d'un mot de passe) ;
– les changements significatifs : ces changements impactent de façon plus importante le système d'information et nécessitent la plupart du temps la modification du code informatique des applicatifs. Ces changements significatifs pourront également être répartis en deux sous-catégories : les changements non urgents et les changements urgents. L'établissement pourra adapter sa gestion des changements afin de permettre une mise en production accélérée et contrôlée des changements urgents.

Éléments utiles à la démarche d'auditabilité du SIH

Concernant cette gestion des changements, il s'agira d'avoir défini une politique de gestion des changements, communiquée aux agents (et prestataires) adéquats. La politique de gestion des changements aborde les thèmes tels que :

– l'initiation de la demande de changement ;
– la validation par la DSI des demandes de changement ;
– la mise en œuvre du changement et les contrôles réalisés.

Les risques inhérents à tout changement peuvent avoir des impacts sur la production des éléments financiers qui doivent être pris en compte.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Demandes de changements non formalisées (le besoin n'est pas clairement exprimé, ni formalisé par les directions métier). Évolutions faites sur le SI non documentées. Manque d'information : les utilisateurs ne sont pas tenus informés des changements réalisés, ni formés sur les éventuelles nouveautés mises en œuvre (le risque induit peut être une mauvaise utilisation des solutions en place. Les impacts éventuels sur l'organisation peuvent induire une modification des rôles et responsabilités au sein d'un processus qui ne serait pas tracée). Développements ou modifications réalisés et mis en production sans phase de test par le métier ni autorisation formelle (les principaux risques pourraient dans ce cas être les suivants : – dysfonctionnements constatés sur une application jugée critique, par défaut de tests et risque sur la continuité d'activité ; – risque d'acte malveillant, par absence d'un processus maîtrisé et d'une séparation entre le développement et l'exploitation qui met en production ; – absence de processus de suivi des demandes et risque de mécontentement des utilisateurs qui pourraient détourner certaines fonctionnalités ou briques du SIH en dehors de tout contrôle).	La politique de gestion des changements est formalisée, validée par la direction et aborde les domaines évoqués ci-après : – initiation d'une demande formelle de changement ; – validation par la direction des demandes de changement ; – réalisation de tests unitaires et systèmes dans un environnement de test ; – réalisation d'une recette utilisateur et validation formelle ; – mise en production en environnement de production. La communication sur la politique de changement est assurée auprès des utilisateurs afin de limiter les initiatives isolées et qui ne rentreraient pas sous le contrôle de l'établissement. Un outil spécifique permet de tracer les modifications et constitue un référentiel dont les principaux objectifs seront les suivants : – identifier les différentes demandes et assurer leur traçabilité ; – prioriser les demandes qui pourront être classées (par exemple : bloquant, important, évolution souhaitée) ; – assurer le suivi et la communication de l'avancement aux utilisateurs. Pour les demandes de changement en urgence, qui peuvent être la conséquence de dysfonctionnements d'un élément du SIH, la mise en production des changements, qu'ils touchent les applications, leur paramétrage ou les éléments de l'infrastructure font l'objet d'une validation formelle avant mise en production.	Formalisation d'une procédure de gestion des changements traitant des différents points évoqués, communiquée et partagée avec la direction et les acteurs métiers. Mise en place d'un outil permettant d'assurer une traçabilité des demandes et de leur traitement. Formalisation des différents changements et traçabilité des opérations effectuées, de l'initiation à la mise en production, avec notamment la « preuve » des contrôles réalisés. Mise en œuvre d'une séparation entre les environnements de tests et ceux de production et réalisation des changements en environnement de test avec une phase de contrôle.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Fiches pratiques liées.	La politique de changement, notamment lorsqu'elle s'attache à l'évolution des solutions existantes (nouvelles technologies mises en œuvre, nouvelles fonctionnalités...) précise les actions de communication à destination des utilisateurs ainsi que les actions de formation entreprises afin d'assurer la continuité d'exploitation.	
	Fiche 11. – Autorisation des changements aux applications. Fiche 12. – Gestion des changements – Approbation des tests unitairesd'intégration et des tests utilisateurs. Fiche 13. – Mise en production des évolutions applicatives. Fiche 14. – Changements applicatifs en urgence.	

2.2.3. Gestion des développements, acquisitions et migrations

Dans ce paragraphe, il sera notamment traité des projets majeurs qui pourraient conduire l'établissement à faire l'acquisition d'une nouvelle application ou à réaliser un développement spécifique, et plus largement de tout changement majeur pouvant avoir un impact sur la production des états financiers.

Les principes sont les mêmes que ceux évoqués dans les paragraphes traitant de la gestion de projet et de la gestion des changements. Il conviendra également d'évaluer les opérations de migration qui auront un impact sur la cible définie par l'établissement. Une migration représente le passage d'un état existant d'un système d'information ou d'une application vers une cible définie dans un projet ou un programme. La migration de données vise à modifier l'ensemble des données gérées par un système informatique source (matériel et logiciel) pour pouvoir les utiliser sur un autre système cible. Les différences entre les logiciels obligent à transformer les données pour qu'elles soient compatibles avec le nouveau système. Après chargement dans le système cible, les données migrées doivent être vérifiées pour déterminer si elles sont exactes, exhaustives et supportent correctement les processus du nouveau système. Un nettoyage de données est communément effectué afin d'améliorer la qualité des données migrées et d'éliminer les données redondantes ou obsolètes. Une migration peut aussi aboutir à la modification de certains référentiels de données.

Éléments utiles à la démarche d'auditabilité du SIH

Dans le cadre des développements ou acquisitions de nouveaux programmes, il est nécessaire d'avoir défini une procédure qui permette de tracer :

- que les besoins des utilisateurs ont bien été pris en compte et qu'ils ont notamment été retranscrits avec leur contribution directe dans un cahier des charges ou une expression de besoins ;
- que les développements réalisés par le service « études » ont été testés et validés comme conformes aux attentes par les utilisateurs ;
- que la mise en production de ces développements respecte le principe de séparation des tâches, en l'occurrence par le service « exploitation » ;
- que ces développements ou solutions progicielles mises en œuvre font l'objet d'une documentation qui sera tenue à jour lors des évolutions futures de l'organisation ou des solutions.

Le déroulement opérationnel de la migration et la qualité des données comptables et des données de base (séjours, patients, fournisseurs, plan de comptes...) reprises dans le nouveau système sont systémiquement tracés et matérialisés.

La fiabilité du processus de migration mis en place par l'établissement permet de vérifier l'exhaustivité, l'exactitude et l'existence des données reprises dans la nouvelle application. Certains points font l'objet d'attentions particulières, comme :

- la stratégie de migration et la méthodologie de reprise des données retenues, par exemple pour :
  - les soldes comptables (balance générale) ;
  - les postes non soldés (balances auxiliaires : séjours, fournisseurs, immobilisations, factures non parvenues, etc.) et données critiques associées (date d'émission des factures séjours, date d'échéance des factures fournisseurs, traçabilité avec l'ancien système...) ;
  - les autres données reprises (immobilisations, marchés, stocks...) ;
  - le plan comptable ;
  - les données maîtres patients, séjours, fournisseurs... ;
- les opérations de prémigration (nettoyage de l'historique des données, lettrage, transcodification...) ;
- les dossiers de contrôle sur les tests réalisés par l'établissement visant à s'assurer de la correcte reprise des données (nature des tests, anomalies rencontrées et correction, documents conservés).

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Inadéquation des évolutions réalisées avec les besoins définis par le métier. Mise en production d'évolutions non autorisées. Mise en production de versions non stabilisées entraînant des erreurs, des dysfonctionnements, des régressions sur les fonctionnalités de l'application ou une altération des données. Absence de traçabilité des évolutions mises en production. Perte de maîtrise de l'application. Non-séparation des fonctions augmentant le risque de fraude.	**Pilotage du projet, recensement des besoins :** Chaque mise en production de changement (applicatifs/techniques) fait l'objet d'une demande préalable formalisée. Cette étape de validation doit être archivée afin d'assurer la traçabilité des évolutions apportées aux systèmes. Les besoins ont été recensés et formalisés dans un cahier des charges. Les développements mis en œuvre ou les paramétrages retenus ont été testés par les utilisateurs et répondent à leurs attentes. Les solutions ont été testées et formellement approuvées par les utilisateurs. Les applications ou développements font l'objet d'une documentation qui sera régulièrement mise à jour. **Développement, mise en production :** Les principes de séparation des environnements de développement, tests et production ont été mis en place. La séparation des fonctions au sein de la DSI entre développement et mise en production a été respectée ou tracée. Mise en œuvre de tests unitaires pour chaque développement ou changement et identification des anomalies identifiées, puis corrections appropriées avant la mise en production des changements. **Stratégie de migration :** Existence d'un comité de pilotage. Existence d'un planning de migration détaillé. Existence d'une stratégie de migration documentée. Validation formalisée par le métier de la mise en production. **Méthodologie de reprise des données :** Existence d'une méthode de reprise des données documentée. Documentation des règles de transcodification. Matérialisation des contrôles d'intégrité, d'exhaustivité et d'existence. Traçabilité du nettoyage des données historiques. **Contrôles prémigration et traçabilité :** Traçabilité des tests de reprises à blanc. Existence d'un plan de tests prémigration. Formalisation/traçabilité des contrôles effectués. Suivi et correction des anomalies rencontrées. **Contrôles détaillés réalisés suite à la reprise des données et traçabilité :** Rapprochement entre les balances des anciens et nouveaux systèmes compte par compte (comptes généraux et auxiliaires). Rapprochement entre les deux systèmes ou contrôle par sondage des postes non soldés. Contrôle des référentiels tiers repris. Suivi et correction des anomalies identifiées. Conservation des éléments justificatifs.	Formalisation d'une procédure de gestion des changements décrivant, *a minima* : – le dispositif de contrôle à mettre en œuvre dans le cadre de chacune des phases du cycle de changement ; – les validations formelles intervenant dans le processus de gestion du changement. La procédure de gestion des changements est validée par la DSI, mise à jour régulièrement et communiquée aux interlocuteurs appropriés (chefs de projets, notamment). Mise en œuvre d'un outil permettant de garantir la traçabilité des demandes de changements aux applications, systèmes d'exploitation et bases de données ainsi que leur approbation. Sécurisation des canaux de mise en production des changements (applicatifs/techniques) afin que seules les personnes autorisées disposent des droits permettant de réaliser les mises en production. Formalisation d'une procédure de gestion des changements, décrivant le dispositif de contrôle à mettre en œuvre dans le cadre de changements en urgence et ne respectant pas l'intégralité des étapes habituelles du cycle de gestion des changements.
Fiche pratique liée.	Fiche 15. Approbation des développements/acquisitions.	

2.2.4. Gestion de l'exploitation informatique

La gestion de l'exploitation informatique couvre les fonctions nécessaires à la mise en œuvre et la sécurisation des composants du SI, qu'ils soient applicatifs, matériels ou autres. Elle recouvre classiquement les moyens et dispositifs mis en œuvre afin de garantir la fiabilité et la sécurité des traitements, des infrastructures, dans ses objectifs d'apporter aux utilisateurs du SIH la qualité de service et la disponibilité attendues. Dans ces principales composantes, elle s'attache à la supervision de :

- la sécurité physique et logique, si elle n'est pas assurée par une fonction sécurité indépendante ;
- l'exploitation des applications (traitements différés, sauvegarde, reprise...) ;
- l'administration de l'infrastructure informatique (serveur, réseau...) ;
- le suivi et l'optimisation des performances (disponibilité, temps de traitement...) ;
- la mise en production des applications acquises ou développées par la fonction études informatiques.

Éléments utiles à la démarche d'auditabilité du SIH

Trois domaines principaux peuvent être définis :

La gestion des traitements automatisés : il convient de contrôler s'il existe des contrôles sur l'exécution des traitements automatisés afin d'assurer l'exactitude, l'exhaustivité et la rapidité du traitement des données concourant à la constitution de l'information financière.

Le point des traitements automatisés constituera probablement un enjeu majeur au regard des nombreuses interfaces qui composent le SIH et des risques inhérents : dans un exemple cité plus haut concernant l'interface avec une solution de spécialité, une analyse quotidienne des traitements automatisés (interfaces) aurait pu permettre d'identifier un dysfonctionnement.

La gestion des sauvegardes et des procédures de restauration : il convient de déterminer s'il existe des procédures appropriées de sauvegarde et de restauration afin de s'assurer que les données, les programmes et les environnements qui sont nécessaires à la constitution de l'information financière peuvent être récupérés.

Il est souhaitable de s'assurer que des procédures efficaces existent et sont suivies, afin de tester périodiquement l'efficacité du processus de restauration ainsi que la qualité des supports de sauvegarde.

L'accès aux supports de sauvegarde sera également pris en compte afin de garantir la sécurité de l'information financière.

Les procédures de gestion des incidents : il convient de déterminer s'il existe des contrôles permettant de s'assurer que les problèmes du système qui pourraient avoir une incidence sur le processus de génération de l'information financière sont identifiés et résolus dans un délai raisonnable.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
	Définition claire des rôles et des responsabilités (entre équipes exploitation et développement), dans la logique de séparation des fonctions. Un SI est dédié à l'exploitation, notamment pour suivre la gestion des incidents, la gestion des ressources, la planification des travaux, les procédures d'exploitation, et permet la remontée d'indicateurs partagés avec le métier, en vue d'identifier : évolution du SIH, formation complémentaire... Mesure de l'efficacité et de la qualité des services fournis par l'exploitation informatique. Mise en place d'une procédure d'exploitation validée par la direction et permettant d'identifier l'ensemble des tâches à assurer par l'équipe informatique afin d'assurer un niveau de service en lien avec les besoins métiers. L'exploitation quotidienne est consignée au travers d'une liste de contrôles (informatisés ou non) permettant de tracer les opérations réalisées par l'équipe informatique. En cas d'identification d'une anomalie (traitement automatique en erreur, sauvegarde incomplète, surcharge serveur...), un ticket d'incident est ouvert et tracé dans l'outil de gestion des incidents.	

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Traitements automatisés : Présence de traitements automatiques en erreur non détectés impactant l'exactitude et/ou l'exhaustivité de l'information financière.	**Traitements automatisés :** La liste des personnes disposant d'un accès aux programmateurs de travaux est revue *a minima* annuellement par la DSI. Les autorisations de modifier le programmateur de travaux, les traitements batch et les interfaces automatiques doivent être tracées. L'exécution des traitements automatiques (batch, interface, sauvegarde...) est revue quotidiennement, par exemple sur la base d'états générés par le système. Les incidents de traitements sont tracés *via* l'outil de suivi des incidents, revus par le service exploitation et corrigés. Ces corrections doivent être documentées et conservées. La DSI réalise une revue régulière du statut des incidents relatifs aux traitements d'exploitation qui ne sont pas résolus.	**Traitements automatisés :** Formalisation d'une procédure de gestion des traitements automatisés, à mettre à jour régulièrement, traitant des différents points évoqués, communiquée et partagée avec la direction et les acteurs métiers. Définition d'une liste des utilisateurs pouvant accéder aux programmateurs de travaux, à faire validée par la DSI, et élaboration d'une procédure de demande d'accès aux programmateurs de travaux pour les nouveaux arrivants, comprenant une validation de la DSI. Mettre en place une revue quotidienne des traitements automatisés dont les anomalies identifiées donnent lieu à l'ouverture d'un ticket d'incident.
Gestion des incidents et des problèmes : Incidents non résolus entraînant un dysfonctionnement des applicatifs et impactant les états financiers. Demandes utilisateurs non prises en compte dans des délais raisonnables entraînant une perte d'image pour le service informatique et/ou une perte de productivité des équipes.	**Gestion des incidents et des problèmes :** Une procédure de gestion des incidents est définie et formalisée et définit les moyens de suivi (acteurs, outils), les indicateurs de criticité, les dispositifs d'escalade. Tout incident est déclaré, documenté *via* un outil de suivi des incidents et fait l'objet d'une analyse ainsi que d'un plan d'actions jusqu'à sa résolution. La DSI réalise une revue régulière du statut des incidents qui ne sont pas résolus et prend les mesures nécessaires pour solutionner les points de blocage.	**Gestion des incidents et des problèmes :** Élaboration et mise en œuvre d'une procédure de gestion des incidents permettant de documenter, suivre la résolution de ces derniers dans un intervalle de temps en conformité avec les engagements du service informatique vis-à-vis du métier.
Fiches pratiques liées.	Fiche 16. Accès et revue des traitements d'exploitation. Fiche 19. Gestion des incidents.	

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Sauvegardes et restauration : Sauvegardes incomplètes ou corrompues entraînant une perte irréversible de données en cas de défaillance d'un serveur.	**Sauvegardes et restauration :** Les contrôles portent sur : – la fréquence de réalisation des sauvegardes ; – la rotation des supports de sauvegarde ; – le stockage des supports de sauvegarde ; – le contenu des sauvegardes ; – le remplacement des bandes ; – les tests de restauration. Les sauvegardes sont réalisées en fonction des risques identifiés par la DSI. Toutefois, les rotations et fréquences de sauvegardes dépendent de l'analyse d'impact d'une perte des données réalisée par la DSI. *A minima* les sauvegardes sont réalisées quotidiennement et font l'objet de contrôles de bon déroulement (suivi de log, rapports d'anomalies...). Les supports sont distincts pour chaque jour de la semaine et doivent être régulièrement prélevés afin de permettre une rétention des données en phase avec les besoins métiers. Les sauvegardes contiennent l'intégralité des données. *A minima* à chaque modification, les fichiers systèmes et les OS doivent également être sauvegardés. Le remplacement des bandes se fait en fonction des recommandations du constructeur (basé sur le MTBF – *mean time between failures*/moyenne des temps entre deux pannes), *a minima* tous les ans. Un listing des bandes est maintenu et permet d'en connaître le contenu. Les tests de restauration effectués à l'initiative des utilisateurs finaux (par exemple, demande de réplication du système de production sur le système de test) ou du personnel informatique sont globaux. Ils incluent à la fois les données, les programmes et les données systèmes de l'environnement informatique restauré. Les bandes sont stockées dans un coffre ignifugé afin d'assurer la sécurité de l'accès aux bandes et/ou en cas de sinistre. Elles peuvent, selon une périodicité à définir, être externalisées. L'externalisation des sauvegardes auprès d'un tiers peut également être envisagée. Il s'agira de s'assurer dans ce cas, auprès du prestataire, que les dispositifs de continuité, de sécurité mis en œuvre sont conformes aux attentes de l'établissement et aux bonnes pratiques. La fréquence des tests de restauration est annuelle au minimum. Les tests de restauration sont validés par des représentants « métiers » afin de s'assurer du correct fonctionnement du système restauré à partir des bandes de sauvegarde.	**Sauvegardes et restaurations :** Élaboration d'une procédure de gestion des traitements automatisés : – à revoir régulièrement, traitant les différents points évoqués, communiquée et partagée avec la direction et les acteurs métiers ; – définissant les besoins en sauvegarde, pour la restauration ainsi que les périodes de rétentions des données. Formalisation des modalités de stockage, de renouvellement et d'externalisation des bandes de sauvegardes sont formalisées. Réaliser des tests permettant d'identifier l'ensemble des anomalies de restauration de sauvegardes.
Fiches pratiques liées.	Fiche 17. Stratégie de sauvegarde. Fiche 18. Restauration des sauvegardes.	

2.2.5. Informatique « bureautique »

L'informatique bureautique inclut toutes les applications développées par les utilisateurs finaux, généralement à partir d'outils bureautiques de type tableur ou base de données.

Éléments utiles à la démarche d'auditabilité du SIH

L'établissement peut vérifier qu'il existe un minimum de contrôles sur les données exploitées par les applications bureautiques qui échappent aux contrôles généraux, car ils n'entrent généralement pas dans le périmètre de la DSI de l'établissement.

Il est notamment important :

– d'établir et vérifier la liste des fichiers critiques, qui sera validée par la direction ;
– d'établir la liste des utilisateurs ayant accès au répertoire réseau de la comptabilité/reporting financier et de valider cette liste ;
– de contrôler que les serveurs de fichiers sur lesquels sont situés les répertoires critiques sont bien inclus dans le processus de sauvegarde quotidien ;
– de contrôler l'application de la méthodologie de développement et de gestion du changement.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Absence de contrôle des accès aux fichiers impactant la production des états financiers. Modification non autorisée des fichiers impactant la production des états financiers. Perte de données suite à la défaillance des postes informatiques stockant les fichiers bureautiques critiques et dont les espaces personnels des utilisateurs n'auront pas été sauvegardés (stockage disque local du poste irrécupérable). Perte de contrôle des outils suite à l'indisponibilité du concepteur des fichiers bureautiques. Difficultés de maintenance et d'évolution des outils du fait de l'absence de documentation des développements réalisés.	Les fichiers critiques pour l'établissement des résultats financiers ont été recensés par la direction et/ou la DSI. Les fichiers critiques pour l'établissement des résultats financiers ne peuvent être utilisés et modifiés que par le personnel approprié. Les fichiers critiques sont sauvegardés tous les jours. Une procédure invite les utilisateurs à placer leurs fichiers sur des serveurs sauvegardés quotidiennement. Une méthodologie de développement/gestion du changement/*versioning* est appliquée aux fichiers bureautiques utilisés dans le cadre de l'établissement des résultats financiers. Les développements bureautiques sont documentés et testés. La connaissance de ces outils est répartie sur plusieurs collaborateurs de sorte à limiter la dépendance à une seule et même personne.	Lister les fichiers bureautiques critiques impactant les états financiers. Stocker les fichiers bureautiques critiques sur des serveurs entrantdans le champ d'application des contrôles généraux informatiques, pour garantir : – une restriction appropriée des accès ; – une sauvegarde régulière. Réaliser une revue régulière des fichiers bureautiques critiques, et notamment de la documentation disponible vis-à-vis des développements réalisés. S'assurer de la maîtrise des outils par un nombre suffisant de collaborateurs.

2.2.6. Plan de reprise d'activité

Le plan de reprise d'activité (PRA) informatique regroupe l'ensemble des mesures définies pour faire face à un sinistre majeur survenu dans l'établissement mettant hors service les moyens informatiques vitaux. Il fait partie des éléments critiques traités dans le cadre d'un plan de continuité d'activité, qui comprend les procédures, les moyens logistiques et humains mis en œuvre pour garantir la continuité d'activité de l'établissement en situation de sinistre informatique.

Un plan type d'un PRA du SI ainsi que les questions clés à étudier lors de la définition des procédures de retour à la normale en cas de panne sont disponibles dans la boîte à outils pour l'accompagnement des établissements de santé à l'atteinte des prérequis du programme Hôpital numérique, disponible sur l'espace Internet du programme Hôpital numérique (http://www.sante.gouv.fr/programme-hopital-numerique.html) et communiquée aux établissements *via* l'instruction DGOS/MSIOS n° 2012-376 du 31 octobre 2012.

Objectifs et enjeux du plan de continuité d'activité

Seule la partie PRA fait partie des contrôles généraux informatiques. Néanmoins, à titre d'information, sont précisées ci-après quelques notions relatives au plan de continuité des activités (PCA), qui seraient à prendre en considération dans le cadre de l'environnement de contrôle de l'établissement.

Le plan de continuité d'activité est un document qui décrit l'ensemble des procédures et des moyens humains, techniques et logistiques mis en œuvre pour garantir la continuité d'activité de l'établissement en situation de sinistre informatique ayant un impact financier, opérationnel ou d'image majeur.

De la qualité du plan de continuité dépendent l'efficacité et la rapidité de réaction des équipes d'intervention et le retour à une situation d'équilibre. Pour cette raison le plan de secours doit être :

– opérationnel : les procédures doivent être détaillées, explicites et adaptées au type de sinistre et mises en sécurité en dehors de l'outil informatique lui-même ;
– exhaustif : toutes les actions à entreprendre doivent être clairement recensées et synchronisées ;
– maintenu : les équipes doivent s'impliquer pour le tester et le faire évoluer.

Le plan de continuité doit régulièrement être validé par des tests qui, seuls, permettent de mesurer en grandeur réelle la pérennité de l'adéquation de la solution de secours aux objectifs de reprise d'activité. À titre d'exemple, il conviendra notamment de s'assurer des dispositifs mis en œuvre afin :
– d'assurer le suivi des actes réalisés qui seront à facturer ;
– tracer les mouvements de stock...

Éléments utiles à la démarche d'auditabilité du SIH

Afin d'évaluer la cohérence du plan de reprise d'activité avec les besoins de l'établissement en cas de sinistre majeur, il est important de vérifier qu'il reprend les éléments suivants :
– le périmètre couvert par le plan ;
– la fréquence de test du plan et l'implication des utilisateurs métiers ;
– la cohérence du plan vis-à-vis des besoins métiers.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Absence de PRA. Le PRA existe, mais n'est pas testé ou est testé sans le concours des utilisateurs. Le périmètre du PRA ne couvre pas l'exhaustivité des applications critiques (au regard de la production de l'information financière). Indisponibilité du SIH suite à la survenance d'un sinistre majeur relatif à un problème physique, logique ou humain. Les procédures de reprise ne sont pas documentées. À l'issue de test du PRA, les plans d'actions ne sont pas réalisés. Absence de documentation d'un mode de fonctionnement dégradé.	En amont, un travail de fond est à réaliser avec les services concernés et la DSI au cours duquel seront déterminés : – le RTO (*recovery time objective*) qui correspond à la durée maximale d'interruption admissible, c'est-à-dire, jusqu'à la bascule vers le système de secours ; – le RPO (*recovery point objective*) qui correspond à la perte de données maximale admissible, c'est-à-dire l'historique des transactions qui seront conservées et restituées au redémarrage de la solution de secours. En réponse à ces attentes, la mise en œuvre d'un plan de reprise d'activité nécessite la prise en compte des sujets suivant : – gestion générale du plan de reprise d'activité – architecture de secours – cellule de crise – équipe d'intervention ; – restauration technique ordinateur et réseau ; – restauration applicative – remise en phase des traitements ; – gestion du plan de secours utilisateurs ; – retour à la normale ; – plan de test – tests du plan de reprise d'activité – procédures de sauvegarde et d'archivage. Les solutions techniques mises en œuvre devront donc, dans l'analyse, être en adéquation avec les attentes de disponibilité définies par le métier.	Le PRA est formalisé, et prévoit notamment les scenarii de tests réguliers, l'implication des utilisateurs, le traitement des anomalies identifiées. Le PRA est à jour (au regard de la cartographie existante, des personnes impliquées ou prestataires...). Le cas échéant, les tests réalisés sont recensés, les plans d'actions identifiés ainsi que leur traitement. La traçabilité des actions engagées, réalisées, est conservée.

2.3. *Préparer l'étape 3 : revue ciblée de processus et tests des contrôles applicatifs*

2.3.1. Séparation des fonctions

Le COSO (référentiel de contrôle interne défini par le Committee of Sponsoring Organizations of the Treadway Commission) définit la séparation des fonctions comme suit : activité qui consiste à définir et répartir les tâches entre différentes personnes dans le but de réduire les risques d'erreurs et la fraude.

Une politique de séparation des fonctions établit de manière formelle les règles de séparation de tâches au sein d'une organisation. Elle constitue un référentiel au niveau du contrôle interne de l'organisation. Elle se décline généralement au travers d'une matrice d'incompatibilités des fonctions et permet ainsi de définir les profils informatiques en fonction des fiches de poste qui auront été définies. La revue régulière de cette matrice de séparation des fonctions est indispensable afin de s'assurer qu'elle correspond toujours aux activités de l'établissement, à l'évolution de son organisation.

Les risques liés à la séparation des tâches se manifestent suite à une série d'actions réalisées par une même personne qui entraînent une erreur ou une fraude.

Par exemple, un utilisateur ayant accès aux transactions de création/modification du référentiel des fournisseurs et aux transactions de paiement pourrait créer un fournisseur fictif, ou modifier les coordonnées bancaires d'un fournisseur existant, et initier un paiement.

Dans le cadre de cette séparation des fonctions, il sera principalement attendu une séparation des tâches qui permet de bien distinguer les tâches d'enregistrements comptables (accès aux écritures comptables), les tâches opérationnelles (accès aux systèmes opérationnels) et les tâches de conservation des actifs (accès au cash ou bien de valeur).

En d'autres termes, la séparation des fonctions doit être conçue de façon à permettre un contrôle indépendant. Cette séparation des fonctions, adaptée à la situation de l'établissement, doit s'efforcer de dissocier les tâches et fonctions relevant de l'opérationnel, de la protection des biens et de leur enregistrement comptable.

Les règles de séparation des fonctions s'appliquent :

– d'une part, au sein des applications informatiques, à travers la mise en œuvre par exemple de profils applicatifs, afin d'éviter que certaines personnes aient un accès trop large à des fonctions au sein des applications ;
– d'autre part, au sein de la DSI, entre les différents services : par exemple, entre les études informatiques (accès aux outils de développement) et la production informatique (accès à l'environnement de production et aux outils de production).

Ces règles doivent être nuancées, notamment en fonction de la taille de l'établissement et des services concernés par les principes de séparation. En effet, en dessous d'une certaine taille, il peut être difficile de mettre en œuvre une séparation effective des fonctions. Dans ce cas, il est souhaitable de mettre en place des contrôles compensatoires pour limiter les risques liés au cumul des fonctions.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Non-détection d'erreur du fait de l'existence de situations d'autocontrôle (par exemple, liquidation et mandatement). Fraude permise par la détention par une même personne de fonctions applicatives clés incompatibles entre elles (engagement, liquidation et mandatement).	Une revue de processus a permis d'identifier les différentes tâches réalisées par les utilisateurs du système d'information. Une liste des tâches incompatibles a été définie par la direction et celles-ci ont été rapprochées des transactions applicatives correspondantes. Une matrice de séparation des tâches permettant de visualiser facilement les tâches incompatibles a été constituée. Une revue des conflits de séparation des tâches a été effectuée et les mesures adéquates ont été mises en œuvre : – soit la réaffectation des tâches et droits applicatifs correspondants entre les utilisateurs permettent une correcte séparation des tâches ; – soit une validation formelle de la direction des conflits lorsqu'une séparation stricte des tâches n'est pas permise par la structure organisationnelle de l'établissement. Dans cette situation, des contrôles compensatoires devront être mis en place afin de s'assurer de l'absence d'utilisation abusive des fonctions incompatibles.	Pour être efficace, un référentiel de séparation des tâches doit donc être décliné dans les systèmes d'information afin de s'assurer que les droits attribués aux utilisateurs sont conformes aux règles de séparation des tâches et aux délégations de pouvoir accordées dans l'établissement. Sur la base d'une cartographie des processus de l'établissement, la première étape vise à identifier les opérations et leurs interactions entre elles. Sur cette base, les différents intervenants sont identifiés sur la base d'une matrice des responsabilités de type RACI (responsables, acteurs, consultés, informés) déclinée au niveau de chaque processus, voire sous-processus et activités. Ce travail permet d'identifier, sur les processus ou activités jugés critiques, si certaines tâches réalisées par une même personne ne sont pas incompatibles entre elles. Une fois cette matrice réalisée, elle sera mise en œuvre au sein du système d'information et fera l'objet de revues régulières. Cette séparation des tâches s'applique également à la répartition des tâches entre les fonctions métiers et la DSI. Dans le cadre de la gestion des changements ou des développements abordés plus haut dans le document, il a bien été souligné la nécessité d'impliquer les acteurs métiers dans la définition du besoin, les phases de tests ou de validation avant mise en production. Il s'agit de s'assurer d'une correcte répartition des responsabilités entre le métier qui exprime son besoin, la DSI ou le prestataire qui réalise les évolutions souhaitées qui seront testées en fin de cycle par les métiers. Le tout étant contrôlé par la direction.

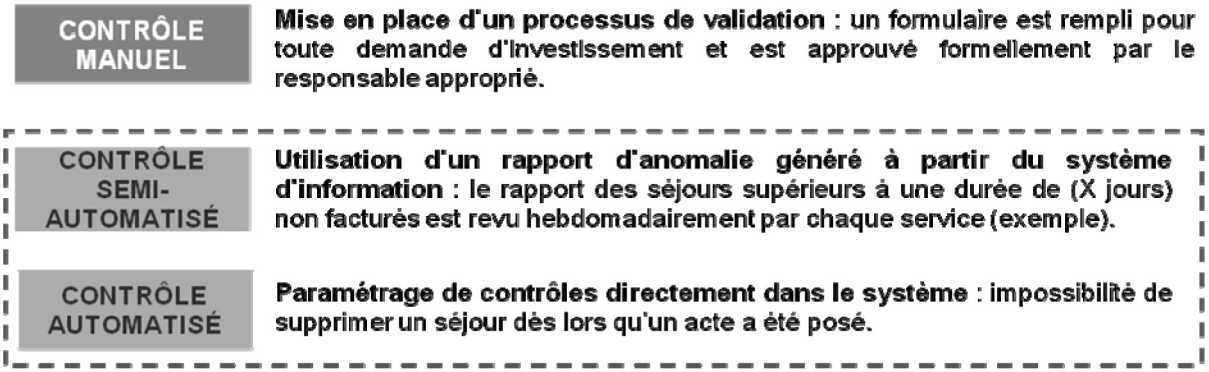
2.3.2. Les types de contrôles

Les contrôles applicatifs et les contrôles généraux informatiques sont étroitement liés. La fiabilité des contrôles généraux informatiques est indispensable pour pouvoir se fier aux contrôles applicatifs, comme l'illustrent les exemples suivants :

Exemple 1 : les applications mises en production ne font pas l'objet de tests. Dans ce cas, les traitements et les états de sortie peuvent être altérés et la production d'information non fiable.

Exemple 2 : les droits d'accès ne sont pas correctement définis. Au-delà d'actes malveillants ou d'erreurs de manipulation, la cohérence des données peut être altérée.

Les contrôles applicatifs sont des contrôles intégrés dans les systèmes et applications qui sont utilisés pour :
– initier ;
– autoriser ;
– enregistrer ;
– générer les informations liées aux états financiers.
Les différentes natures de contrôles sont les suivantes (avec indication d'un exemple) :



Les contrôles applicatifs sont donc :
– les procédures de contrôle automatisées ou programmées présentes dans les applications ;
– les procédures manuelles, effectuées par l'utilisateur, sur lesquelles s'appuie l'établissement pour s'assurer que le traitement des données s'est déroulé correctement.
Ces deux types de contrôle peuvent être préventifs ou de détection :
– les contrôles préventifs sont des contrôles qui sont effectués *a priori*, c'est-à-dire avant d'effectuer toute action dans le système. Exemple : identification/authentification par un mot de passe ;
– les contrôles de détection sont des contrôles effectués *a posteriori* et qui permettent de déterminer si une anomalie s'est produite. Exemple : état des tentatives d'accès non autorisées.
Les contrôles peuvent être des contrôles bloquants, empêchant l'utilisateur d'aller plus loin si le résultat du contrôle est négatif, ou simplement des alertes qui ont pour objectif d'informer du résultat du contrôle.
Les contrôles automatisés sont effectués automatiquement par les programmes aux différents stades du traitement de l'information.
On en distingue quatre types :
– les contrôles d'accès à l'application, qui ont pour objectifs la vérification de la protection et la confidentialité des informations. À titre d'exemple, nous pouvons citer les restrictions d'accès à des applications ou fonctions suivant le profil utilisateur ;
– les contrôles à la saisie des données, qui permettent de contrôler la valeur d'un champ (par exemple, en fonction de son format, du caractère de la saisie obligatoire ou non, qui doit être inclus dans une plage de valeurs...) ou d'un ensemble de champs (par exemple, pour une valeur conditionnée par d'autres champs) ;
– les contrôles des traitements, qui ont, par exemple, pour objectif de vérifier que toutes les données sont traitées, qu'aucune donnée ne disparaît ou n'est artificiellement créée, que les calculs effectués sont exacts. Dans le cas des interfaces, il conviendra notamment de s'assurer que le fichier reçu est identique au fichier émis, ainsi que son contenu. En règle générale, des états de rejets peuvent être utilisés afin de vérifier le déroulement des programmes et l'intégrité des données ;
– les contrôles des sorties qui correspondent généralement aux états mis en forme et diffusés dont le contenu doit être complet et exact au regard des informations présentes dans le système.

2.3.3. Processus et contrôles applicatifs

L'appréciation du risque lié aux contrôles applicatifs porte sur les processus et les applications identifiées comme critiques et est basée sur les critères (ou assertions d'audit) suivants en distinguant les opérations et événements des soldes :
Concernant les flux d'opérations et les événements :
– réalité (existence) : les opérations et les événements qui ont été enregistrés se sont produits et se rapportent à l'entité ;
– exhaustivité : toutes les opérations et tous les événements qui auraient dû être enregistrés sont enregistrés ;

– mesure : les montants et autres données relatives aux opérations et événements ont été correctement enregistrés ;
– séparation des exercices : les opérations et les événements ont été enregistrés dans la bonne période ;
– classification : les opérations et événements ont été enregistrés dans les comptes adéquats).

Concernant les soldes de comptes en fin de période :
– existence : les actifs et passifs existent ;
– droits et obligations : l'entité détient et contrôle les droits sur les actifs et les dettes correspondent aux obligations de l'entité ;
– exhaustivité : tous les actifs et passifs qui auraient dû être enregistrés l'ont bien été ;
– évaluation et imputations : les actifs et les passifs sont inscrits dans les comptes pour des montants appropriés et tous les ajustements résultant de leur évaluation ou imputation sont correctement enregistrés.

Éléments utiles à la démarche d'auditabilité du SIH

L'amélioration du contrôle interne informatique au sein des applications repose sur une analyse des processus.

Cette analyse permettra notamment d'identifier, pour le processus concerné :
– les applications concernées ;
– les interfaces existantes (flux entrants et sortants) ;
– les référentiels en place ;
– les droits d'accès mis en œuvre ;
– les traitements réalisés au sein des applications...

et de mettre en évidence l'identification des risques potentiels.

Exemple de démarche de revue de processus

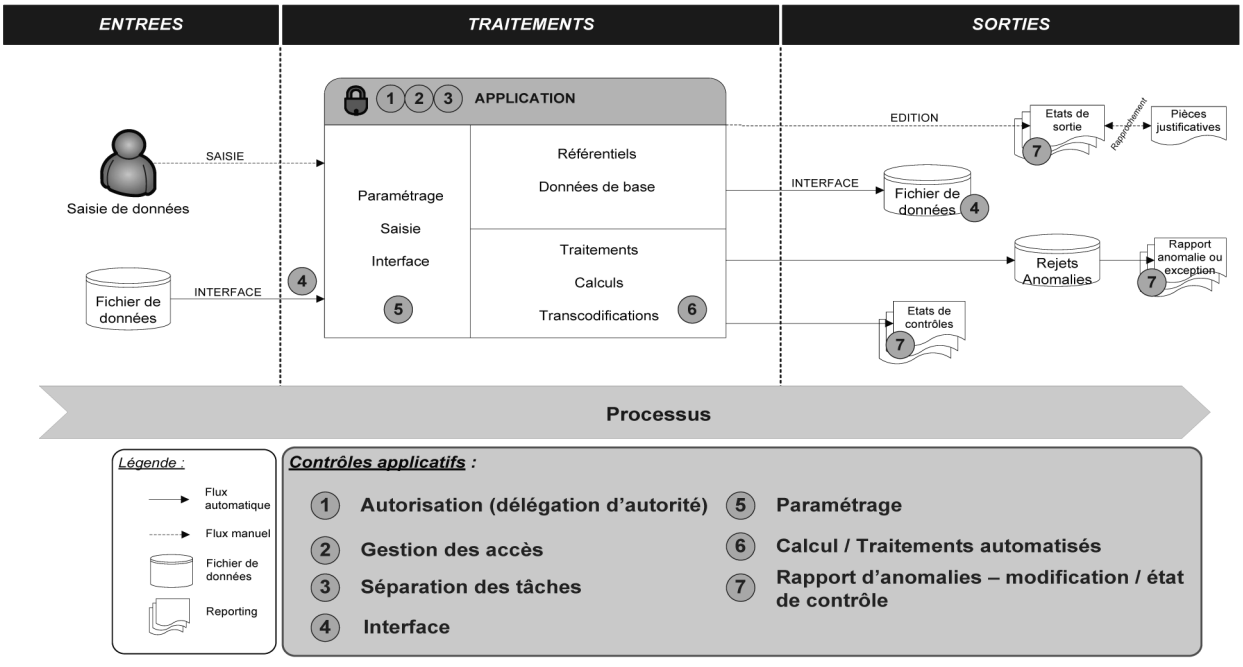
Pour chacun des processus concourant directement ou indirectement à la production des comptes, il est nécessaire de déterminer les applications qui participent aux traitements des données. Cette détermination s'effectue à partir de la cartographie réalisée précédemment.

Selon l'importance du rôle joué par les applications et les interfaces dans chaque processus, seront sélectionnés le ou les processus à analyser.

Ainsi, l'analyse d'une application peut nécessiter l'analyse de plusieurs processus, lorsqu'une même application intervient dans plusieurs processus.

La première étape consistera en une formalisation du processus qui permettra de visualiser l'enchaînement des différentes étapes ou tâches de ce dernier, d'identifier les risques potentiels (interfaces, habilitation, référentiels, traitements et états) ainsi que les contrôles existants (manuels ou automatisés). L'exemple ci-dessous représente une analyse de processus :

Cette phase implique à la fois la DSI qui a la connaissance du système, mais aussi très fortement les services concernés, seuls garants des processus opérationnels.



Dans la revue des processus, les principaux éléments à prendre en considération pourront être les suivants :

POINTS DE VIGILANCE	EXEMPLES DE BONNES PRATIQUES
Les habilitations : Absence de séparation des tâches ou tâches incompatibles entre elles. Accès inappropriés aux applications.	Les profils définis répondent aux principes de séparation des tâches (voir 2.3.1). La définition des habilitations est correcte (voir 2.2.1).
Les interfaces : Absence de contrôle régulier des interfaces. Absence de personne responsable du traitement des anomalies.	Les interfaces sont testées avant mise en production. Pour les flux entrants, les opérations entrées dans le système sont autorisées et validées de manière adéquate. Les données sont enregistrées dans des fichiers *ad hoc*. Les anomalies sont identifiées et leur traitement suivi. Pour les flux sortants, les informations sont exhaustives et font l'objet d'un contrôle.
Les référentiels : Les habilitations ne permettent pas de restreindre l'accès en modification. Les référentiels sont dupliqués sans contrôle (absence de procédure).	Les référentiels sont centralisés ou une procédure permet de s'assurer de la correcte réplication des informations. Seules les personnes habilitées peuvent avoir accès aux modifications des données concernées. Des procédures de mise à jour des référentiels existent et sont appliquées. Les mises à jour sont effectuées de manière simultanée sur l'ensemble du système d'information. Les changements majeurs pouvant avoir un impact sur le traitement de l'information financière sont tracés et archivés.
Les traitements : Absence de procédure de traitement des anomalies. Absence de revue périodique des traitements. Pas de tests avant mise en production de l'application. Absence de documentation des paramétrages et contrôles existants (manuels ou automatisés).	Les opérations sont correctement traitées par le système (résultats conformes à ceux attendus). Des tests réalisés avant mise en production de l'application permettent de s'assurer que les opérations sont traitées de façon cohérente et conforme aux attentes. Périodiquement, des rapprochements de données sont effectués entre différentes sources afin de s'assurer de la cohérence des informations (rapprocher sur une période donnée les séjours clôturés et les factures émises). Il n'existe pas de perte, d'addition, de duplication ou de modification non autorisée des données. Les anomalies sont identifiées et traitées et suivent une procédure définie. La liste des paramétrages, contrôles est documentée et à jour.

2.4. *Externalisation et cadre de contrôle des logiciels et progiciels*

2.4.1. Externalisation

L'externalisation consiste à faire appel à un fournisseur de services externes pour gérer une partie des services informatiques. Dans le but de maîtriser les risques liés à cette externalisation, les partenaires (l'établissement qui externalise et le prestataire) doivent mettre en place et gérer des règles et des mesures de contrôle qui se regroupent autour des trois éléments essentiels suivants :

– le contrat d'externalisation ;
– les SLAs (définition ci-dessous) ;
– l'audit des tiers informatiques (prestataire informatique, GCS, GIP).

Le contrat d'externalisation

Le contrat est un accord exécutoire légal entre deux parties ou plus qui a pour principal but de décrire l'étendue de l'externalisation et les responsabilités de chaque partenaire.

L'appréciation du risque entraîné par l'externalisation de la fonction informatique doit porter sur l'analyse du contrat qui lie l'établissement à son prestataire, ainsi que sur la maîtrise par l'établissement des prestations sous-traitées.

Pour chaque fonction externalisée, un contrat écrit doit préciser les rôles et responsabilités de chaque partie, les prestations et le niveau de service attendu.

La fiabilité du prestataire choisi, l'adéquation de ses compétences avec les besoins de l'établissement, la qualité des services rendus ainsi que sa pérennité constituent des éléments de référence importants : un contrat de prestation de services peu formalisé, ou un prestataire peu fiable, peut entraîner un risque de pertes financières et, dans les cas les plus graves, un risque de continuité d'exploitation.

Il est important de s'assurer que les contrôles généraux tels que décrits dans ce guide sont également mis en œuvre par le prestataire lorsque l'activité sous-traitée inclut des activités de contrôle. Il est préférable de mentionner ces activités de contrôle dans le contrat.

Les SLAs

Un SLA (*service level agreement* ou accord sur les niveaux de service) est un accord entre un fournisseur de service informatique et un client. Le SLA décrit le service informatique, documente les cibles de niveau de service et spécifie les responsabilités du fournisseur de service informatique et du client. Un seul SLA peut couvrir plusieurs services informatiques ou plusieurs clients.

À l'aide de métriques fournies par le prestataire, le client peut apprécier le niveau de respect des accords convenus dans les SLAs.

L'audit des tiers informatiques

Chaque établissement doit considérer dans son système de contrôle interne les contrôles mis en place par le prestataire et doit installer des contrôles compensatoires en cas de faiblesse des contrôles internes du prestataire. Pour être en mesure de connaître les forces et les faiblesses des contrôles du prestataire, un organisme indépendant peut les auditer et, en accord avec le prestataire, l'établissement doit pouvoir prendre connaissance des résultats de l'audit.

L'établissement ne peut pas déléguer les contrôles au prestataire, il ne peut que les lui assigner.

Le prestataire doit notamment disposer d'une politique de sécurité informatique, si possible basée sur une norme. Cet aspect est important pour le prestataire, car il démontre ainsi sa volonté de protéger efficacement les données de ses clients. Pour s'assurer du niveau de contrôle interne du prestataire, la DSI peut se reposer sur les rapports obtenus par le prestataire dans le cadre d'un audit réalisé suivant la norme ISAE 3402.

La norme ISAE 3402

ISAE (*International Standards for Assurance Engagements*) 3402 est une norme d'assurance globale pour rendre compte des contrôles en place chez les organismes de services.

Cette norme est entrée en vigueur le 15 juin 2011, en partie en réponse à l'adoption de la loi Sarbanes-Oxley (souvent désignée par l'acronyme SOX) à la suite des scandales financiers Enron et WorldCom. La norme a pour objectif de protéger les actionnaires, et le public en général, des erreurs comptables et des pratiques frauduleuses.

La norme ISAE 3402 est une extension et l'expansion de SAS 70 (la déclaration sur des normes de vérification n° 70), qui définit les normes que l'auditeur doit employer pour évaluer les contrôles internes en place au sein d'une entreprise de service. SAS 70 a été développé par l'American Institute of Certified Public Accountants (AICPA) comme une simplification d'un ensemble de critères pour les normes d'audit définies à l'origine en 1988.

Dans la norme ISAE 3402, comme dans son prédécesseur SAS 70, les rapports des auditeurs sont classés comme étant de type I ou de type II. Dans un rapport de type I, l'auditeur évalue les efforts d'une organisation de service au moment de la vérification pour éviter les incohérences, les erreurs et les fausses déclarations. L'auditeur évalue également la probabilité que ces efforts produisent des résultats futurs souhaités. Un rapport de type II contient les mêmes informations que celles contenues dans un rapport de type I. En outre, l'auditeur tente de déterminer l'efficacité des contrôles depuis leur mise en œuvre. Le rapport de type II présente généralement les tests réalisés à partir de données recueillies sur une période de trois à douze mois.

L'établissement devra ainsi privilégier les prestataires ayant obtenu un rapport de type II permettant de s'assurer de l'efficacité opérationnelle du contrôle interne du prestataire.

Éléments utiles à la démarche d'auditabilité du SIH

Dans ce contexte, il est important d'assurer un suivi de l'ensemble des contrats d'externalisation souscrits par l'établissement.

Il sera ainsi possible de vérifier et démontrer que les sous-traitants choisis correspondent aux besoins de l'établissement en présentant :

- les procédures de choix et de validation du choix du sous-traitant ;
- les caractéristiques des sous-traitants choisis ;
- les SLAs existants dans les contrats et leur niveau d'application ;
- les clauses d'audit et leur modalité d'application.

POINTS DE VIGILANCE	EXEMPLES de bonnes pratiques	EXEMPLES D'ACTIONS à mener et documents à préparer
Défaillance du prestataire. Non-respect des niveaux de service contractualisés. Difficultés à récupérer les données externalisées en cas de dénonciation du contrat. Fuite de données.	La présence d'un contrat pour chaque activité externalisée contenant *a minima* les sujets suivants : – le périmètre du contrat (applications, infrastructure, services...) ; – la responsabilité des deux parties ; – les clauses de résiliation ; – les niveaux de service attendus et leurs modes de revue ; – les actions à mettre en œuvre en cas de non-atteinte des niveaux de service ; – les modalités de fin des prestations ; – les modalités d'échanges avec le prestataire, notamment en matière de délai, d'états souhaités, de documentation des systèmes ; – les modalités d'audit du prestataire. La traçabilité des opérations réalisées par le prestataire est assurée par l'utilisation de comptes nominatifs.	Les contrats relatifs aux activités externalisées contiennent, *a minima*, les sujets recommandés par les pratiques. À défaut, un avenant au contrat pourra être négocié avec le prestataire. Une revue périodique du niveau de service délivré par le prestataire est réalisée et comparée aux conditions contractualisées. Une revue périodique est réalisée des comptes applicatifs de base de données et d'administration du domaine détenus par le prestataire de sorte à s'assurer que : – les comptes nominatifs correspondent à des salariés toujours en poste chez le prestataire ; – les comptes génériques sont restreints à des exigences techniques.

2.4.2. Recommandations pour l'acquisition de nouveaux logiciels ou progiciels

Au-delà des fonctionnalités classiques recherchées, ce paragraphe a pour objectif d'apporter un éclairage sur certains points qui peuvent être importants lors de l'acquisition de nouveaux logiciels ou progiciels, dans le cadre de l'auditabilité des systèmes d'information :

– la documentation ;
– la gestion des habilitations ;
– les contrôles applicatifs ;
– la piste d'audit.

Documentation

Il sera souhaitable que le concepteur (éditeur et/ou intégrateur), pour la solution retenue, puisse mettre à disposition de l'établissement :

– une documentation de la solution précisant notamment le périmètre de cette dernière et des modules ou fonctionnalités retenus par l'établissement. Cette documentation sera tenue à jour des modifications engagées par le concepteur dans le cadre des mises à jour de son produit ;
– le modèle de données retenu permettant notamment à l'établissement de s'assurer de la cohérence des référentiels du SIH au regard des interfaces qui pourraient être mises en œuvre (cohérence des formats de données, des zones utilisées...). Au titre des contrôles de cohérence envisageables, la connaissance de ces modèles de données sera également utile afin d'extraire certaines données spécifiques permettant de confronter les données présentes en base à celles reportées dans des états standards ou spécifiques du progiciel ;
– les procédures de saisie, enregistrement, modification de données devront être documentées ainsi que les traitements existants au sein même de l'application ;
– la documentation des paramétrages réalisés qui pourra être à la charge de l'intégrateur ou de l'établissement et qui sera mise à jour des évolutions réalisées dans le cadre du cycle de vie produit ;
– le cas de défaillance du prestataire devra être également prévu sur un plan contractuel, notamment le dépôt des sources auprès d'un tiers agréé permettant, le cas échéant, à l'établissement de disposer des sources afin d'assurer la continuité d'exploitation de celle-ci.

Habilitations

La gestion des droits d'accès est un domaine qui doit être étudié systématiquement. Le choix d'un logiciel, en fonction de sa couverture, peut conduire au regroupement au sein d'une même application de nombreuses fonctionnalités qui, auparavant, pouvaient être réparties entre plusieurs systèmes. Par exemple, la gestion du cycle achats peut intégrer les fonctionnalités suivantes :

– le référencement des fournisseurs, des marchés ;
– la passation des marchés, des bons de commandes ;
– la vérification des bons de livraison ;
– le rapprochement des factures ;
– la liquidation.

La gestion des habilitations, élément essentiel de la sécurité logique, permet généralement de définir des profils utilisateurs types.

Il convient de s'assurer :
- de la manière dont la gestion des habilitations est réalisée afin de s'assurer de la capacité de la solution à appliquer les droits d'accès utilisateurs conformément aux attentes définies par le contrôle interne de l'établissement ;
- des caractéristiques des paramètres généraux de sécurité, leur absence étant considérée comme une faiblesse générale du système d'information, à savoir (*cf.* 1.2.1) :
  - gestion des mots de passe (longueur, fréquence de renouvellement...) ;
  - protection du poste de l'utilisateur (blocage en cas de tentatives de connexion, déconnexion automatique passé un certain délai sans utilisation) ;
  - historique des opérations effectuées par les utilisateurs qui doivent être horodatées et nommées.

Contrôles applicatifs

Au travers du paramétrage de la solution, il sera également intéressant d'identifier les contrôles existants, qu'ils soient automatiques ou semi-automatiques, comme par exemple :

OBJET DU CONTRÔLE	NATURE	TYPE DE CONTRÔLE	POINT DE VIGILANCE
Les actes ne peuvent être posés sur un séjour clôturé ou dans une plage de dates antérieure.	Traitement	Automatisé	Contrôle de cohérence permettant de s'assurer de la correcte imputation d'un acte au bon séjour.
La suppression physique d'un enregistrement en base est proscrite.	Traitement	Automatisé	Acte malveillant, fraude possible.
La suppression logique d'un enregistrement est proscrite.	Traitement	Automatisé	Acte malveillant, erreur. Les opérations en base doivent être tracées, nommées et horodatées.
Un état périodique permet de contrôler les anomalies constatées (incohérence, erreur de traitement d'interface...).	État	Semi-automatisé	S'assurer que les anomalies sont détectées et pourront faire l'objet d'un traitement.

Dans ce cadre, une attention particulière de l'établissement sera à porter sur les thématiques suivantes, qui dépendent de chaque établissement, de son organisation, des applications en place et des niveaux d'automatisation mis en œuvre :
- correct paramétrage des contrôles ;
- règles de gestion comptable ;
- niveau d'automatisation des contrôles ;
- fiabilité des traitements et des calculs réalisés au sein des applications clés du processus ;
- fiabilité des états de contrôle ou d'anomalie ;
- identification des interfaces existantes entre les applications clés et analyse des contrôles permettant de s'assurer du correct déversement des données ;
- analyse des accès aux transactions sensibles des applications clés et de la séparation des fonctions.

Piste d'audit

La piste d'audit recouvre une importance particulière, car elle permet de retrouver une pièce justificative. En effet, dans une application comptable classique, lors de l'enregistrement d'une écriture, un utilisateur saisit également une référence permettant de retrouver la pièce justifiant l'écriture comptable (cette pièce pouvant être par exemple une facture).

Dans ce cadre, il peut être proposé des fonctionnalités de piste d'audit dynamique qui permettent d'identifier les opérations qui sont à la source d'une écriture comptable. Par exemple, une écriture d'achat passée dans la comptabilité fournisseurs peut trouver son origine dans le module achats. Une fonctionnalité de piste d'audit dynamique doit permettre, à partir de l'écriture comptable, de revenir au document de base (une facture par exemple), voire à toutes les opérations liées à ce document et présentes dans le système (exemples : un bon de livraison, un bon de commande, une demande d'achat).

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

PARTIE 3

FICHES PRATIQUES

Les fiches pratiques présentées ci-après sont à consulter en lien avec la partie 2 de ce guide dédiée à la préparation des établissements à l'audit de leur SIH. Elles sont également téléchargeables sur l'espace Internet du programme (http://www.sante.gouv.fr/la-fiabilisation-et-la-certification-des-comptes-des-etablissements-publics-de-sante.html) en version tableur, modifiables par les établissements qui peuvent ainsi les remplir et les adapter.

Elles ont pour objectif d'aider les établissements à identifier concrètement les objectifs, bonnes pratiques, documentation à préparer et tests à mener sur des points essentiels d'auditabilité des SI :

FICHE 1 : Présentation du système d'information.

FICHE 2 : Mécanismes d'identification.

FICHE 3 : Comptes génériques.

FICHE 4 : Configuration des mots de passe – Applications.

FICHE 5 : Accès administrateur.

FICHE 6 : Gestion des droits d'accès.

FICHE 7 : Matrice de séparation des tâches.

FICHE 8 : Gestion des accès aux applications, bases de données et systèmes d'exploitation Création, modification et suppression des accès.

FICHE 9 : Revue périodique des accès aux applications.

FICHE 10 : Restriction des accès physiques.

FICHE 11 : Autorisation des changements aux applications.

FICHE 12 : Gestion des changements – Approbation des tests unitaires d'intégration et des tests utilisateurs.

FICHE 13 : Mise en production des évolutions applicatives.

FICHE 14 : Changements applicatifs en urgence.

FICHE 15 : Approbation des développements/acquisitions.

FICHE 16 : Accès et revue des traitements d'exploitation.

FICHE 17 : Stratégie de sauvegarde.

FICHE 18 : Restauration des sauvegardes.

FICHE 19 : Gestion des incidents.

NB. – Les applications concernées par l'auditabilité du système d'information sont définies dans le paragraphe 1.2.1 de ce document.

FICHE 1

Présentation du système d'information

FICHE 1.1.

Prise de connaissance du SI

Etablissement		**Période (année)**	
Périmètre	Toutes applications	**Responsable du contrôle**	
Objectif d'audit	L'objectif de cette fiche est de synthétiser les principaux indicateurs permettant une meilleure compréhension du système d'information.		
Procédure	Compléter l'ensemble des informations demandées dans la présente fiche et référencer la documentation.		

Schéma Directeur SIH

Contrôle	Documentation attendue	Pièces justificatives
La stratégie du SIH est définie, partagée avec la direction générale de l'établissement et les métiers. Ce schéma directeur fait l'objet d'une planification pluriannuelle, réajustée en fonction du contexte de l'établissement ou des contraintes règlementaires. La gestion des changements (évolutions fonctionnelles du SI, infrastructure) est alignée sur le schéma directeur.	Schéma directeur Liste des Projets en cours ou à venir	Insérer la référence du document ici

Organigramme de la DSI

Contrôle	Documentation attendue	Pièces justificatives
L'organigramme permet d'identifier les liens fonctionnels, organisationnels et hiérarchiques de la fonction informatique au sein des établissements.	Organigramme de la DSI	Insérer la référence du document ici

Revue des applications

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principales applications financières ainsi que les applications métiers significatives.	Tableau de synthèse des applications dûment complété	Voir onglet Applications

Interfaces

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principales interfaces entre les principales applications du SI.	Tableau de synthèse des principales interfaces dûment complété	Voir onglet Interfaces

Cartographie applicative

Contrôle	Documentation attendue	Pièces justificatives
La cartographie applicative est disponible et représente sous forme graphique les principales applications du système d'information (fonctionnalités, système d'exploitation, base de données...) ainsi que les flux de données (type de données, format, fréquence du flux...). Un exemple de cartographie applicative est disponible dans l'onglet "cartographie applicative".	Cartographie applicative	Insérer la référence du document ici

Contrats/mutualisation

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principaux contrats conclus par la DSI ou ayant un impact direct sur la disponibilité des systèmes d'informations (contrats de maintenance, contrats de service…)	Tableau de synthèse des principaux contrats dûment complété	Voir onglet contrats

Effectifs

Contrôle	Documentation attendue	Pièces justificatives
Document, à jour, synthétisant les effectifs internes et externes agissant pour le compte de la DSI	Tableau de synthèse des effectifs internes et externes	Insérer la référence du document ici

FICHE 1.2.

Liste des applications

APPLICATION	INTER-locuteur MOA	INTER-locuteur MOE	FONCTION-nalités	HÉBER-gement (lieu si héb. en propre et/ou nom u tiers si applicable)	HÉBER-gement (local, externalisé)	TYPE 1. Dévelo-ppements internes 2. Dévelop-pements par un tiers 3. Progiciel 4. Fichier bureautique	DATE de mise en place	SUPPORT éditeur (N/A si déve-loppement spécifique)	Prestataire pour la maintenance	DATE de fin d'utilisation prévue (si applicable)	OS du serveur hébergeant l'application	BASE de données	PROJET d'évolution	VIRTUALISÉ (O/N)	CRITICITÉ (1 à 5)
Exemple															
Finance E +	Contrôle de gestion	XX	Compta-bilité générale Compta-bilité analytique	Salle serveur	Local	Progiciel	11/04/2001	OUI Jusqu'au 31/12/2018	XX Informa-tique	31/10/2016	Windows Server 2003	SQL Server	Montée de version en v8.2 en janvier 2013	OUI	1
Applications financières critiques															
Autres applications significatives															

FICHE 1.3.

Liste des principales interfaces internes et externes

ID	SOURCE	DESTINATION	TYPE DE FLUX	PROTOCOLE	PÉRIODICITÉ	DÉCLEN-chement	DONNÉES échangées	CONTRÔLES

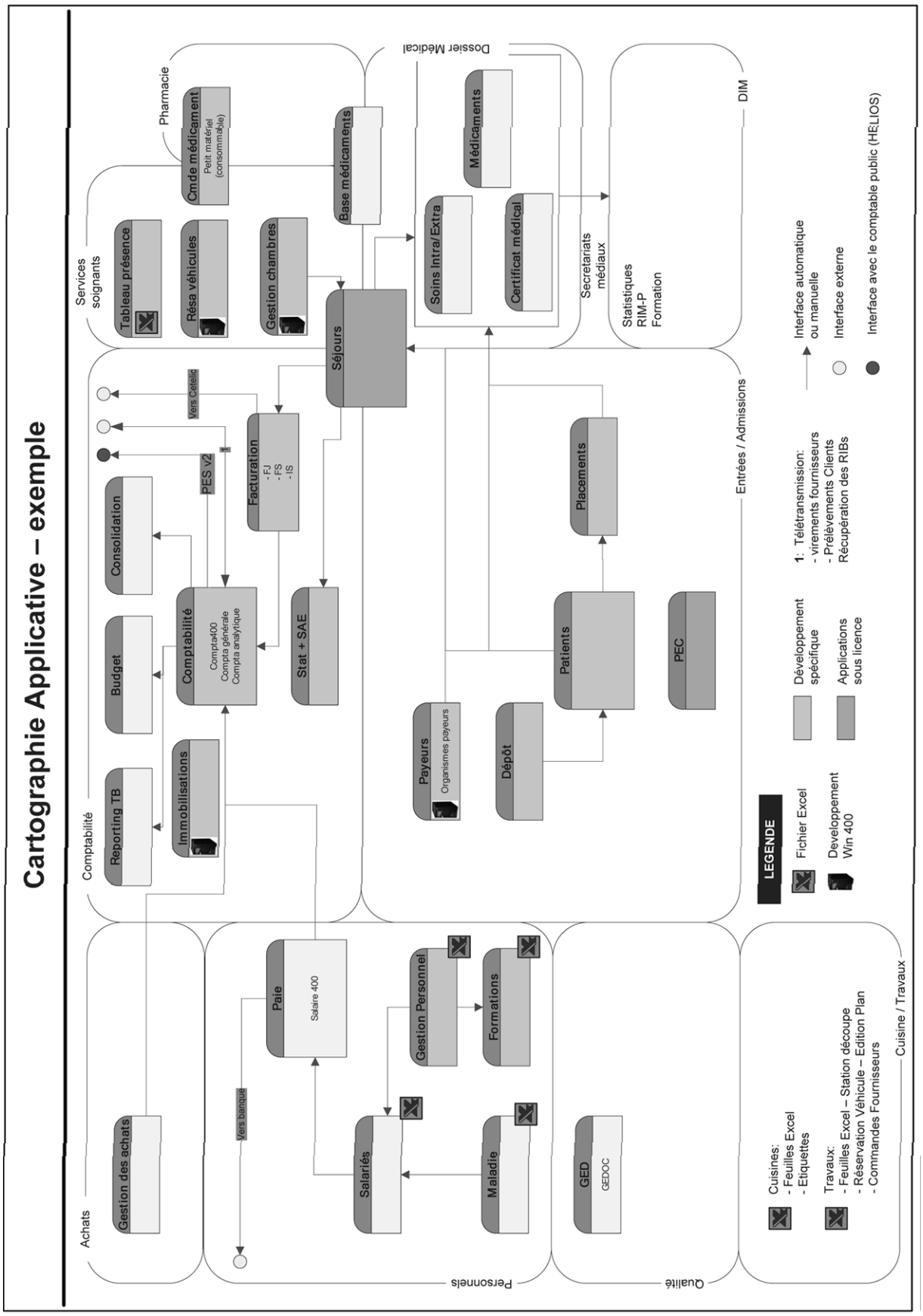
FICHE 1.4.

Liste des principaux contrats internes et externes

PARTENAIRE	OBJET DU CONTRAT	DATE d'engagement	DATE DE FIN d'engagement	INDICATEURS de niveau de service	....

FICHE 1.5.

Exemple de cartographie applicative



FICHE 2

Mécanismes d'identification

Catégorie	Contrôles généraux informatiques	**Domaine**	Identification et authentification
Thème	Mécanismes d'identification		

Objectif

Les applications clés du SIH mettent en œuvre un mécanisme d'identification permettant d'associer un identifiant et un mot de passe à un utilisateur.

Exemples de bonnes pratiques

La politique de sécurité précise que l'ensemble des applications clés du SIH doit mettre en œuvre des mécanismes d'identification permettant d'associer un identifiant et un mot de passe à un utilisateur.

Les revues annuelles des comptes utilisateurs sont validées par les responsables hiérarchiques des utilisateurs.

Documentation à préparer

Liste des utilisateurs des applications, bases de données et systèmes d'exploitation clés.
Documentation justifiant de la nécessité d'utilisation d'un mot de passe pour se connecter aux applications, bases de données et systèmes d'exploitation clés (copies d'écran, extraction de tables de paramétrage...)

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux mécanismes d'identification.
Mise en œuvre	Vérifier le paramétrage des accès aux applications et s'assurer qu'un mot de passe et un identifiant sont requis pour toute connexion.

FICHE 3

Comptes génériques

Catégorie	Contrôles généraux informatiques	**Domaine**	Identification et authentification
Thème	Comptes génériques		

Objectif

Les comptes génériques sont limités et justifiés par les besoins des services.

Exemples de bonnes pratiques

Les comptes génériques doivent être limités au maximum afin de garantir la traçabilité des opérations.

Documentation à préparer

Liste des utilisateurs des applications, bases de données et systèmes d'exploitation clés.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux comptes génériques.
Mise en œuvre	Lister les comptes utilisateurs et contrôler qu'il n'existe pas de comptes génériques ou qu'ils sont limités et justifiés.

FICHE 4

Configuration des mots de passe – Applications

Catégorie	Contrôles généraux informatiques	**Domaine**	Identification et authentification

Thème	Configuration des mots de passe - Applications

Objectif

Les paramètres de gestion des mots de passe applicatifs sont configurés en accord avec la politique de sécurité de l'établissement et les meilleures pratiques.

Exemples de bonnes pratiques

Les mots de passe utilisés pour l'authentification aux applications clés suivent des règles de gestion et de syntaxe établies par l'établissement, conformes aux meilleures pratiques :
- obligation de changer le mot de passe lors de la première connexion,
- modification régulière du mot de passe (durée de vie maximale recommandée <= 90 jours),
- non trivialité des mots de passe
- règles de syntaxe :
    - longueur minimale >= 8 caractères recommandés,
    - obligation de recourir à des caractères alphanumériques et/ou caractères spéciaux recommandés,
- historisation des derniers mots de passe (12 recommandé).
- hombre maximal de tentatives infructueuses de connexion avant blocage du compte (3 recommandé).

Documentation à préparer

Extractions système du paramétrage des contraintes de mot de passe pour les applications du périmètre.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux contraintes de mot de passe.
Mise en œuvre	Recenser le paramétrage des contraintes de mot de passe pour les applications concernées. S'assurer, dans la limite des contraintes techniques, que le paramétrage est conforme à celui décrit dans la politique de sécurité.

FICHE 5

Accès administrateur

Catégorie	Contrôles généraux informatiques	**Domaine**	Administrateurs
Thème	Accès administrateur		

Objectif

L'attribution des droits d'administration est limitée.

Exemples de bonnes pratiques

L'accès aux comptes d'administrateurs des applications clés, ou ayant des droits étendus, est limité à un nombre restreint d'administrateurs justifiés par les besoins des services.

Documentation à préparer

Liste des administrateurs par application, système et domaine
Liste des employés (RH) avec précision de la fonction de la personne.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux comptes d'administration.
Mise en œuvre	Les utilisateurs ayant des droits d'administrateur ou ayant accès au compte administrateur pour les applications, bases de données et systèmes d'exploitation clés sont justifiés.

FICHE 6

Gestion des droits d'accès

Catégorie	Contrôles généraux informatiques	**Domaine**	Configuration des droits d'accès
Thème	Gestion des règles d'accès		

Objectif

L'attribution des droits d'accès des applications, bases de données et systèmes d'exploitation clés est réalisée conformément aux besoins métiers de l'utilisateur.

Exemples de bonnes pratiques

Des profils ont été définis dans les applications et les systèmes afin d'attribuer des droits d'accès en relation avec les rôles et les responsabilités des utilisateurs.

Documentation à préparer

Extraction des profils utilisateurs et des droits associés
Extraction de la liste des utilisateurs avec indication des profils attribués pour les applications, bases de données et systèmes d'exploitation clés
Liste des employés (RH) avec précision de la fonction de la personne

Eléments à préparer

Formalisation	La politique de sécurité identifie les règles de gestion des droits d'accès.
Mise en œuvre	Les profils d'autorisation dans les applications sont définis en fonction des besoins opérationnels des utilisateurs.

FICHE 7

Matrice de séparation des tâches

Catégorie	Contrôles généraux informatiques	**Domaine**	Configuration des droits d'accès

Thème	Matrice de séparation des tâches

Objectif

Les principes de séparation des tâches sont respectés pour les applications du périmètre (voir guide partie 2.3.1).

Exemples de bonnes pratiques

Une matrice de séparation des fonctions est définie et validée par la direction générale et est appliquée au niveau informatique.

Documentation à préparer

Matrice de séparation des tâches validée par la DSI
Extraction des profils utilisateurs et des droits associés

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs à la séparation des tâches.
Mise en œuvre	Une matrice de séparation des tâches existe et est validée. La matrice a été appliquée dans les systèmes (construction des profils, etc.). Les profils d'autorisation dans les applications correspondent à la matrice de séparation des tâches.

FICHE 8

Gestion des accès aux applications, bases de données et systèmes d'exploitation Création, modification et suppression des accès

Catégorie	Contrôles généraux informatiques	Domaine	Gestion des accès

Thème	Gestion des accès aux applications, bases de données et systèmes d'exploitation - Création/modification et suppression des accès

Objectif

Les processus de gestion des utilisateurs, dans les applications, bases de données et systèmes d'exploitation sont encadrés par une procédure régulièrement testée.

Exemples de bonnes pratiques

La procédure de gestion des accès aux applications, bases de données et systèmes d'exploitation clés est formalisée et précise les modalités de création-modification-suppression des accès utilisateurs.
La procédure précise notamment l'émetteur des demandes, les modalités d'approbation ainsi que les revues périodiques.
L'ensemble des créations ou modifications de compte applicatif (y compris les comptes techniques et temporaires) font l'objet d'une demande formalisée précisant notamment les droits associés au compte. Chaque demande doit être validée par les personnes appropriées.
Dans le cas de départ (même à titre provisoire) les comptes sont désactivés le jour du départ

Documentation à préparer

Liste des utilisateurs des applications, bases de données et systèmes d'exploitation clés.
Liste des agents (RH) ou liste des entrées/sorties de personnel sur la période auditée.
Formulaires de demande de création/modification/suppression de compte réalisés sur la période.

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs à la gestion des accès

Mise en œuvre	Extraire de l'application les comptes créés sur l'exercice. Selon le volume, pour un échantillon ou l'exhaustivité des comptes créés, vérifier qu'ils ont fait l'objet de demandes et ont été validés par la hiérarchie appropriée. Comparer la liste des agents qui ont quitté l'établissement avec la liste des comptes qui ont été fermés/supprimés en provenance du système (vérifier également le délai entre la date de départ et la fermeture des comptes).

FICHE 9

Revue périodique des accès aux applications

Catégorie	Contrôles généraux informatiques	**Domaine**	Gestion des accès

Thème	Revue périodique des accès aux applications

Objectif

Les accès aux applications, bases de données et systèmes d'exploitation clés sont régulièrement revus.

Exemples de bonnes pratiques

Une procédure de revue périodique des comptes, des droits d'accès associés et du respect de la séparation des fonctions par les responsables "Métiers" est en place pour les applications clés. Ces revues impliquent la DSI et les responsables de services.
La DSI initie la revue en éditant les listes d'utilisateurs avec leurs droits d'accès.
Les responsables de service revoient ces listes en identifiant les utilisateurs et les droits d'accès injustifiés.
Les responsables applicatifs effectuent dans le système les corrections nécessaires sur les droits d'accès conformément aux commentaires des responsables de service.

Documentation à préparer

Documents formalisant la revue des droits d'accès
Preuves de la correction des anomalies identifiées
Logs de connexion des applications du périmètre

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs aux revues périodiques des accès aux applications
Mise en œuvre	La dernière revue des comptes utilisateurs a été formalisée et date de moins d'un an. Elle a été réalisée avec les responsables des services concernés. Les anomalies détectées ont été corrigées. Si applicable, sélectionner aléatoirement X comptes à supprimer et recenser des preuves que les corrections nécessaires ont été effectuées dans le système, dans des délais raisonnables (par exemple, moins d'une semaine après la revue). Si applicable, vérifier que les logs de connexions infructueuses sont contrôlés et que des actions sont prises afin d'en détecter les origines.

FICHE 10

Restriction des accès physiques

Catégorie	Contrôles généraux informatiques	Domaine	Gestion des accès

Thème	Restriction des accès physiques

Objectif

L'accès aux installations informatiques est limité aux personnes autorisées. Des dispositifs de sécurité adéquats sont mis en place.

Exemples de bonnes pratiques

Les installations informatiques sont équipées de dispositifs de sécurité permettant d'assurer la sécurité des infrastructures. Les autorisations d'accès sont attribuées sur la base d'une demande formalisée validée par les responsables informatiques. En cas de départ d'un agent, les accès aux installations informatiques sont supprimés dans les plus courts délais.
Des revues périodiques de la liste des personnes ayant accès aux installations informatiques sont formellement validées par le DSI pour s'assurer que les droits correspondent aux responsabilités assignées.
Une revue des logs d'accès est réalisée régulièrement afin de s'assurer de la régularité des accès aux installations informatiques.

Documentation à préparer

Liste des utilisateurs autorisés à accéder à la salle informatique (validation DSI)
Extraction du système de badgeage de la liste des personnes ayant la possibilité d'accéder à la salle informatique
Extraction des logs d'accès du système de badgeage.
Compte rendu de la dernière revue des accès à la salle informatique
Liste des employés (RH) ou liste des entrées/sorties de personnel sur la période auditée

Eléments à préparer

Formalisation	La politique de sécurité traite des points relatifs à la gestion des accès physiques
Mise en œuvre	Les éléments de sécurité (système d'accès à badges, détection incendie, climatisation) sont opérationnels. L'extraction du système de badgeage des personnes ayant un accès à la salle informatique est conforme avec la liste validée par la DSI (si le système ne conserve pas les logs ou s'il n'y a pas de système de badge, un formulaire d'accès ou un registre papier des E/S est à jour et consultable). Les formulaires de demandes d'attribution d'accès aux installations informatiques (y compris pour les prestataires) sont validés par les responsables informatiques. Les personnes (y compris prestataires sous contrat) disposant d'accès à la salle informatique font toujours partie du personnel.

FICHE 11

Autorisation des changements aux applications

Catégorie	Contrôles généraux informatiques	**Domaine**	Autorisation, développement, test et approbation

Thème	Autorisation des changements aux applications

Objectif

Les changements apportés aux applications sensibles sont autorisés par les personnes habilitées. Les demandes de changements sont formalisées et suivies grâce à un outil spécifique.

Exemples de bonnes pratiques

Les demandes de changements applicatifs et techniques sont formalisées, analysées puis validées par la DSI et/ou le responsable de service.
Les demandes de changements sont documentées et suivies grâce à un outil spécifique.

Documentation à préparer

Procédure de gestion des changements applicatifs.
Modèle de fiche de demande d'intervention diffusée aux utilisateurs.
Liste des changements de l'exercice pour les applications, systèmes d'exploitation et bases de données du périmètre (à partir de la liste des mises en production).
Validations de la DSI.

Eléments à préparer

Formalisation	Les procédures et méthodologies de gestion des changements applicatifs sont disponibles et traitent notamment de la gestion des demandes des changements.
Mise en œuvre	Les modifications applicatives, sont : - documentées, - validées par la DSI. La liste des modifications applicatives a été revue par la DSI Les demandes de changement sont tracées.

FICHE 12

Gestion des changements – Approbation des tests unitaires d'intégration et des tests utilisateurs

Catégorie	Contrôles généraux informatiques	**Domaine**	Autorisation, développement, test et approbation

Thème	Gestion des changements : approbation des tests unitaires, d'intégration et des tests utilisateurs.

Objectif

Les changements apportés aux applications sensibles ont fait l'objet de tests par la DSI et les utilisateurs, sur des bases de tests. Ces tests sont documentés et ont permis la validation pour mise en production.

Exemples de bonnes pratiques

Les changements font l'objet de tests unitaires par l'informatique, de tests d'intégration et d'une recette fonctionnelle par les utilisateurs avant la mise en production.
Les changements sont testés dans un environnement de test séparé.
Les changements applicatifs sont validés formellement par le demandeur et/ou la DSI avant la mise en production.

Documentation à préparer

Procédure de gestion des changements applicatifs.
Liste des évolutions de l'exercice pour les applications, systèmes d'exploitation et bases de données du périmètre (à partir de la liste des mises en production).
Documentation réalisée au cours de la phase de test.

Eléments à préparer

Formalisation	Les procédures et méthodologies de gestion des changements applicatifs existent, sont disponibles, à jour et traitent notamment des tests réalisés dans le cadre des changements.
Mise en œuvre	Pour toute modification applicative : - la phase de test unitaire est documentée par le service informatique, - la recette fonctionnelle a été documentée par les utilisateurs.

FICHE 13

Mise en production des évolutions applicatives

Catégorie	Contrôles généraux informatiques	**Domaine**	Autorisation, développement, test et approbation

Thème	Mise en production des changements applicatifs

Objectif

Les migrations, (applicatives et systèmes) ont fait l'objet d'une demande formelle de mise en production validée par la DSI. L'accès aux mises en production est suffisamment restreint et les changements significatifs donnent lieu à la mise à jour de la documentation applicative.

Exemples de bonnes pratiques

Une procédure de mise en production est formalisée.
Les migrations (applicatives et systèmes) ont fait l'objet d'une demande formelle de mise en production validée par le demandeur et par la DSI.
Les migrations en environnement de production sont automatiquement tracées et revues.
Un nombre limité de personnes a un accès à l'environnement de production et les habilitations en place permettent une correcte séparation des tâches.
Les changements significatifs donnent lieu à la mise à jour des documentations du SI (documentations techniques, manuels utilisateurs…).

Documentation à préparer

Procédure de mise en production
Demandes et validations des mises en production survenues sur l'exercice

Eléments à préparer

Formalisation	Les procédures et méthodologies de gestion des changements applicatifs sont disponibles et traitent notamment de la mise en production des changements
Mise en œuvre	La procédure de mise en production existe et est à jour. Les rôles et les tâches attribués à la maîtrise d'ouvrage, aux études et à l'exploitation sont définis. Il existe une demande et un compte rendu d'intervention pour chaque mise en production. Chaque mise en production est tracée et une revue par la direction des mises en production est réalisée. Il existe une fiche de test validée pour chaque mise en production réalisée. Il a été défini une liste des utilisateurs avec accès à l'environnement de production et une liste des utilisateurs avec accès à l'environnement de développement. Le département études ne dispose pas d'accès à l'environnement de production.

FICHE 14

Changements applicatifs en urgence

Catégorie	Contrôles généraux informatiques	Domaine	Changements urgents

Thème	Changements applicatifs en urgence

Objectif

Les changements applicatifs en urgence suivent une procédure permettant le suivi, la validation et la documentation *a posteriori* des évolutions apportées.

Exemples de bonnes pratiques

Une procédure est définie pour les changements en urgence
- suivi,
- tests,
- validation d'un responsable pour le changement,
- documentation.

Les modifications réalisées directement en production sont exceptionnelles et font l'objet d'une procédure particulière intégrant des contrôles visant à limiter le risque d'instabilité de l'application.
Une procédure établissant les règles à suivre lors d'une modification de paramétrage (applicatif/système) directement en production ("à chaud") est formalisée et suivie.

Documentation à préparer

Procédure de gestion des changements en urgence.
Liste de suivi des changements en urgence.
Documentation de test et validation des changements en urgence.

Eléments à préparer

Formalisation	Consulter les procédures et méthodologies de gestion des changements applicatifs disponibles et notamment le paragraphe traitant de la mise en production des évolutions applicatives.
Mise en œuvre	La procédure de gestion des changements en urgence est formalisée. Il existe une liste (un fichier de suivi/une copie d'écran de l'application) de suivi des changements en urgence. Tout changement en urgence est documenté et fait l'objet de tests de validation. Les changements en urgence restent exceptionnels et suivent des critères définis. La procédure de gestion des modifications directement en production est formalisée et la liste des modifications effectuées directement en production est tracée et les modifications sont validées par les responsables appropriés (conformément à la procédure).

FICHE 15

Approbation des développements/acquisitions

Catégorie	Contrôles généraux informatiques	**Domaine**	Conception, développement, test, approbation et implémentations des développements /acquisitions

Thème	Approbation des développements/acquisitions

Objectif
Une procédure de gestion des développements et acquisitions est définie et appliquée. Les projets de développement/acquisition d'applications, y compris leur infrastructure, sont tracés et approuvés par les personnes ou organes décisionnels habilités.
Exemples de bonnes pratiques
Une procédure de gestion des développements et acquisitions est définie et appliquée. La méthodologie prévoit que la DSI et les services concernés sont associés aux différentes étapes du projet. La méthodologie inclut notamment la documentation des développements et une stratégie de test (unitaire, non régression, d'intégration). La méthodologie doit également intégrer la prise en compte des contraintes définies par le contrôle interne en termes par exemple de restriction d'accès aux applications concernées. La documentation de gestion du projet définissant le périmètre, les besoins et le coût, est préparée pour les projets jugés significatifs et est revue et validée par la DSI et les services concernés.

Documentation à préparer
Méthodologie de gestion de projet (type plan d'assurance qualité) Procédure d'acquisition Liste des demandes de développements (O/S, base de données, applicatifs) et des principales acquisitions informatiques de l'exercice (software, hardware, etc.) Validations de la DSI (sur papier, compte rendu de réunion ou comité…) Comptes rendus de projet/documentation de suivi Documentation de tests et validation utilisateurs Document de spécification pour les achats et d'analyse préalable pour les développements.

Eléments à préparer	
Formalisation	Les procédures et méthodologies de gestion des développements et acquisitions existent et sont formalisées.
Mise en œuvre	La procédure de gestion des développements et acquisitions est formalisée. Il existe des spécifications générales pour les projets de tout type. Les demandes d'évolution sont validées par la DSI et/ou le responsable de service concerné.

FICHE 16

Accès et revue des traitements d'exploitation

Catégorie	Contrôles généraux informatiques	Domaine	Traitements automatisés

Thème	Accès et revue des traitements d'exploitation

Objectif

Une procédure de gestion des traitements automatisés est définie et formalisée.
Cette procédure définit les modalités d'accès et de revues des traitements automatisés.

Exemples de bonnes pratiques

Accès aux traitements d'exploitation
La DSI accorde la possibilité de modifier le programmateur de travaux ("job scheduler"), les traitements batch et les interfaces automatiques sur la base d'une autorisation formelle.
La liste des personnes disposant d'un accès aux programmateurs de travaux est revue périodiquement par la DSI (à minima annuellement).
Revue des traitements d'exploitation
L'exécution des traitements automatiques (batch, interface, sauvegarde...) est revue quotidiennement,
Les incidents de traitements sont tracés via l'outil de suivi des incidents, revus par le service exploitation et corrigés,
La DSI réalise une revue régulière du statut des incidents relatifs aux traitements d'exploitation qui ne sont pas résolus.

Documentation à préparer

Procédure d'exploitation
Liste des traitements d'exploitation
Documentation justifiant de la revue quotidienne des traitements d'exploitation

Eléments à préparer	
Formalisation	Les procédures et méthodologies de gestion d'exploitation sont disponibles et traitent notamment de la gestion des traitements automatisés.
Mise en œuvre	La procédure d'exploitation est formalisée et détaille les principaux traitements et les procédures de lancement associées. Une liste des utilisateurs pouvant accédant aux programmateurs de travaux a été validée par la DSI. Pour les nouveaux utilisateurs, les formulaires de demandes d'accès au programmateur de travaux sont validés par la DSI. Les traitements automatisés sont revus quotidiennement et les anomalies identifiées donnent lieu à l'ouverture d'un ticket d'incident.
Mise en œuvre	La procédure de gestion des développements et acquisitions est formalisée. Il existe des spécifications générales pour les projets de tout type. Les demandes d'évolution sont validées par la DSI et/ou le responsable de service concerné.

FICHE 17

Stratégie de sauvegarde

Catégorie	Contrôles généraux informatiques	**Domaine**	Sauvegardes et restaurations
Thème	Stratégie de sauvegarde		

Objectif

Une stratégie de sauvegarde des applications clés est définie, incluant les besoins en sauvegarde (fréquence), les besoins pour la restauration et la période de rétention des données.

Exemples de bonnes pratiques

Une procédure de sauvegarde des données du périmètre d'audit est formalisée, incluant les besoins en sauvegarde, les besoins pour la restauration et la période de rétention des données.

Stockage

Des mesures de restriction d'accès et de protection des supports de sauvegarde stockés sur site ont été mises en place,

Un jeu de supports de sauvegarde est conservé à l'extérieur de l'établissement et dans des conditions de stockage appropriées.

Fréquence

Les sauvegardes sont réalisées au moins 1 fois par jour. Le bon déroulement des sauvegardes est contrôlé quotidiennement (suivi de log, rapports d'anomalies…).

Rotation et rétention

Le nombre de supports de sauvegardes en rotation doit permettre la réalisation des sauvegardes sur des supports distincts pour chaque jour de la semaine. Des supports doivent être régulièrement prélevés afin de permettre une rétention des données en phase avec les besoins métiers.

Contenu

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

Remplacement des bandes

Le remplacement des bandes doit se faire en fonction des recommandations du constructeur (basé sur la moyenne des temps entre 2 pannes)

A défaut il doit être réalisé au minimum tous les ans.

Listing

Un listing des bandes doit être réalisé. Le nommage des bandes doit permettre de connaître le contenu de chaque bande.

Il doit être possible de façon simple de savoir sur quelle bande trouver par exemple les sauvegardes de l'application comptable du jeudi précédent.

Documentation à préparer

Procédure de sauvegarde
Logs de sauvegarde
Documentation justifiant de la revue quotidienne des sauvegardes
Document de suivi des bandes
Copies d'écran du logiciel de gestion des sauvegardes

Eléments à préparer	
Formalisation	Les procédures et méthodologies de gestion d'exploitation détaillent la gestion des sauvegardes.
Mise en œuvre	La procédure de sauvegarde définit les besoins en sauvegarde, pour la restauration ainsi que les périodes de rétentions des données pour les applications concernées. Les sauvegardes sont effectuées en conformité avec les besoins métiers. Les bandes de sauvegardes font l'objet d'un remplacement régulier et sont stockées dans un lieu sécurisé (accès, incendie, inondation…) ou externalisées. La rotation des bandes de sauvegardes est adaptée.

FICHE 18

Restauration des sauvegardes

Catégorie	Contrôles généraux informatiques	Domaine	Sauvegardes et restaurations

Thème	Restauration des sauvegardes

Objectif
Une procédure de restauration des sauvegardes est en place et des tests périodiques sont réalisés.

Exemples de bonnes pratiques
Une périodicité minimale doit être définie et appliquée pour les tests de restauration. Les tests de restauration effectués à l'initiative des utilisateurs finaux (par exemple demande de réplication du système de production sur le système de test) ou du personnel informatique doivent être globaux, c'est-à-dire inclure à la fois les données, les programmes et les données systèmes de l'environnement informatique restauré. La fréquence des tests de restauration doit être annuelle au minimum. Les tests de restauration doivent être validés par des représentants "Métiers" afin de s'assurer du correct fonctionnement du système restauré à partir des bandes de sauvegarde.

Documentation à préparer
Dernier test global de restauration des sauvegardes

Eléments à préparer	
Formalisation	Les procédures et méthodologies de gestion d'exploitation détaillent les opérations relatives à la restauration des sauvegardes.
Mise en œuvre	Un test global de restauration des sauvegardes est régulièrement réalisé impliquant DSI et services. Le dernier qui a moins d'un an a été documenté et archivé. Pour l'ensemble des anomalies identifiées : - un plan d'action a été mis en place, - les corrections ont été apportées dans un délai raisonnable, - les sauvegardes en défaut ont été à nouveau testées, aucune nouvelle anomalie n'a été identifiée.

FICHE 19

Gestion des incidents

Catégorie	Contrôles généraux informatiques	**Domaine**	Procédures de gestion des problèmes et des incidents

Thème	Gestion des incidents

Objectif

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

Exemples de bonnes pratiques

Une procédure de gestion des incidents est définie et formalisée. Cette procédure définit les moyens de suivi (acteurs, outils), les indicateurs de criticité, les dispositifs d'escalade.
Chaque incident, incluant ceux déclarés par les utilisateurs, est documenté via un outil de suivi des incidents et fait l'objet d'une analyse ainsi que d'un plan d'actions jusqu'à sa résolution.
La direction réalise une revue régulière du statut des incidents qui ne sont pas résolus et prend les mesures nécessaires pour solutionner les points de blocage.

Documentation à préparer

Liste des incidents de l'exercice à partir de l'outil de suivi des incidents
Statistiques de résolution des incidents
Rapport de traitement des incidents par un tiers (cas de TMA)

Eléments à préparer

Formalisation	Les procédures et méthodologies de gestion d'exploitation détaillent la gestion des incidents.
Mise en œuvre	Un outil de suivi des incidents est en place et permet de recenser et tracer les évènements indésirables. Les incidents sont documentés, suivis, résolus et clôturés dans un intervalle de temps conforme aux engagements du service informatique (SLA) vis-à-vis des services.

ANNEXES

ANNEXE 1

RAPPEL DES NORMES PROFESSIONNELLES ET DES OBLIGATIONS DU COMMISSAIRE AUX COMPTES

La certification des comptes implique un contrôle externe, c'est-à-dire un audit. L'audit des états financiers consiste en un examen de ces états dans leur ensemble par un auditeur indépendant qui émet une opinion sur l'application correcte des principes comptables et le respect de la législation en vigueur dans la préparation, la confection et la présentation de ces états financiers (selon le décret n° 2010-425 du 29 avril 2010 qui a modifié l'article R. 6145-43 pour définir plus précisément les états composant le compte financier, en distinguant notamment les comptes annuels qui constitueront les seuls états soumis à certification), en vue de donner une image fidèle de la situation financière et des résultats de l'établissement.

Le commissariat aux comptes, ou contrôle légal des comptes selon la terminologie européenne, est une profession réglementée et indépendante qui contribue à la qualité et à la transparence de l'information financière et comptable émise par les entités contrôlées.

L'article L. 823-9 du code de commerce précise que « Les commissaires aux comptes certifient, en justifiant de leurs appréciations, que les comptes annuels sont réguliers et sincères et donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de la situation financière et du patrimoine de la personne ou de l'entité à la fin de cet exercice. »

Par appréciation de la sincérité et de la régularité des comptes, il est entendu les notions suivantes :

– régularité : conformité des comptes avec les règles d'évaluation et de présentation ;
– sincérité : loyauté et bonne foi dans l'établissement des comptes.

Dans le cadre des établissements de santé, le cadre applicable est défini par l'instruction budgétaire et comptable M21 et l'avis du Conseil de normalisation des comptes publics (CNoCP).

Le rôle des commissaires aux comptes est très encadré et s'appuie sur un certain nombre de principes fondamentaux, parmi lesquels :

– il est indépendant, extérieur à l'établissement, mais rémunéré par elle ;
– il prête serment devant la cour d'appel ;
– il est tenu au secret professionnel ;
– il a une déontologie stricte ;
– il engage sa responsabilité civile, pénale et disciplinaire ;
– le certificateur est rattaché au ministère de la justice ;
– il est nommé par l'organe délibérant de l'entité pour une durée de six exercices, soit en vertu d'une obligation légale, soit sur une base volontaire.

Les missions exercées par le commissaire aux comptes dans les entreprises et les structures des secteurs associatif, syndical et public reposent donc sur une obligation légale. Dans cet esprit, pour former son opinion sur les comptes, le commissaire aux comptes procède à un audit en appliquant les normes d'exercice professionnel (NEP) homologuées par le garde des sceaux, après avis du Haut Conseil du commissariat aux comptes (H3C) et sur proposition de la Compagnie nationale des commissaires aux comptes (CNCC). Celles-ci sont en harmonie avec les normes internationales (IFAC pour *International Federation of Accountants*). Depuis le 1er mai 2007, les normes d'exercice professionnel homologuées se sont substituées aux anciennes normes du recueil de la CNCC, paru en 2000 et mis à jour en juillet 2003. La publication des NEP au *Journal officiel* leur confère de fait force de loi : l'application des NEP est opposable tant vis-à-vis des commissaires aux comptes que des entités auditées.

Pour les sujets non couverts par les normes d'exercice professionnel homologuées, les anciennes normes du recueil de la CNCC de juillet 2003 constituent un référentiel de bonnes pratiques concourant à la bonne information des professionnels.

L'environnement des entités contrôlées s'appuie de façon quasi systématique sur des systèmes d'informations (SI) de plus en plus complexes, étendus et intégrés. Dans cet esprit, les normes professionnelles impliquent une prise en compte des systèmes d'information. Parmi les normes relatives à la mission d'audit, celles qui traitent de « l'appréciation du contrôle interne » sont principalement :

– NEP-315. Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives dans les comptes ;
– NEP-330. Procédures d'audit mises en œuvre par le certificateur à l'issue de son évaluation des risques.

GLOSSAIRE

TERME	DÉFINITION
AFNOR	L'Association française de normalisation (AFNOR) est l'organisme officiel français de normalisation, membre de l'Organisation internationale de normalisation (ISO) auprès de laquelle elle représente la France.
ARS	Agence régionale de santé.
CME	Commission médicale d'établissement.
CNCC	Compagnie nationale des commissaires aux comptes.
CNoCP	Conseil de normalisation des comptes publics.
COBIT	Control objectives for information and related technology – Objectifs de contrôle de l'information et des technologies associées, outil fédérateur permettant d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information. Le référentiel COBIT a été développé en 1994 (et publié en 1996) par l'ISACA (information systems audit and control association). L'ISACA a été créé en 1967 et est représenté en France depuis 1982 par l'AFAI (association française de l'audit et du conseil informatiques). C'est un cadre de contrôle qui vise à aider le management à gérer les risques (sécurité, fiabilité, conformité) et les investissements. Le référentiel COBIT est une approche orientée processus, qui regroupe en quatre domaines (planification, construction, exécution et métrologie), les principaux processus, activités et pratiques de contrôle.
COSO	Référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission.
DGFiP	Direction générale des finances publiques.
DGOS	Direction générale de l'offre de soins.
DPI	Dossier patient informatisé, dossier regroupant l'ensemble des données médicales d'un patient.
DSI(O)	Direction des systèmes d'information (et de l'organisation).
FIDES	Facturation individuelle des établissements de santé.
GAM	Gestion administrative du malade.
GCS	Groupement de coopération sanitaire.
GEF	Gestion économique et financière.
GRH	Gestion des ressources humaines.
HAS	Haute Autorité de santé.
Hotline	Anglicisme désignant un centre d'assistance chargé de répondre aux demandes d'assistance émanant des utilisateurs de produits ou de services.
IFAC	International Federation of Accountants, organisation professionnelle internationale ayant pour objectif la publication de normes internationales dans un esprit de convergence des normes professionnelles.
ISAE	Norme d'assurance globale souvent désignée par son sigle anglais ISAE (International Standards for Assurance Engagements).
ISO	L'Organisation internationale de normalisation (International Organization for Standardization), ou ISO, est un organisme de normalisation international.
IT	Le terme anglais IT (Information Technologies) désigne les notions de technologies de l'information et de la communication. Il pourra également se traduire par le terme « informatique ».
ITIL	ITIL (Information Technology Infrastructure Library) est constitué d'un ensemble de bonnes pratiques du management du système d'information. L'adoption des bonnes pratiques de l'ITIL ont notamment pour objectif : – d'apporter aux clients (internes comme externes) un service répondant à des normes de qualité préétablies au niveau international, basées sur une approche par processus clairement définie et contrôlée ; – d'améliorer la qualité des SI et de l'assistance aux utilisateurs.
MOE	Le terme maîtrise d'œuvre (souvent abrégé MOE ou MŒ ou ME) désigne une personne ou entité chargée de la conduite opérationnelle de travaux.

TERME	DÉFINITION
MSIOS	Mission systèmes d'information des acteurs de l'offre de soins.
MTBF	Temps moyen entre pannes, expression souvent désignée par son sigle anglais MTBF (mean time between failures), est une des valeurs qui indiquent la fiabilité d'un composant d'un produit ou d'un système. C'est la moyenne arithmétique du temps entre les pannes d'un système réparable.
NEP	Normes d'exercice professionnel.
OS	OS est un sigle anglais pouvant désigner Operating System, il sera traduit en français par « système d'exploitation ».
PES V2	Le protocole d'échange standard d'Hélios version 2 (PES V2) est la solution de dématérialisation des titres de recette, des mandats de dépense et des bordereaux récapitulatifs.
PMSI	Programme de médicalisation des systèmes d'information.
PRA	Un plan de reprise d'activité permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.
RACI	RACI dans le management représente une matrice des responsabilités qui indique les rôles et les responsabilités des intervenants au sein de chaque processus et activité.
RSSI	Responsable de la sécurité des systèmes d'information.
SI(H)	Système d'information (hospitalier).
SLA	Service level agreement ou accord sur les niveaux de service.
SOX	Aux États-Unis, la loi de 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs est une loi fédérale imposant de nouvelles règles sur la comptabilité et la transparence financière. Le texte est couramment appelé loi Sarbanes-Oxley, du nom de ses promoteurs, le sénateur Paul Sarbanes et le député Mike Oxley. Ce nom peut être abrégé en SOX, Sarbox, ou SOA.
TMA	La tierce maintenance applicative est la maintenance appliquée à un logiciel (« applicative ») et assurée par une expertise externe dans le domaine des technologies de l'information et de la communication.
Unix	Système d'exploitation multitâche et multiutilisateur créé en 1969.