Guide d'audit des systèmes d'information

CHAI
Comité d'harmonisation de l'audit interne

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Guide pratique du CHAI

Parmi les thèmes d'audit abordés dans ce guide :

Version 1.0 – juin 2014

Précaution concernant l'utilisation du présent document

Le présent guide a été élaboré par un groupe de travail interministériel, sous l'égide du Comité d'harmonisation de l'audit interne (CHAI). Il est le fruit de plusieurs mois de travaux collectifs, de partage d'expériences et de mise en commun des meilleures pratiques ayant cours dans les corps de contrôle ou les missions ministérielles d'audit interne. Son objet est au premier chef de faciliter l'harmonisation de la méthodologie de travail des auditeurs internes et il se rapporte à ce titre à la partie « dispositions recommandées » du cadre de référence de l'audit interne de l'Etat.

Ce document est une première version, actuellement en cours d'expérimentation par les praticiens de l'audit interne en fonction dans les différents ministères.

L'attention du lecteur est appelée sur le fait que, même une fois devenu définitif, le présent guide ne pourra en aucun cas être considéré comme le seul référentiel à la lumière duquel les auditeurs auront à former leur opinion globale et porter leur jugement professionnel dans le domaine considéré.

Ce document a été produit **dans le cadre d'un groupe de travail du Comité d'harmonisation de l'audit interne (CHAI)** animé par Marcel **DAVID** (CGA) composé de :

- Anne **AUBURTIN** (IGAS),
- Patrick **BADARD** (SAE),
- Simon **BARRY** (CGEFI),
- Philippe **BELLOSTA** (DGFIP),
- Pierre **BOURGEOIS** (IGA),
- Luc **CHARRIÉ** (CHAI),
- Jean-Pierre **DALLE** (IGA),
- Nicole **DARRAS** (CGEDD),
- Rémy **MAZZOCCHI** (DISIC),
- Hervé **PEREZ** (CHAI),
- Philippe **PERREY** (IGAENR),
- Jean-François **PICQ** (IGAENR),
- Clément **REMARS** (CGA).

SOMMAIRE

INTRODUCTION

L'essentiel des travaux d'audit relatifs au système d'information ne nécessite pas de connaissances très approfondies en informatique mais une bonne maîtrise des pratiques d'audit.

Ce guide s'adresse toutefois à des auditeurs *a minima* avertis, c'est-à-dire ayant suivi une session de sensibilisation ou ayant déjà effectué une ou deux missions d'audit dans le domaine en compagnie d'un auditeur spécialisé dans le domaine des SI. La sensibilisation pourra, notamment, s'appuyer sur des guides de formation mis à disposition par le CHAI.

Il propose dans une première partie une information générale sur les facteurs clés permettant d'améliorer la performance de la fonction et du système informatique, en les articulant avec les principaux risques du domaine.

Il décrit en deuxième partie, d'une part, la dimension informatique des principaux audits généralistes (audit en organisation, audits de processus, etc.) et, d'autre part, les aspects plus généraux des audits visant spécifiquement le domaine SI (audits d'application, de la sécurité informatique, des projets, etc.).

Il présente en troisième partie les points à aborder en fonction de l'aspect audité. Ainsi, pour chaque thème, l'auditeur sera renvoyé à un tableau identifiant les principaux points de contrôle correspondant. Ce tableau doit permettre à un auditeur non spécialiste des SI de percevoir le contenu d'un thème d'audit donné, et à un auditeur spécialisé de ne rien oublier.

Cependant, ce guide est orienté vers l'audit de structures de taille conséquente. L'auditeur devra évidemment adapter son approche et ses attentes à la taille et aux moyens de l'organisation auditée, en particulier dans l'utilisation de cette troisième partie.

Enfin, un dictionnaire permet de revenir sur certaines notions fréquemment rencontrées lors d'un audit SI. Il est tout particulièrement important de veiller à la clarté des termes et notions utilisés dans les documents contractuels.

En complément de ce guide, il est à noter que les auditeurs ministériels peuvent s'appuyer en matière d'audit des SI sur la direction des systèmes d'information et de communication de l'État (DISIC). La maîtrise des risques qui s'attachent au SI de l'État et à ses grands projets informatiques est, en effet, l'une de ses missions essentielles.

1. LES SYSTEMES INFORMATIQUES : ENJEUX ET RISQUES

1.1. LE SYSTEME INFORMATIQUE

1.1.1. DEFINITION

Le *système informatique*, appelé aussi *système d'information*, (noté SI) représente l'ensemble des logiciels et matériels participant au stockage, à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation.

La *fonction informatique* vise à fournir à ces ressources l'organisation. Elle comprend donc, outre le système informatique, les personnes, processus, ressources financières et informationnelles qui y contribuent.

Elle ne doit pas être confondue avec la *fonction d'information*, ensemble organisé de personnes, de procédures et d'équipement qui a pour objet de réunir, de trier, d'analyser, d'évaluer et de distribuer, en temps utile, de l'information pertinente et valide, provenant de sources internes et externes à l'organisation, afin que tous ceux qui ont à prendre des décisions disposent des éléments leur permettant de choisir l'action la plus appropriée au moment adéquat.
La fonction d'information, qui doit être pensée comme telle et non comme une émanation de la fonction informatique, s'appuie évidemment sur des ressources informatiques. En raison de la confusion fréquente entre ces notions, les commanditaires attendent parfois des auditeurs SI un travail sur la fonction d'information plus que sur le seul système informatique. Il convient donc d'être très clair sur les attendus de l'audit.

Un système informatique est constitué de ressources matérielles et logicielles organisées pour collecter, stocker, traiter et communiquer les informations. Les ressources humaines nécessaires à son fonctionnement (par exemple les administrateurs) sont parfois incluses dans ce périmètre.

Le système informatique ne doit pas être conçu comme une fin en soi : il est l'un des outils qui permet à l'organisation d'atteindre ses objectifs. Il ne se justifie qu'en tant qu'il soutient des processus « métier », sans lesquels il n'a aucun sens. Il doit donc être aligné avec les objectifs stratégiques de l'organisation. Cet *alignement stratégique* est fondamental : désormais, un système informatique est un facteur déterminant de la performance (efficacité, efficience, maîtrise des risques) d'une organisation. Inversement, un système informatique inadapté ou mal maîtrisé peut être une source inépuisable de difficultés.

Les développements suivants exposent, de manière synthétique, les principaux facteurs clés de la performance du SI et les risques spécifiques qui pèsent sur son fonctionnement.

1.1.1.1. LA PERFORMANCE DU SI DE L'ÉTAT

Le développement de services pertinents pour le citoyen et l'entreprise, la modernisation des outils mis à disposition des agents, l'ouverture des données publiques au profit d'une meilleure transparence et de l'innovation doivent s'appuyer sur des systèmes d'information performants. C'est pourquoi le Premier Ministre a validé et diffusé par circulaire, le 7 mars 2013, le cadre stratégique commun du système d'information de l'État élaboré par la direction interministérielle des systèmes d'information et de communication (DISIC).

Ce cadre stratégique commun du SI de l'État fixe une ambition commune portée par les systèmes d'information ministériels et interministériels. Cette ambition se décline en trois axes stratégiques :

1. Le SI doit créer une valeur croissante pour ses utilisateurs. À cet effet, les directions métiers doivent mieux s'appuyer sur les systèmes d'information pour optimiser les processus de fonctionnement de l'administration, augmenter la performance de celle-ci et la qualité du service rendu par les agents publics. Le système d'information doit être mieux structuré et utilisé pour développer les relations numériques entre les métiers et les usagers.

2. Le SI de l'État doit être construit de façon efficiente. Parallèlement aux investissements d''innovation qui créent de la valeur pour les utilisateurs du SI de l'État, les coûts non justifiés des composantes de ce SI doivent être réduits.

3. La fonction SI de l'État doit être pilotée. Les visions ministérielles des SI, et particulièrement leur alignement avec la stratégie des métiers, doivent s'appuyer sur une vision transversale du système d'information de l'État afin de concilier enjeux métiers et enjeux globaux des politiques publiques. En particulier, certains enjeux d'organisation et de politique publique de long terme constituent des chantiers essentiels pour la réussite de l'évolution du système d'information de l'État, au-delà de visions trop locales ou ministérielles.

L'urbanisation du SI de l'État est l'outil pour le pilotage du patrimoine SI et une aide à la décision pour toutes les actions de transformation. Le cadre commun d'urbanisation (CCU) du SI de l'État constitue un des éléments du corpus réglementaire applicable pour la construction, la gestion, l'exploitation et la transformation du SI de l'État, à tous les niveaux. Ce corpus se compose de documents de politique globale applicables à l'ensemble du SI de l'État :

- le cadre stratégique, qui définit la stratégie de l'État en matière de SI,
- la politique de sécurité, définissant les règles générales de sécurité,
- le cadre commun d'urbanisation définissant la démarche d'urbanisation,
- le cadre commun d'interopérabilité.

Ce corpus comprend également des documents réglementaires techniques à portée plus large (administrations de l'État, collectivités territoriales, organismes de la sphère sécurité et protection sociale), définis par l'ordonnance n°2005-1516 du 8 décembre 2005 :

- le référentiel général d'interopérabilité,
- le référentiel général de sécurité,
- le référentiel général d'accessibilité pour l'administration.

Il comprend également des documents à portée ministérielle :

- un cadre stratégique ministériel (ou schéma directeur), déclinant le cadre stratégique du SI de l'État, dans le contexte métier d'un ministère ;
- un cadre de cohérence technique : normes, standards et règles d'architecture applicables localement ;

- une méthode de conduite de projet qui définit et structure les relations maîtrise d'ouvrage (MOA) et maîtrise d'œuvre (MOE) et le pilotage des projets de transformation du SI pour un ministère (ou une administration) ;

Il comprend éventuellement une charte d'urbanisation qui décline localement le cadre commun d'urbanisation, sans pour autant modifier les principes, ou le cadre d'activité, mais uniquement en précisant l'organisation, les méthodes de travail et le fonctionnement local.

1.1.1.2. LES FACTEURS CLEFS D'UN SI PERFORMANT

Un SI idéal :

- est en adéquation avec la stratégie de l'organisation et les objectifs des métiers ;
- est en conformité avec les obligations légales ;
- est sécurisé ;
- est facile à utiliser ;
- est fiable ;
- est adaptatif ;
- est pérenne ;
- est disponible ;
- est efficient ;
- respecte le plan d'urbanisme ;
- quand il fait l'objet de marchés, est conforme aux bonnes pratiques de la commande publique.

Les principaux facteurs clefs d'un SI performant sont les suivants :

- une forte implication de la direction dans la gestion du SI. Elle doit notamment superviser la gestion du SI par la mise en place des outils de pilotage suivants :
  - un schéma directeur informatique (SDI), qui définit la stratégie informatique pluriannuelle, dont la validation par la direction entérine l'adéquation entre la stratégie informatique et la stratégie de l'entité ;
  - des documents d'organisation de la gouvernance du SI, mis à jour régulièrement ;
  - des comités de pilotage informatiques réguliers (suivi des incidents, suivi des projets, suivi des budgets, etc.), au sein desquels la direction doit être représentée à bon niveau ;
  - des tableaux de bord de suivi de l'informatique ;
  - un portefeuille des projets SI et des analyses de la valeur des systèmes d'information ;
  - une politique de sécurité (voir ci-après), approuvée au plus haut niveau de la direction ;
  - des comités de sécurité réguliers, au sein desquels la direction doit être représentée à bon niveau ;
  - une cartographie des applications et systèmes informatiques à jour, incluse dans une politique

d'urbanisme informatique. Cette cartographie est fondamentale pour les auditeurs, les certificateurs ou tout autre organisme de contrôle.

- une politique de sécurité, qui doit être validée et soutenue par la direction de l'entité :
    - la politique de sécurité des systèmes d'information (PSSI) constitue le principal document de référence en matière de sécurité des systèmes d'information (SSI). Elle reflète la vision stratégique de l'entité et montre l'importance qu'accorde la direction à la sécurité de son SI ;

    - elle se matérialise par un document présentant, de manière ordonnée, les règles de sécurité à appliquer et à respecter dans l'organisme. Ces règles sont généralement issues d'une étude des risques SSI ;

    - après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires…). Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir ;

    - la PSSI est un document vivant qui doit évoluer afin de prendre en compte les transformations du contexte de l'organisme (changement d'organisation, de missions...) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux) ;

    - idéalement, il devrait exister une charte d'utilisation du système d'information, dans le but de sensibiliser les utilisateurs à la sécurité informatique, informer les utilisateurs des responsabilités qui leur incombent. Pour une meilleure efficacité, cette charte devrait être signée par tous les agents et une communication régulière sur le sujet devrait être mise en place avec le support de la direction. Cette charte contiendrait par exemple les règles de sécurité et de bon usage (protection du PC, mots de passe, confidentialité, utilisation d'Internet, de la messagerie, protection du PC, etc.), les normes relatives aux logiciels (installation, licences, etc.), une description de la traçabilité des actions sur le SI à laquelle chaque utilisateur est assujetti et les sanctions applicables en cas de non-respect des règles décrites.

- le respect de la législation en matière de système d'information :
    - la législation ne peut être appréciée en termes uniquement de contrainte. La mise en conformité du SI permet de garantir de façon raisonnable un environnement de contrôle satisfaisant de son SI ;

    - les principaux textes applicables sont la loi de sécurité financière (LSF), avec un volet informatique puisque l'objectif est de renforcer la fiabilité des informations financières des entreprises mais aussi le contrôle interne sur les aspects opérationnels (de même que la loi Sarbanes-Oxley aux États-Unis mais uniquement sur les aspects financiers) ;

    - en France, la loi de finances sur le contrôle des comptabilités informatisées (votée en 1991 puis complétée en 1996 et 2006) contribue à la justification informatique de la piste d'audit ;

- la déclaration CNIL a, en revanche, un objectif différent puisqu'elle sert à protéger les données personnelles des individus, manipulées dans les applications informatiques.

- le respect des bonnes pratiques en matière de commande publique :
  - l'achat de prestations ou de logiciels est un acte complexe, qui suppose une excellente coopération entre les opérationnels et les services acheteurs. La possibilité de recourir au « sur-mesure », plus fréquente que pour d'autres types d'achats, impose en contrepartie une rigueur particulière s'agissant des spécifications, des procédures de passation et de réception et du pilotage des assistances à la MOA ou à la MOE ;

  - cette complexité rend d'autant plus important le respect du code des marchés publics et des guides de bonnes pratiques rédigés par le SAE, et ce, quelle que soit la méthode de développement utilisée. Contrairement à ce que l'on entend parfois, les dispositions encadrant la commande publique sont, en effet, adaptées au domaine informatique, y compris à la méthode agile, et leur application rigoureuse et sincère peut éviter nombre de déconvenues.

- un paramétrage correct des droits d'accès aux applications informatiques :
  - les droits d'accès au SI doivent refléter les règles de séparation des tâches telles que définies dans l'organisation ;

  - au niveau informatique, les développeurs ne peuvent pas avoir accès à l'environnement de production et le personnel d'exploitation ne peut pas avoir accès à l'environnement de développement. Par ailleurs, l'attribution de droits très élevés (« administrateurs ») doit être limitée et toute action de ces profils « sensibles » doit être tracée et revue régulièrement ;

  - au niveau des applications informatiques, les droits d'accès attribués doivent traduire de façon informatique les rôles de chacun dans l'organisation. Chaque agent n'a accès qu'aux applications qui le concernent dans sa fonction, et à l'intérieur des applications, il existe des restrictions au niveau de chaque fonctionnalité, voire au niveau des données ;

  - les droits d'accès doivent faire l'objet d'une gestion rigoureuse, par un service dédié. Ainsi, les demandes d'octroi de droit d'accès doivent être formalisées et obligatoirement validées par les chefs de service. Les déblocages en cas de perte de mot de passe doivent être organisés. Enfin, la liste des habilitations, application par application, doit être revue régulièrement, et les droits d'accès supprimés en cas de départ.

- une bonne gestion des projets de développements informatiques. La réussite d'un projet informatique nécessite *a minima* les éléments suivants :
  - une vision claire de l'objectif et des résultats attendus ;

  - l'implication de la direction générale ;

- une définition claire des responsabilités des parties prenantes ;
- l'implication des utilisateurs (« bureaux métiers ») ;
- la constitution d'une équipe projet dédiée dirigée par des cadres expérimentés ;
- des choix techniques pérennes ;
- une gestion rigoureuse et organisée du projet ;
- un déploiement échelonné ;
- un suivi des risques ;
- un accompagnement du changement.

- un SI intégré :
  - un SI est dit intégré quand toutes les applications communiquent entre elles de façon automatique à l'aide d'interfaces. Ainsi, les informations ne sont saisies qu'une seule fois dans les systèmes (notion de base de données maîtresse) et les échanges de données font l'objet de contrôles d'intégrité automatiques. L'action humaine, source potentielle d'erreurs ou de fraude, est donc très limitée.
  - par ailleurs, la piste d'audit peut être entièrement informatisée.

  NB : Voir dans les risques informatiques, les progiciels de gestion intégrés

- une démarche qualité informatique : la mise en place d'une démarche qualité pour la gestion de la production et le développement informatique permet d'améliorer les performances du système d'information, de normaliser les procédures de gestion en fonction des référentiels existants et d'améliorer les compétences des acteurs du système d'information. Il existe en la matière de nombreux référentiels, dont les principaux sont les suivants :
  - **CMMI (Capability Maturity Model + Integration) pour les développements informatiques (avec plusieurs niveaux de certification de 1 à 5) ;**
  - **ITIL** (Information Technology Infrastructure Library) : plus spécifique à la gestion de la production informatique ;
  - **COBIT** (Control Objectives for Information and related Technology) : est un référentiel en matière de gouvernance informatique ;
  - **ISO 27001** (auparavant la BS7799) : présente les exigences en matière de sécurité informatique ;
  - le « guide des bonnes pratiques des achats de services informatiques » du service des achats de l'État (SAE) ;
  - les guides et recommandations sectorielles publiés par l'ANSSI et la DISIC ;
  - le cadre stratégique commun du SI de l'État et le cadre commun d'urbanisation ;
  - méthode MAREVA 2 d'analyse de la valeur des projets SI (Forum de la performance).

1.2. LES RISQUES INFORMATIQUES

1.2.1. GENERALITES

Les développements ci-dessous décrivent, pour chaque risque informatique, les principaux facteurs de risque et les contrôles ou procédures qui doivent être mis en place pour prévenir, réduire voire supprimer ce risque.

Pour mémoire, l'externalisation d'un service SI conduit à transférer les risques, sans pour autant les couvrir de manière certaine. En matière informatique, comme dans tous les autres domaines, l'externalisation d'un risque ne dispense ainsi pas une organisation de s'assurer qu'il est effectivement maîtrisé par son cocontractant et ne l'exonère en rien de sa responsabilité finale.

Les principaux risques informatiques peuvent être regroupés en 3 domaines :

- les risques opérationnels, qui sont les plus nombreux pour le sujet traité ;
- les risques financiers, puisque l'informatique et l'information sont des actifs ;
- les risques légaux de non-conformité, puisque les entités sont soumises à des normes internes et externes, certaines de portée légale, concernant la gestion du SI.

1.2.2. LES PRINCIPAUX RISQUES INFORMATIQUES

Les principaux risques, facteurs de risques et dispositifs ou moyens de contrôles des risques informatiques sont les suivants :

- **Inadéquation du SI avec la stratégie de l'entité et les besoins des utilisateurs**
  - Facteurs de risque :
    - manque d'implication de la direction dans la gestion de l'informatique ;
    - absence de schéma directeur ;
    - absence de gouvernance informatique ;
    - manque d'implication des utilisateurs (« bureaux métiers ») dans les projets informatiques ;
    - absence d'analyse de la valeur des SI mis en place.
  - Contrôles ou procédures attendus :
    - supervision de l'informatique par la direction de l'entité ;
    - existence d'une stratégie en adéquation avec la stratégie de l'organisation, traduite par exemple dans un schéma directeur informatique ;
    - gouvernance informatique en place et validée par la direction ;

- analyse de la valeur (par exemple par MAREVA 2) ;
- forte implication des utilisateurs (« bureaux métiers ») dans les projets informatiques.

- **Incapacité de l'organisation à redémarrer les systèmes informatiques en cas arrêt ou destruction**
  - Facteurs de risque :
    - absence de sauvegarde régulière du SI (sauvegardes externes) ;
    - absence de plan de secours ;
    - absence de site de secours.
  - Contrôles ou procédures attendus :
    - mise en place d'un plan de secours (documenté, mis à jour lors de modifications majeures de l'environnement informatique, et testé au moins une fois par an) ;
    - procédure de sauvegarde quotidienne des données et programmes critiques ;
    - stockage des sauvegardes à l'extérieur de l'entité ;
    - les sauvegardes doivent être testées régulièrement ;
    - lorsqu'une activité est fortement dépendante de l'informatique, mise en place d'un site de secours.

- **Sécurité du SI inadaptée au niveau de risque identifié et accepté par la direction**
  - Les facteurs de risque sont multiples car la sécurité est transversale à tous les processus de l'informatique :
    - sécurité physique ;
    - sécurité logique ;
    - sécurité du réseau ;
    - sécurité de l'exploitation ;
    - sécurité des PC ;
    - sécurité des données ;
    - etc.
  - Contrôles ou procédures attendus :
    - politique de sécurité en place, validée et supportée par la direction de l'entité ;
    - outils de surveillance du système informatique (par exemple supervision) ;
    - équipe sécurité dédiée recensant tous les incidents relatifs à la sécurité et capable d'intervenir en cas d'événement de sécurité.

- **Accès aux données et aux applications par des personnes non autorisées**
  - Facteurs de risque :
    - absence de politique de sécurité ;
    - absence de gestion rigoureuse d'attribution des droits d'accès ;
    - absence de gestion rigoureuse des points d'accès ;
    - systèmes informatiques ne permettant pas une gestion fine des droits d'accès ;
    - gestion des mots de passe insuffisante.
  - Contrôles ou procédures attendus :
    - politique de sécurité validée par la direction de l'entité ;
    - politique de gestion des mots de passe efficace ;
    - gestion rigoureuse des droits d'accès au système d'information en cohérence avec la séparation fonctionnelle des tâches ;
    - revue régulière de la liste des habilitations, application par application ;
    - revue régulière des points d'accès ;
    - séparation des tâches effective entre les fonctions développements et exploitation ;
    - supervision des profils sensibles alloués au personnel informatique ;
    - traçabilité des accès et actions sensibles.

- **Applications informatiques non fiables**
  - Facteurs de risque :
    - erreurs dans la programmation des applications par rapport aux spécifications fonctionnelles ;
    - applications insuffisamment testées ;
    - utilisateurs insuffisamment impliqués dans les phases de développements de l'application.
  - Contrôles ou procédures attendus :
    - forte implication des utilisateurs dans les développements informatiques ;
    - bonne gestion de projet ;
    - veille environnementale ;
    - procédures de recensement des anomalies ;
    - procédures de maintenances correctives, adaptatives et évolutives.

- **Indisponibilité du système informatique**
  - Facteurs de risque :
    - mauvaise gestion de l'environnement matériel du SI (énergie, climatisation, protection physique, etc.) ;
    - absence de convention de service ;
    - absence d'outil de surveillance de la disponibilité du SI ;
    - absence de cellule réactive en cas d'indisponibilité ;
    - absence de contrat de maintenance des matériels informatiques.
  - Contrôles ou procédures attendus :
    - convention de service entre l'informatique et les utilisateurs, portant notamment sur des objectifs de performance du SI, tels le niveau de disponibilité des serveurs ;
    - support utilisateur performant ;
    - procédure de gestion des anomalies ;
    - procédure de maintenance corrective des applications informatiques ;
    - contrats de maintenance des matériels informatiques ;
    - environnement matériel adapté ;
    - plans de continuité et de reprise de l'activité.

- **Mauvaise utilisation du SI par les utilisateurs**
  - Facteurs de risque :
    - applications informatiques non conviviales ;
    - utilisateurs insuffisamment formés ;
    - documentation utilisateur insuffisante et pas mise à jour ;
    - manque de contrôles bloquants dans les applications informatiques.
  - Contrôles ou procédures attendus :
    - applications faciles d'utilisation ;
    - formation initiale des utilisateurs réalisée en temps utile et complétée par une formation au fil de l'eau ;
    - documentation utilisateur complète et mise à jour régulièrement ;
    - contrôles bloquants dans les applications ;
    - procédures de gestion des maintenances évolutives, adaptatives et correctives.

- **SI non conforme avec la législation**
    - Les lois et décrets portant sur le renforcement des procédures de contrôles internes concernent pour partie l'informatique. Les actions à mettre en place font, pour la plupart, partie des recommandations déjà citées pour couvrir certains risques informatiques comme :
        - la politique de sécurité informatique ;
        - la documentation informatique à jour ;
        - la sécurité des développements informatiques ;
        - la gestion rigoureuse des droits d'accès au SI.
    - S'agissant des déclarations CNIL, il est recommandé qu'une personne soit spécifiquement désignée dans l'organisation pour gérer ce sujet et l'anticiper. Elle doit notamment sensibiliser sur le sujet les services en charge des développements informatiques.

- **SI non pérenne**
    - Facteurs de risque :
        - utilisation de la sous-traitance informatique sans transfert de compétence en interne ;
        - documentation informatique inexistante ou non mise à jour suite aux évolutions du SI ;
        - obsolescence de l'application et/ou de la technologie utilisée ;
        - forte dépendance vis-à-vis de personnes clés qui peuvent quitter l'entité.
    - Contrôles ou procédures attendus :
        - le SI doit faire l'objet d'un schéma directeur informatique ;
        - la documentation informatique doit être complète et à jour, notamment dans un contexte de forte utilisation de la sous-traitance ou d'applications anciennes ;
        - des procédures de transfert de compétence entre les sous-traitants et les équipes informatiques internes doivent être mises en place.

Les progiciels de gestion intégrés (PGI) constituent un cas particulier, porteurs d'avantages, d'inconvénients et de risques spécifiques.
Les PGI (*Entreprise Ressource Planning* (ERP) en anglais) présentent l'avantage de couvrir plusieurs domaines métiers d'une entreprise en une seule application par l'intermédiaire de modules. Par exemple, le PGI le plus connu (« SAP », sur lequel repose CHORUS) intègre sous forme de modules les principales fonctions suivantes :

- module FI (*Financial*) : comptabilité générale ;
- module CO (*Controlling*) : contrôle de gestion (comptabilité auxiliaire) ;
- module SD (*Sales & Distribution*) : administration des ventes ;
- module MM (*Material Management*) : achat et gestion des stocks ;
- module PP (*Production Planning*) : gestion de la production ;
- module RE (*Real Estate*) : gestion immobilière.

Les principaux avantages des PGI sont les suivants :

- réduction des délais administratifs ;
- saisie unique dans le SI de l'organisation ;
- disponibilité immédiate de l'information ;
- piste d'audit « garantie » en principe ;
- la réduction des coûts informatiques est parfois mise en avant, malgré un investissement initial élevé.

En contrepartie, certaines exigences sont généralement imposées par la mise en place d'un PGI :

- mise en œuvre rigoureuse et exigeante en matière d'intégration, de paramétrage et de développements spécifiques potentiellement coûteux, y compris dans la durée ;
- revue de l'architecture technique pouvant conduire au remplacement des infrastructures matérielles et réseaux ;
- une adéquation des processus et de l'organisation au PGI pouvant offrir une opportunité de transformation si cette dernière est anticipée et pilotée ou *a contrario* constituer un frein au projet si elle n'est pas souhaitée et assumée ;
- partage de l'information pouvant entraîner un rejet de la part de certains acteurs ;
- maîtrise globale de la solution dans le temps car des incidents peuvent bloquer toute l'entité.

Les risques liés aux PGI sont les suivants :

- dérapage des projets (dans le temps et dans les coûts) compte tenu de la complexité et des enjeux ;
- les développements de programmes « spécifiques » éloignent l'outil du standard ce qui entraîne des problèmes de maîtrise du PGI voire des problèmes en termes d'auditabilité (altération possible de la piste d'audit) ;
- une inadaptation in fine du PGI à l'organisation dans le cas où la refonte des processus n'a pas été préalablement conduite et portée par la direction générale ;
- utilisateurs insuffisamment formés qui rejettent l'application ;
- forte dépendance vis-à-vis du sous-traitant et insuffisance de transfert de compétence en interne sur le PGI ;
- paramétrage des droits d'accès et des profils utilisateurs souvent galvaudé lors de la phase de développement.

Conformément aux pratiques de l'audit, ces risques sont habituellement analysés à travers une matrice des risques spécifique.

2. APPROCHE DE CERTAINS THEMES D'AUDIT

L'audit des SI peut soit constituer un sous-domaine d'un audit généraliste (organisation, processus, régularité, etc.), soit être l'objet principal de la mission (application, projet, sécurité, respect de la législation, etc.).

2.1. L'AUDIT DES SI A L'OCCASION DE MISSIONS « GENERALISTES »

La présente partie a pour objectif de montrer en quoi des audits ayant *a priori* peu à voir avec l'informatique doivent aborder *a minima* le domaine SI.

Elle fournit **une approche des implications SI** de quelques missions-types et dresse la liste des principaux enjeux et risques associés, acteurs à rencontrer, documents à récupérer et principales questions à aborder. Pour une approche plus spécifique, l'auditeur pourra se référer à la troisième partie du présent guide.

2.1.1. L'AUDIT D'UNE ORGANISATION

Les organisations utilisent quotidiennement l'informatique. Celle-ci peut prendre la forme de simple bureautique, d'applications dédiées, les mettant, le cas échéant, en relation avec leurs cocontractants ou usagers via l'Internet, voire de systèmes informatiques plus complexes. Ces outils informatiques sont, désormais, indispensables au bon fonctionnement de l'organisation. Ils sont parfois au cœur de sa performance.

Pourtant, les organisations n'en ont pas toujours conscience. Celles qui perçoivent l'importance de l'informatique ne maîtrisent pas toujours les arcanes de son pilotage, de sa conduite et de sa sécurité. Enfin, qu'elles disposent d'une fonction informatique en leur sein ou s'adressent à des prestataires internes ou extérieurs à l'administration, elles sont parfois peu ou mal organisées pour tirer le meilleur de ces ressources.

L'audit d'une organisation doit donc désormais nécessairement inclure un audit de sa relation au fait informatique. Comment définit-elle ses besoins fonctionnels, comment alloue-t-elle ses ressources humaines et financières en vue de les satisfaire, s'est-elle organisée et a-t-elle mis en place les processus lui permettant de disposer d'une informatique en phase avec ses besoins (alignement fonctionnel), réactive, sûre et efficiente ?

L'auditeur devra donc, à l'occasion de l'audit d'une organisation :

- étudier à travers les documents d'organisation et financiers les ressources organisationnelles (structures), humaines et financières qu'elle consacre à l'informatique ;
- étudier le fonctionnement de la comitologie associée au pilotage des SI ;
- se demander si ces ressources sont convenablement dimensionnées en regard de ce que d'autres organisations équivalentes consacrent à l'informatique ;
- étudier les processus stratégiques de l'organisation, inventorier les SI qui les outillent, et vérifier que l'entité s'est convenablement organisée pour garantir leur pilotage au juste niveau ;

- vérifier que l'organisation a mis en place le corpus minimal, ou décline convenablement celui fixé par le niveau supérieur (politique du SI, politique de sécurité du SI, charte d'utilisation).

Si l'entité possède une fonction informatique dédiée (études, production, etc.), l'auditeur généraliste devra si possible solliciter les spécialistes de l'audit des SI et pourra se référer à la troisième partie du présent guide.

L'auditeur devra rencontrer :

- la direction générale pour mesurer son degré de sensibilisation au fait informatique et l'organisation qu'elle a mise en place pour piloter ses SI ;

- une ou plusieurs directions fonctionnelles, le cas échéant les responsables de zones fonctionnelles, pour évaluer l'organisation qu'elles ont mise en place en vue de définir leurs besoins, de les exprimer et de contribuer efficacement aux processus visant à les satisfaire ;

- le cas échéant, la direction chargée des SI, pour évaluer la pertinence et les conséquences de son positionnement dans l'organisation et dans les processus de gouvernance ;

- le cas échéant, la direction chargée des achats, pour mesurer la part des SI dans son activité et vérifier la bonne prise en compte de leur spécificité ;

- le cas échéant, la direction chargée des ressources humaines, pour mesurer le poids des compétences SI (y compris indirectes, telles les compétences d'acheteur ou de juriste spécialisés dans le domaine SI) et des actions de formation dans le domaine.

Il devra se procurer :

- les politiques SI et de sécurité SI de l'organisation ;

- le plan d'occupation des sols (POS) du SI et la liste des responsables de zones fonctionnelles ;

- la charte de l'utilisateur des SI à laquelle sont soumis les membres de l'organisation ;

- la liste des processus de l'organisation incluant les SI qui les supportent ;

- les comptes-rendus des comités ou groupes de travail (GT) consacrés pour tout ou partie aux SI ;

- la liste et le poids financier des principaux marchés SI en cours ;

- la politique RH et de formation.

Au final, l'auditeur devra porter une appréciation sur la capacité de l'organisation à piloter son informatique, à apprécier ses enjeux (notamment la valeur de son patrimoine numérique) et évaluer les risques qui pèsent sur eux. Il peut aussi, si ses diligences lui fournissent une matière suffisante, évaluer l'alignement du SI sur les objectifs stratégiques de l'organisation.

Il lui appartient de formuler les recommandations utiles en la matière.

2.1.2. LES AUDITS DE PROCESSUS

Les processus sont désormais pour la plupart très fortement dépendants des outils informatiques. Dans le meilleur des cas, ils s'appuient sur un système informatique répondant à leurs besoins. Souvent, ils s'appuient au fil de leur déroulement sur des outils disparates, conçus dans une logique d'organisation et leur imposant des ruptures de charges. Ainsi, la performance d'un processus est intimement liée à l'alignement et à la qualité des systèmes informatiques.

Dans une organisation pratiquant le pilotage par les processus (niveau de maturité encore peu répandu dans l'administration), les projets informatiques devraient être pensés nativement dans une logique de processus.

L'audit d'un processus doit donc inclure un audit des outils informatiques sur lesquels il s'appuie. Cet audit doit inclure l'examen des données et informations manipulées au cours du déroulement du processus, y compris celles provenant d'autres processus, des applications qui servent ou automatisent tout ou partie des tâches ou procédures qui le composent, et des infrastructures informatiques de traitement et communication qu'il utilise.

L'auditeur devra donc, à l'occasion de l'audit d'un processus :

- étudier à travers les documents décrivant le processus et rendant compte de son fonctionnement, les données et informations manipulées, et les applications et les infrastructures utilisées. À défaut, il devra lui-même décrire le processus avant d'identifier ces éléments ;

- vérifier que les instances de gouvernance qui pilotent ce processus sont également compétentes pour orienter les SI y concourant ;

- vérifier l'alignement stratégique des outils informatiques et des processus qu'ils servent. Cette approche devra être étendue aux projets applicatifs ;

- vérifier que la sécurité physique et logique de ces données, informations, applications et infrastructures est en cohérence avec l'analyse des risques de ce processus. Il devra au préalable vérifier la pertinence de cette analyse des risques, voire procéder à sa propre analyse des risques ;

- étudier le dispositif de contrôle interne destiné à maîtriser ce processus, vérifier s'il existe qu'il est pertinent, et s'assurer que les outils informatiques y contribuent de manière efficace et efficiente ;

- vérifier que les infrastructures (particulièrement réseaux et serveurs) et les dispositifs d'assistance aux usagers de ces systèmes sont suffisants pour répondre aux besoins du processus.

L'auditeur devra rencontrer :

- la direction générale pour évaluer dans quelle mesure l'organisation pilote ses processus, voire pratique le pilotage par les processus, mesurer son degré de sensibilisation au fait informatique et vérifier que l'organisation qu'elle a mise en place pour piloter ses SI est en cohérence avec celle mise en place pour piloter les processus ;

- la ou les directions concernées par le processus audité, pour évaluer le degré de maturité de leur approche du processus, et étudier l'organisation qu'elles ont mise en place en vue de définir et exprimer des besoins en matière informatique qui soient bien alignés avec leurs processus ;

- s'ils existent, le pilote du processus audité et la direction chargée du pilotage des processus ou du pilotage par les processus, pour évaluer leur degré de sensibilisation au fait informatique et la qualité de leurs relations avec la direction chargée des SI ;

- la direction chargée des SI, pour évaluer la pertinence et les conséquences de son positionnement dans l'organisation et dans les processus de gouvernance vis-à-vis du processus audité.

Il devra se procurer :

- la cartographie des processus de l'organisation ;

- la description du processus audité, incluant l'inventaire des données et informations manipulées et des applications et infrastructures utilisées ;

- les tableaux de bord rendant compte de son déroulement et de sa performance ;

- la cartographie des données, informations et applications informatiques de l'organisation ;

- les politiques SI et de sécurité SI de l'organisation, et, le cas échéant, leur déclinaison à l'égard du processus audité ;

- la (ou les) charte(s) de l'utilisateur des SI à laquelle sont soumis les acteurs du processus ;

- le cas échéant, les comptes-rendus des comités ou groupes de travail consacrés pour tout ou partie au processus audité, notamment lorsqu'ils abordent le patrimoine informationnel qu'il manipule et les outils informatiques qui le servent ;

- la liste des projets applicatifs en cours, principalement ceux qui ont un impact sur le processus s'ils sont identifiés selon cette clé.

Au final, l'auditeur devra porter une appréciation sur l'adaptation (efficacité, efficience, sécurité, résilience) de l'informatique aux besoins du processus audité et sur sa contribution au dispositif de contrôle interne. Il pourra le cas échéant se prononcer sur la pertinence des projets informatiques en cours, voire recommander des évolutions du système informatique.

2.1.3. LES AUDITS DE REGULARITE

Les organisations s'appuient de plus en plus sur des outils informatiques. C'est à travers eux qu'elles gèrent leur ressource humaine, qu'elles exécutent leur budget et tiennent leur comptabilité, qu'elles conservent les données relatives à leurs interlocuteurs et à leurs administrés.

Leur fonctionnement régulier est donc largement sous-tendu par la conformité aux règles de leurs systèmes informatiques, qu'il s'agisse d'inventaire des licences, de validité des règles informatiques d'exécution budgétaire et de comptabilité, de respect des normes de conservation des données personnelles, de la mise en œuvre automatisée des règles statutaires applicables à la gestion de carrière ou au traitement des agents, etc.

L'audit de la régularité d'une situation, qu'il s'agisse de vérifier le fonctionnement d'une entité, le déroulement d'un processus ou, plus généralement, le respect d'une norme ou d'un corpus normatif, implique donc le plus souvent l'audit des ressources informatiques qui y contribuent. L'auditeur cherchera à vérifier que les activités portées par les ressources informatiques sont en elles-mêmes régulières et à mesurer leur contribution au contrôle interne de l'entité ou du processus, par leur architecture ou les règles qu'elles portent.

L'auditeur devra donc, à l'occasion d'un audit de régularité :

- identifier les ressources informatiques utilisées dans le périmètre de son audit ;

- vérifier que ces ressources sont en elles-mêmes régulières (licences, respect des règles de conservation des données personnelles, respect des règles de confidentialité, etc.) ;

- vérifier que les traitements automatiques réalisés par ces ressources sont conformes au corpus normatif applicable, et évaluer leur fiabilité ;

- vérifier que la sécurité appliquée à ces ressources, outre le respect des règles de confidentialité, garantit raisonnablement qu'elles ne peuvent être utilisées à des fins frauduleuses.

L'auditeur devra selon les cas rencontrer :

- la direction générale du périmètre auquel appartient le champ audité, pour évaluer dans quelle mesure elle est consciente de la dimension informatique de l'obligation de fonctionnement régulier qui pèse sur elle, et savoir comment cette dimension est prise en compte ;

- les acteurs opérationnels de l'entité ou du processus audité, pour identifier les ressources informatiques (y compris de bureautique) utilisées ;

- la direction chargée des ressources informatiques utilisées dans le périmètre audité, pour vérifier qu'elle connaît, respecte, et fait respecter les divers corpus normatifs applicables ;

- la direction chargée de la supervision du contrôle interne, pour vérifier qu'elle a bien pris en compte les ressources informatiques dans le dispositif de contrôle interne du périmètre audité, voire s'appuie sur elles pour la réalisation de ses propres objectifs.

Il devra se procurer :

- l'inventaire des ressources informatiques utilisées dans le périmètre audité (notamment la cartographie des applications et des systèmes) ;

- les contrats et inventaires de licences ;
- les déclarations CNIL ;
- la description du dispositif de contrôle interne incluant la part prise par l'application des règles informatiques ;
- les rapports de vérifications issus du dispositif de contrôle interne et les bases de données répertoriant les incidents d'exploitation, pour évaluer la fiabilité des traitements informatiques ;
- si nécessaire, les spécifications détaillées des applications concourant à la mise en œuvre d'un corpus normatif par un traitement automatisé.

Au final, l'auditeur devra porter une appréciation à la fois sur la valeur de la contribution de l'informatique à la régularité des opérations auditées et sur la régularité des activités informatiques elles-mêmes.
Il lui appartient de formuler les recommandations utiles en la matière.

2.1.4. LES AUDITS DES FONCTIONS EXTERNALISEES

Rares sont les fonctions externalisées qui n'ont pas besoin d'échanger régulièrement des données avec l'organisation, ce qui suppose une interconnexion entre systèmes informatiques. Souvent, le bon déroulement de ces échanges de données, en temps réel ou non, constituent une partie des obligations des deux cocontractants. Ils sont aussi le motif d'une ouverture du système informatique de l'organisation vers l'extérieur, parfois pour des actions aussi sensibles que de l'administration de serveurs, de données ou d'applications.

Plus rares encore sont les fonctions externalisées qui n'ont pas à manipuler des données ou informations appartenant au patrimoine de l'organisation. Le cocontractant a alors la responsabilité de l'intégrité, de l'accessibilité et de la protection des données.

Dans tous les cas, la dimension informatique de l'externalisation est au cœur de sa réversibilité. Elle peut être la cause de son irréversibilité.
L'audit d'une fonction externalisée devra donc en aborder la dimension informatique, tant pour l'organisation que pour son cocontractant.

L'auditeur devra donc, à l'occasion de l'audit d'une fonction externalisée :

- identifier les données et informations numériques échangées à l'occasion de l'exécution de la prestation externalisée ;

- identifier les ressources informatiques matérielles (serveurs, réseaux, etc.) et applicatives qui y contribuent, et le personnel interne et extérieur qui les administrent et les utilisent ;

- vérifier que le contrôle interne (y compris la résilience) appliqué à ces ressources est en cohérence avec leur importance pour l'organisation ;

- vérifier que le marché d'externalisation traite convenablement des aspects informatiques, notamment en ce qu'il prévoit bien quelles sont les obligations des deux parties en matière de manipulation et de conservation des ressources informationnelles et matérielles, et qu'il organise de manière crédible la réversibilité ;

- vérifier qu'il existe une instance de gouvernance de la relation entre l'organisation et son prestataire qui permette en cas de besoin l'adaptation de la relation contractuelle à l'évolution de l'environnement informatique.

L'auditeur devra selon les cas rencontrer :

- les acteurs opérationnels de l'organisation chargés des relations courantes avec le prestataire, pour identifier les ressources informatiques (informationnelles, matérielles et humaines) concernées par la prestation externalisée ;

- la direction générale du périmètre auquel appartient le champ audité, pour évaluer dans quelle mesure elle est consciente de la dimension informatique de la prestation externalisée ;

- la direction chargée des achats, pour examiner comment les aspects informatiques ont été traités dans le marché d'externalisation. Dans l'idéal, ce marché comportera une clause d'audit permettant à l'auditeur d'examiner les opérations informatiques réalisées par le prestataire à l'occasion de l'exécution du marché ;

- la direction chargée des systèmes informatiques, pour vérifier qu'elle a validé les échanges avec le prestataire, y compris le cas échéant les modalités d'interconnexion entre le système informatique de l'organisation et celui du prestataire ;

- si le marché le permet, le prestataire, pour examiner la sûreté, la sécurité, la régularité et la conformité au marché des opérations informatiques qu'il effectue à l'occasion de la prestation ;

- la direction chargée de la supervision du contrôle interne, pour vérifier qu'elle a bien pris en compte l'existence d'une externalisation dans le dispositif de contrôle interne appliqué aux ressources informatiques.

Il devra se procurer :

- le ou les marché(s) organisant l'externalisation ;

- la description des processus externalisés et de ceux impactés par l'externalisation ;

- l'inventaire des ressources informatiques utilisées pour ou impactées par l'exécution de la prestation externalisée (notamment la cartographie des applications et des systèmes) ;

- les documents contractuels à fournir par le prestataire assurant de son respect des dispositions contractuelles et réglementaires dans le domaine informatique ;

- la description du dispositif de contrôle interne précisant la part revenant au prestataire et celle supportée par les systèmes informatiques.

Au final, l'auditeur devra porter une appréciation sur la qualité de la prise en compte des problématiques informatiques dans le cadre de l'externalisation auditée. Il devra se prononcer sur les fragilités éventuelles résultant de la dimension informatique de l'externalisation, notamment en termes de réversibilité, de sécurité et de contrôle interne.
Il lui appartient de formuler les recommandations utiles en la matière.

2.1.5. LES AUDITS DE PROJETS NON SI

Au-delà des projets spécifiquement informatiques (applications, infrastructures, migrations de données, etc.) qui font l'objet de développements ultérieurs, la plupart des projets contiennent une dimension informatique, qui concerne à la fois la conduite du projet et la cible visée.

Ainsi, les ressources informatiques mises à la disposition de l'équipe projet doivent être adaptées et utilisées convenablement. Il s'agit autant d'ergonomie que de résilience et de sécurité, surtout pour un projet stratégique ou sensible.

Par ailleurs, quel que soit le projet (organisationnel, industriel, RH, création d'un nouveau service aux administrés, etc.), la cible finale comportera très certainement une dimension informatique. Il pourra par exemple s'agir de développer les outils nécessaires à un nouveau processus, de déménager des services avec leurs ressources informatiques associées, sans rupture de la production, d'assurer la convergence entre les systèmes informatiques de deux entités fusionnées ou, au contraire, leur séparation lors d'une scission.

Dans tous les cas, une mauvaise anticipation des opérations à réaliser sur les outils informatiques est susceptible d'avoir un impact fortement négatif sur le déroulement, voire la réussite, du projet. L'audit d'un projet devra donc en identifier les enjeux informatiques et vérifier leur correcte prise en compte.

L'auditeur devra donc, à l'occasion de l'audit d'un projet :

- identifier précisément le périmètre informatique (matériels, applications, données et ressources humaines) du projet, en distinguant clairement le projet lui-même et la cible visée ;
- s'agissant du projet, vérifier que les ressources mises à disposition de l'équipe projet (matériels, applications, support) sont adaptées, et que les règles, notamment celles relatives à la sécurité des systèmes d'information (SSI), sont adaptées, connues et appliquées. Il lui faudra notamment vérifier qu'elle inclut des personnes capables de traiter les enjeux informatiques de la cible du projet ;
- s'agissant de la cible du projet, vérifier que la dimension informatique des processus, organisation, etc. visés sont convenablement inventoriés et pris en compte de manière réaliste.

L'auditeur devra rencontrer :

- la direction du projet, pour s'assurer qu'elle dispose des leviers d'action et des ressources nécessaires à la bonne conduite du projet, et pour vérifier qu'elle a suffisamment anticipé l'impact du projet en matière SI, notamment en matière de conduite du changement ;
- la direction chargée des systèmes informatiques, pour vérifier qu'elle est convenablement associée à la définition des attendus informatiques du projet.

Il devra se procurer :

- le document de management du projet et les objectifs assignés au projet ;
- la description des processus cibles et de leur dimension informatique ;
- l'inventaire et la cartographie des données, applications et systèmes informatiques impactés ou mis en place par le projet ;

- les comptes-rendus de la comitologie, notamment ceux qui abordent les aspects informatiques.

Au final, l'auditeur devra porter une appréciation sur la qualité de la prise en compte des problématiques informatiques dans le cadre du projet audité. Il devra se prononcer sur les fragilités éventuelles résultant de la dimension informatique du projet, notamment en termes d'alignement stratégique de l'informatique avec les objectifs du projet, de sécurité physique et logique, et de contrôle interne.

Il lui appartient de formuler les recommandations utiles en la matière.

2.2. LES MISSIONS D'AUDIT DONT L'OBJET PRINCIPAL APPARTIENT AU DOMAINE DES SI

Cette sous-partie a pour objectif de montrer en quoi des audits focalisés sur l'informatique doivent s'extraire du strict périmètre de l'informatique pour aborder des dimensions ayant un impact sur le SI. Elle ne décrit bien sûr pas le cœur de la mission d'audit, objet de la troisième partie, mais donne quelques pistes pour « aller plus loin ».

2.2.1. LES AUDITS D'APPLICATION

Une application n'existe que pour répondre à un besoin. Elle est conçue, réalisée, paramétrée, administrée, entretenue et utilisée par des agents appartenant ou non à l'organisation. Elle peut être utile à un ou plusieurs processus, leur être parfaitement adaptée ou au contraire être une entrave à leur bon déroulement. Elle peut s'inscrire dans une urbanisation maîtrisée ou contribuer à l'hétérogénéité, à la duplication, voire au désordre du système informatique. Elle peut donc être une source de force ou de vulnérabilité – parfois les deux – pour l'organisation.

Au-delà des aspects classiques d'un audit d'application en production (cf. chapitre 3), l'audit d'une application informatique peut donc nécessiter l'examen de l'urbanisation du système informatique, de la cohérence entre les logiciels et les matériels qu'ils utilisent, de l'alignement stratégique du système informatique sur les objectifs de l'organisation, voire de la gouvernance du SI, en ce qu'elle explique pour une large part les forces et faiblesses observées.

En effet, les recommandations émises au terme de l'audit ne peuvent faire abstraction de cet environnement. Tout cela suppose une compréhension de la fonction informatique allant très au-delà du simple objet audité.

Au-delà, si la correction d'une faiblesse de l'application auditée nécessite la modification d'un ou plusieurs éléments de son environnement, l'auditeur doit recommander les évolutions nécessaires.

Ainsi, l'audit d'une application, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause :

- de l'urbanisation du système informatique ;
- de la formation des utilisateurs, y compris le personnel de la production informatique (administrateurs, soutien aux utilisateurs, etc.) ;
- de l'articulation entre les fonctions études et production ;
- du ou des processus au(x)quel(s) contribue l'application, y compris le dispositif de contrôle interne mis en place pour en maîtriser les risques ;
- de l'organisation du soutien externalisé de l'application ;
- de l'organisation de la gouvernance de la fonction informatique.

Cela vient évidemment en complément des aspects à examiner proposés en troisième partie du présent guide.

Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas l'audit de la fonction informatique dans son ensemble mais celui d'une application bien définie. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec l'application auditée.

2.2.2. LES AUDITS DE PROJETS INFORMATIQUES

Un projet informatique n'existe que pour répondre à un besoin. Il faut donc s'assurer, au-delà du respect de la méthodologie de conduite du projet, que le besoin existe, qu'il a été convenablement recueilli et exprimé, et qu'il n'est pas perdu de vue. L'auditeur peut s'appuyer pour cela sur des outils d'analyse de la valeur[1].

L'auditeur peut se retrouver face à un projet qui, au lieu de respecter l'urbanisation en vigueur, contribue au contraire à l'hétérogénéité, voire au désordre du système informatique. Cependant, l'irrespect du cadre urbanistique par un projet ne doit pas entraîner une condamnation automatique, car cette incohérence peut révéler une urbanisation ou une organisation urbanistique inadéquates qui dans ce cas ne doivent pas nécessairement prévaloir sur le projet et ses attendus.

Au-delà des aspects classiques d'un audit de projet (cf. chapitre 3), l'auditeur doit donc examiner la qualité de l'expression, du recueil et de la traduction du besoin, l'urbanisation du système informatique, l'inscription du projet dans cette urbanisation, voire la gouvernance du SI, en ce qu'elle explique pour une large part les forces et faiblesses observées. En effet, les recommandations émises au terme de l'audit ne peuvent faire abstraction de cet environnement. Tout cela suppose une compréhension de la fonction informatique allant très au-delà du simple objet audité.

Au-delà, si la correction d'une faiblesse du projet audité nécessite la modification d'un ou plusieurs éléments de son environnement, l'auditeur doit recommander les évolutions nécessaires.

Ainsi, l'audit d'un projet, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause :

- des modalités d'expression et de recueil des besoins métiers ;
- du processus d'arbitrage entre projets concurrents ;
- de l'organisation de passation des marchés avec les maîtres d'œuvres informatiques, voire avec les assistances à maîtrise d'ouvrage ;
- de la gestion des processus au sein de l'organisation, notamment du processus ayant suscité le projet audité ;
- de l'organisation de ce processus ;
- de l'organisation de la gouvernance de la fonction informatique ;
- de l'urbanisation du SI de l'organisation.

Cela vient évidemment en complément des aspects à examiner proposés en troisième partie du présent guide.

Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas l'audit de la fonction informatique dans son ensemble mais celui d'un projet particulier. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec ce projet.

[1] Par exemple MAREVA 2, spécifiquement créé pour rendre compte de la pertinence des projets SI

2.2.3. LES AUDITS DE SECURITE

Un dispositif de sécurité n'est pas une fin en soi. Il n'existe que pour protéger des actifs. Il faut donc s'assurer, au-delà des aspects examinés habituellement dans le cadre de l'audit de la sécurité générale informatique (cf. chapitre 3), que le dispositif de sécurité est justifié et équilibré.

La sécurité informatique ne se résume pas à l'informatique. Elle intègre bien sûr les sécurités logique et physique de l'informatique, y compris dans leur dimension « résilience », fréquemment oubliées notamment pour les systèmes périphériques, comme les imprimantes ou téléphones en réseau, le contrôle des accès et temps de travail, l'informatique industrielle ou la gestion technique des bâtiments, mais s'étend bien au-delà. Elle s'intègre dans un dispositif global de sécurité, destiné à protéger tous les actifs de l'organisation et non seulement ses actifs informatiques ou dématérialisés, et doit être en cohérence avec les efforts réalisés en dehors du domaine informatique.

Elle découle d'une culture (ou inculture) de la sécurité propre à chaque organisation. Elle procède d'une identification et d'une évaluation de l'importance des actifs, d'une analyse des menaces pesant sur eux et des vulnérabilités de l'organisation, d'une décision quant à l'aversion au risque de l'organisation et aux modalités et dispositifs de sécurité qui en découlent. Elle doit aussi procéder d'une juste évaluation des contraintes normatives pesant sur l'organisation.

Au-delà des aspects classiques d'un audit de sécurité informatique, l'auditeur doit donc examiner la qualité de l'inventaire des actifs, de l'évaluation des risques, du processus décisionnel ayant conduit à la définition d'un dispositif de sécurité et de la pertinence et la qualité de ce dispositif. En effet, les recommandations émises au terme d'un audit de sécurité ne peuvent faire abstraction de ces aspects.

Au-delà, si la correction d'une faiblesse du dispositif de sécurité audité nécessite la modification d'un ou plusieurs éléments de son environnement, l'auditeur doit recommander les évolutions nécessaires.

Ainsi, un audit de sécurité, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause :

- de l'inventaire et de l'évaluation des actifs protégés par le dispositif de sécurité ;
- de l'analyse des menaces pesant sur ces actifs et des vulnérabilités devant être corrigées ;
- de la gouvernance et de la culture de la sécurité au sein de l'organisation, le cas échéant au-delà du seul périmètre informatique ;
- de l'équilibre global d'une part, entre les efforts consacrés à la sécurité informatique et ceux consacrés à la sécurité en général et, d'autre part, entre la valeur des actifs à protéger ou les normes qui leurs sont applicables et les efforts consacrés à la sécurité informatique.

Cela vient évidemment en complément des aspects à examiner proposés en troisième partie du présent guide.

Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas l'audit de la sécurité dans son ensemble mais celui de la sécurité informatique. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec cette dernière.

2.2.4. LES AUDITS DE QUALITE DES DONNEES

Les données, surtout lorsqu'elles sont suffisamment importantes pour susciter un audit, sont parmi les actifs les plus précieux d'une organisation. La qualité des données est généralement indispensable au bon déroulement des processus. Elle porte souvent un enjeu financier (références fournisseurs, éléments de calcul de la paie, etc.), parfois vital (s'agissant par exemple des dossiers médicaux informatisés).

La qualité de la donnée est duale : elle est « interne », s'agissant par exemple de l'exactitude de la donnée, mais aussi « externe », notamment les métadonnées s'y rapportant. En effet, la catégorisation d'une donnée (identification de données comme étant sensibles, telle des coordonnées bancaires ou des écritures comptables, des données personnelles, ou relevant du secret industriel, médical, de la défense nationale, etc. devant à ce titre être protégées), qui conditionne le régime qui lui est applicable (droits d'accès et de modification), peut être aussi importante que la donnée elle-même.

De même, la qualité des libellés en plein texte ou le renseignement des mots clé associés aux documents peuvent être indispensables au bon fonctionnement des fonctions de tri et des algorithmes de recherche automatique.

De nombreux acteurs et processus produisent de la donnée, et de nombreux acteurs et processus peuvent être impliqués dans la création, la mise à jour et la destruction d'une donnée particulière ou de ses métadonnées. C'est pourquoi, toute donnée devrait avoir un propriétaire explicitement désigné dans l'organisation, responsable sinon de sa création, de son entretien, de sa suppression, de sa protection, de son intégrité, de sa disponibilité et de sa localisation, du moins de la définition des droits et règles applicables à la totalité de ces dimensions et de la vérification de leur attribution et de leur respect.

Par ailleurs, pour le fonctionnement d'une organisation, la non duplication (par exemple dans des fichiers bureautiques locaux) est un enjeu au moins aussi important que la qualité interne ou externe d'une donnée.
En effet, une donnée périmée conservée localement peut être utilisée en lieu et place de la donnée actualisée conservée dans la base de données adéquate, et il est très probable que la copie ne bénéficiera pas des règles de gestion applicables à l'originale.

Au-delà de la vérification ponctuelle de la qualité interne d'un ensemble de données, l'auditeur doit donc examiner leur qualité externe. Il devra s'intéresser aux processus aboutissant à une opération sur les données, aux responsabilités relatives à la définition des règles applicables en la matière et au respect de leur mise en œuvre.

Ainsi, un audit de qualité des données peut entraîner la remise en cause :

- des règles et processus applicables à la gestion des données et des métadonnées ;
- de l'organisation mise en place, si elle ne prévoit pas que chaque donnée ait un unique propriétaire ayant autorité pour définir et faire appliquer les règles y relatives ;
- de l'urbanisation du SI, si des phénomènes de duplication des données sont observés, ou si la mise en place d'entrepôts de données s'avérait insuffisamment étudiée ;
- voire des PRI/PCI et PRA/PCA, s'agissant de la disponibilité des données (la réplication non maîtrisée étant parfois une « garantie » contre l'indisponibilité).

Pour autant, le mandat de l'auditeur dans le cas d'espèce n'est pas un audit de l'organisation ou de la résilience mais celui de la qualité des données. Il devra donc veiller constamment à ce que ses diligences et recommandations aient un lien avec cette dernière.

2.2.5. LES AUDITS DE REGULARITE SPECIFIQUES

La régularité des opérations du domaine de l'informatique résulte à la fois d'un corpus normatif interne à l'organisation et de normes fixées par les pouvoirs publics. L'auditeur doit évaluer les écarts entre les activités informatiques et ces normes, impératives.

Toutefois, aucune norme, y compris publique, n'est intangible. Notamment, un auditeur agissant pour le compte d'une organisation étatique, *a fortiori* un auditeur appartenant à un corps d'inspection générale étatique, doit recommander aux services audités de travailler à l'évolution des normes nationales qui leurs sont applicables lorsqu'elles sont inadaptées, plutôt que de céder à la facilité du contournement. Il doit évidemment recommander la modification d'une **norme interne** contre-productive.

Il appartient donc à l'auditeur réalisant un audit de régularité (informatique) de s'assurer que les efforts à fournir pour appliquer les normes sont raisonnables au vu des contraintes et objectifs de l'organisation concernée, voire de se prononcer sur leur (in)applicabilité. Pour ce faire, il ne devra pas hésiter à comparer la situation observée avec celle prévalant dans des organisations équivalentes.

Face à un écart en termes de régularité, l'auditeur doit recommander une action de correction des pratiques ou de modification de la norme, voire les deux, la correction de la norme apparaissant alors comme un objectif de long terme tandis que la mise en conformité doit être un objectif de court terme.
Face à une norme inapplicable, ou dont l'application demanderait des efforts déraisonnables, l'auditeur doit se prononcer sur les risques que l'irrégularité fait peser sur l'organisation, en veillant à ne pas se limiter aux risques juridiques : une norme étant rarement une fin en soi, s'en affranchir expose généralement à des risques opérationnels.

Par ailleurs, l'auditeur ne devra pas se limiter à la régularité vis-à-vis de l'activité informatique (CNIL, licences, sécurité logique, etc.). Il lui appartient également de s'assurer que les opérations réalisées par le système informatique audité sont en elles-mêmes régulières. Par exemple, un système de traitement des données individuelles peut satisfaire les normes de sécurité informatique tout en appliquant des règles de gestion statutaires irrégulières.

Ainsi, un audit de régularité, surtout s'il est suscité par une situation pathologique, peut entraîner la remise en cause :

- du corpus normatif interne à l'organisation ;
- du corpus normatif public applicable ;
- de la régularité des opérations « métier » réalisées au moyen du système informatique audité.

3. APPROCHE THEMATIQUE ET TECHNIQUE DES PRINCIPAUX DOMAINES D'AUDIT DES SI

Les deux premières fiches (3.1 et 3.2) sont transverses. Les fiches suivantes doivent être considérées comme venant en complément thématique des problématiques de gouvernance et de sécurité.

Il est important de noter qu'elles présentent des points de contrôle basiques à caractère illustratif qui doivent être adaptés au contexte, aux enjeux et aux risques propres à l'audit réalisé. Ils ne doivent pas ainsi être considérés comme exhaustifs ou nécessairement suffisants aux travaux d'audit.

Ils sont, en outre, adaptés à des organisations et des cycles de développement classiques (dits cycles en V). Ainsi, ils peuvent ne pas être totalement applicables et appropriés pour les modes d'organisation et les méthodes actuelles prônant le décloisonnement des maîtrises d'ouvrage et d'œuvre et les développements en mode agile.

Par ailleurs, ces approches doivent être appliquées en subsidiarité des éventuels référentiels officiels d'audit et de contrôle en vigueur au moment des audits.

Sommaire des principaux domaines d'audit étudiés

3.1. AUDIT DU PILOTAGE DES SYSTEMES D'INFORMATION

La notion de maturité d'une organisation dans le domaine des systèmes d'information est une notion importante dans la compréhension et l'évaluation du rôle et de la performance de l'informatique dans l'organisation. Cette maturité se décline d'abord sur les plans fonctionnel et technologique, puis sur le plan organisationnel et managérial.

L'objectif de l'audit est d'évaluer la « maturité » informatique de l'Organisation et l'adéquation du rôle, du positionnement et des objectifs de la DSI avec les enjeux de l'Organisation.

Points de contrôle
1. Rôle et positionnement de l'informatique dans l'organisation
1.1. La DSI est-elle rattachée à la DG et présente au COMEX ?
1.2. Vérifier l'existence d'une charte informatique ou de tout autre document définissant le rôle et le périmètre de responsabilité de la DSI : • s'assurer que la DSI est limitée à son rôle de MOE (versus MOA), comprenant notamment : la conception, réalisation, mise en œuvre et l'exploitation des solutions, la responsabilité des choix d'architecture et des solutions techniques afin de garantir la cohérence d'ensemble, la (co)responsabilité des achats informatiques, … • vérifier que la DSI est une force de proposition et de conseil dans le domaine des technologies de l'information.
1.3. Évaluer le degré d'implication et de maîtrise de la DG dans les systèmes d'information de l'Organisation : • systèmes d'information et innovations technologiques intégrées dans le Projet de service ? • prendre connaissance des communications interne et externe.
1.4. Vérifier qu'ont été créés des Comités « informatique » (stratégique, pilotage,..) regroupant les différentes directions de l'Organisation en charge de recenser les besoins et les opportunités, gérer les priorités et suivre les projets : • évaluer le rôle et le « poids » exacts de ce comité. Prendre connaissance de ses objectifs, de sa composition et des comptes-rendus de ses réunions.
1.5. Vérifier que les métiers assurent leur rôle de MOA, en prenant en charge des aspects suivants : • le pilotage du SI et des projets ainsi que la responsabilité des budgets ; • la définition des processus et l'analyse des besoins, notamment dans le domaine de la sécurité (classification des données en termes de disponibilité, d'intégrité et de confidentialité) ; • la gestion du changement, la gestion des évolutions de l'application (gestion des demandes, arbitrages, priorités, budget) et son administration ; • la validation des traitements et la recette des nouvelles versions.

1.6. Vérifier en pratique que le leadership des grands projets :

- informatiques de l'Organisation est assuré par une équipe compétence sous le contrôle et l'autorité des directions générales et métiers et que le modèle de coopération maîtrise d'œuvre / maîtrise d'ouvrage est mature et opérant.

2. Planification stratégique

2.1. Périmètre fonctionnel (couverture, ouverture et dépendance des SI).

2.2. Prendre connaissance du schéma directeur de l'Organisation (ou de ses axes stratégiques et ses grands projets) et analyser le plan informatique et la feuille de route du SI ministériel :

- analyse des processus d'élaboration et de validation du plan (contenant) ;
- analyse de la pertinence du plan (contenu) et de son alignement stratégique ;
- analyse de l'adéquation des compétences et des ressources aux objectifs du plan.

2.3. Analyse des procédures de pilotage et de mise à jour du plan informatique :

- analyse des dispositifs de pilotage et de suivi de la réalisation du plan ;
- analyse du rôle des comités et des procédures de mise à jour du plan (périodicité annuelle minimum).

2.4. Prendre connaissance des documents d'urbanisme de l'Organisation :

- analyse des processus d'élaboration et de validation du document (contenant) ;
- analyse de la pertinence du document (contenu), notamment de la délimitation des zones fonctionnelles ;
- analyse des schémas directeurs des zones fonctionnelles.

2.5 Analyse des procédures de pilotage et de mise à jour du plan d'occupation des sols (POS) :

- analyse des dispositifs de pilotage et de suivi de la réalisation du plan ;
- analyse du rôle des comités et des procédures de mise à jour du plan (périodicité annuelle minimum) ;
- analyse du positionnement dans l'Organisation et du rôle des responsables de zones fonctionnelles, de quartiers fonctionnels et de blocs fonctionnels.

2.6. Cohérence & homogénéité des technologies (homogénéité des OS, SGBD, postes de travail, langages, rationalisation des plateformes, standardisation des configurations,…).

2.7. Intégration et fiabilité des applications.

2.8. Unicité des référentiels (clients, fournisseurs, articles,…) et des saisies.

3. Budgets et coûts informatiques

Prendre connaissance et évaluer l'organisation et les processus :

- analyse du processus d'élaboration et de validation du budget (qui, quand, comment) ;
- analyse du périmètre du budget (géographique et organisationnel, charges et investissement,…) et évaluation de son caractère exhaustif ;
- analyse de l'organisation du contrôle de gestion informatique (existence d'un contrôleur de gestion dédié au sein de la DSI ?) ;

- analyse des outils et procédures de suivi analytique, de contrôle des coûts, d'analyse des écarts et le cas échéant de refacturation des utilisateurs ;
- analyse des tableaux de bord et des procédures de *reporting* (cf. chapitre Mesure et suivi de la performance).

3.2. Établir des ratios et des éléments de *benchmark* (interne et/ou externe, ratio coûts/CA, …). Attention : à manier avec précaution, les ratios de coûts IT ne sont qu'un élément d'évaluation parmi d'autres et les benchmarks doivent être fiables pour être utilisés.

4. Mesure et suivi de la performance informatique

4.1. Des objectifs de court, moyen et long termes ont-ils été assignés à la DSI (approche BSC ?) et ces objectifs sont-ils déclinés au sein des organisations ?

4.2. Existe-t-il un comité informatique regroupant les différentes directions de l'organisation et dont les principaux objectifs sont :

- le recensement des opportunités, la gestion des priorités, la validation des investissements et la politique de sécurité (stratégie) ;
- le suivi et le contrôle des performances, de la qualité de la prestation et de l'atteinte des objectifs fixés (pilotage).

4.3. Vérifier l'existence et la couverture des engagements de service / *Service Level Agreement* (SLA) par application. La qualité de service, pour l'utilisateur, se mesure sur les critères de :

- disponibilité et continuité d'exploitation (disponibilité moyenne de l'application, durée maximum d'indisponibilité, perte maximum de données,..) ;
- performance (temps de réponse TP, traitement batch, Interfaces…) ;
- support (help desk et assistance utilisateur : couverture horaire et linguistique, délais de résolution des incidents, formation….) ;
- sécurité (confidentialité, intégrité des données, authentification, non répudiation,..) ;
- coûts (coûts d'évolution, coûts récurrents de fonctionnement,…).

4.4. Évaluer la pertinence des indicateurs de qualité et de performance ainsi que les moyens et outils de mesure…

4.5. La DSI tient-elle un tableau de bord (idéalement de type BSC) permettant un suivi consolidé de la performance (opérationnelle et financière) et de la qualité des prestations informatiques ?

- suivi global de l'avancement du plan informatique et suivi détaillé projet par projet ;
- suivi des indicateurs de performance (SLA) par application, analyse des taux de conformité, suivi de l'évolution de la performance, etc. ;
- suivi des coûts (mois, YTD) rapprochés du budget ;
- suivi d'indicateurs « internes » (taux d'utilisation des CPU, espace disque, analyse du portefeuille des demandes utilisateurs, productivité des études, formation et gestion des compétences internes, etc.) ;
- enquête périodique de satisfaction auprès des utilisateurs, etc.

4.6. Est-il systématiquement effectué un bilan après chaque projet et notamment un bilan économique (bilan rapproché des prévisions de

l'étude préalable) ?

5. Organisation et structure de la DSI

5.1. Vérifier l'existence d'un organigramme à jour de la DSI.

5.2. Existe-il une définition de fonction et un partage clair des rôles et des responsabilités pour chaque poste figurant sur l'organigramme ?

5.3. Vérifier que l'ensemble des composantes d'une fonction informatique est convenablement pris en compte, notamment la veille technologique, la sécurité informatique, la fonction qualité & méthodes, la gestion des ressources humaines, le contrôle de gestion, le support utilisateurs (de proximité et à distance), l'administration des serveurs...

5.4. Évaluer l'adéquation des effectifs aux besoins et aux enjeux :

- analyse de la couverture fonctionnelle et géographique de l'informatique ;
- benchmarks internes et externes, ratios effectifs/CA et Budget IT/CA, …
- analyse du recours à la sous-traitance ;
- analyse de la charge du personnel informatique : horaires pratiqués, portefeuille des demandes utilisateurs, ...

5.5. Évaluer l'adéquation des qualifications du personnel avec les fonctions qu'ils occupent :

- prendre en compte la stratégie de l'organisation, ainsi que le marché local de l'emploi ;
- remettre en perspective le rôle, les objectifs et les attentes vis-à-vis de l'informatique ;
- prendre en compte le niveau de risque (risque inhérent à l'activité, dépendance de l'organisation vis-à-vis de son système d'information, …).

5.6. L'expression des besoins, les spécifications fonctionnelles et la recette des applications sont-elles effectuées par les utilisateurs ?

5.7. Les tâches, les locaux et les environnements relatifs aux fonctions études et exploitation, qu'ils soient assurés ou fournis en interne, ou externalisés, sont-ils séparés ?

- Vérifier que les accès aux bibliothèques de production (données et programmes) sont interdits aux études (y compris sous-traitants).

5.8. Vérifier l'existence d'une procédure de mise en production :

- évaluer sa pertinence et son niveau d'application.

5.9. Lorsque les organisations le permettent, vérifier que les différentes tâches d'administration des bases de données -DBA- sont séparées entre les études et l'exploitation :

- gestion du contenu : architecture des bases, dictionnaire de données ;
- gestion du contenant : gestion des configurations et des performances.

5.10. La séparation des tâches est-elle maintenue et assurée lors de la rotation des équipes, des vacances et du départ d'un personnel ?

5.11. Évaluer le caractère « raisonnable » du turn-over de la DSI (5 à 15% / an).

5.12. Évaluer la capacité de l'Organisation à gérer les carrières des informaticiens :

- prendre connaissance des évolutions sur les trois dernières années.

5.13. Vérifier l'adéquation du niveau de rémunération du personnel informatique et évaluer le « moral » des équipes :

- évaluer les mesures prises par la DSI ou par les RH pour s'assurer de la cohérence vis-à-vis du marché (étude annuelle, *benchmarking*,…).

5.14. Évaluer la dépendance de l'Organisation vis-à-vis d'une ou plusieurs personnes. Éléments à prendre en compte :

- développements internes versus progiciel, âge des applications et technologies mises en œuvre, taille des équipes, niveau de la documentation…

5.15. Les contrats des informaticiens contiennent-ils des clauses spécifiques de confidentialité et de non-concurrence ?

5.16. Les informaticiens sont-ils dispensés de préavis en cas de rupture brutale du contrat de travail ?

5.17. Existe-il un plan de formation nominatif pour l'ensemble des informaticiens ?

5.18. L'effort de formation est-il adapté, suffisant et s'inscrit-il dans la durée ?

- 5 à 10 jours par an, sur les trois dernières années. Formation individualisée qui répond aux souhaits de l'employé et aux besoins de l'organisation.

6. Cadre législatif et réglementaire Français

6.1. Vérifier que les prescriptions légales découlant de la loi « Informatique et Libertés » sont connues (procédures de déclaration, documentation, règles de confidentialité) et respectées :

- prendre connaissance et évaluer la démarche et les procédures mises en œuvre au sein de l'organisation (information, inventaire,…).

6.2. Vérifier que la loi sur la fraude informatique est connue et que des mesures préventives ont été prises :

- les bannières d'accueil aux routeurs et aux serveurs d'accès distant (de type " Bienvenue.. ", " *Welcome* ",…) sont-elles bannies et remplacées par des messages d'avertissement ?
- prendre connaissance de la nature et de la pertinence de la communication interne sur le sujet.

6.3. Vérifier que les lois sur l'usage de moyens de chiffrement et de la signature électronique sont connues et, le cas échéant, respectées.

6.4. Vérifier que la loi sur le contrôle fiscal des comptabilités informatisées est connue et, dans la mesure du possible, respectée :

- contrôler les procédures annuelles de sauvegarde et d'archivage des données et des programmes des applications concernées ;
- vérifier l'existence de documentations études, exploitation, utilisateurs et d'une procédure de mise à jour de cette documentation ;
- s'assurer que ces obligations fiscales sont contractuellement prises en compte avec les fournisseurs concernés : sous-traitance d'un développement (documentation), ASP ou infogérance (mise à disposition de l'administration), ...

6.5. Vérifier que la loi sur la propriété intellectuelle / logiciel « pirate » est connue et rigoureusement respectée :

- vérifier l'existence d'un inventaire des configurations logicielles ;
- évaluer/valider la procédure de mise à jour de cet inventaire

(une procédure automatique doit être privilégiée) ;

- effectuer des contrôles sur un échantillon de postes de travail ;
- sur la base de l'inventaire fourni, contrôler les justificatifs de licences.

3.2. AUDIT DE SECURITE

L'information est un actif précieux de l'Organisation. À ce titre, il faut la protéger contre la perte, l'altération et la divulgation. Les systèmes qui la supportent doivent quant à eux être protégés contre l'indisponibilité et l'intrusion.

La sécurité est une démarche globale de l'Organisation organisée autour d'une politique de sécurité. Il faut donc considérer les systèmes dans leur globalité et l'ensemble des acteurs.

Points de contrôle
1. Facteurs clés de succès
1.1. Une politique de sécurité est définie et correspond à l'activité de l'Organisation.
1.2. Une démarche de mise en œuvre de la gestion de la sécurité est adoptée et compatible avec la culture de l'Organisation.
1.3. La direction assure un soutien total et un engagement visible.
1.4. Les exigences de sécurité et les risques sont compris et évalués.
1.5. L'ensemble des responsables et des employés sont sensibilisés et informés.
1.6. Les lignes directrices de la politique de sécurité et des normes de sécurité de l'information sont distribuées à tous les employés et à tous les fournisseurs.
1.7. Les acteurs de la sécurité sont formés de manière appropriée.
1.8. Un système de mesure complet et mis en place afin d'évaluer l'efficacité de la gestion de la sécurité de l'information et pour collecter les suggestions d'amélioration.
2. Politique de sécurité
2.1. Il existe une politique de sécurité formalisée avec une implication de la direction générale et une définition claire des responsabilités.
2.2. La communication se fait à tous les utilisateurs sous une forme pertinente, accessible et compréhensible au lecteur.
2.3. Une revue régulière de la politique est réalisée afin de vérifier son adéquation avec : • les évolutions des activités de l'organisation et donc des risques ; • les changements technologiques ; • l'historique des incidents.
2.4. La démarche de sécurité inclut la totalité de l'informatique et non les seuls réseaux, serveurs et applications. Les imprimantes et téléphones sous IP, l'informatique technique et industrielle, l'informatique de gestion technique des bâtiments, celle de gestion des accès et temps de travail, etc. bénéficient sans exception ni zone d'ombre du dispositif de sécurité.
3. Organisation de la sécurité
3.1. Il existe une structure dédiée à la gestion de la sécurité de l'information : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité dans les unités.
3.2. Il y a une attribution claire des responsabilités.
3.3. Un propriétaire est désigné, il est responsable de la mise en œuvre et du suivi des évolutions à apporter.
3.4. Il existe des procédures d'autorisation de nouveaux matériels ou logiciels.

3.5. Il existe des procédures applicables à l'accès aux informations de l'organisation par des tiers :

- les accès par des tiers aux infrastructures de traitement de l'information sont contrôlés ;
- une analyse des risques a été menée ;
- des mesures de protection de l'information ont été établies et sont acceptées contractuellement par le tiers : clause de confidentialité, transfert de propriété, responsabilités, règles d'accès physique et logique, restitution ou destruction de l'information confiée, remplacement de collaborateur....

3.6. En ce qui concerne les modalités de protection de l'information confiée à des sous-traitants, il faut vérifier :

- la prise en compte des exigences de sécurité dans les conditions contractuelles : mesures prises pour sécuriser les données pendant l'échange et pendant la conservation par le sous-traitant, modalité de restitution ou de destruction de l'information confiée, possibilité pour le sous-traitant de faire appel à de la sous-traitance, plan de continuité, clause d'audit ;
- le respect des lois pour les données personnelles et la propriété intellectuelle.

3.7. Vérifier qu'il existe des modalités de réaction aux incidents de sécurité et aux défauts de fonctionnement :

- signalement rapide des incidents de sécurité ;
- signalement des failles de sécurité ;
- signalement du fonctionnement défectueux de logiciels ;
- capitalisation sur la résolution d'incidents ;
- processus disciplinaire.

3.8. Il existe une revue régulière de la sécurité des audits aussi bien internes qu'externes.

4. Classification et contrôle des actifs

4.1. Vérifier que les actifs sont inventoriés et hiérarchisés par valeur pour l'organisation.

4.2. Vérifier que pour tout actif important, un propriétaire est désigné et informé de ses responsabilités.

4.3. Vérifier qu'il existe un système de classification qui définit un ensemble approprié de niveaux de protection.

4.4. Vérifier que chaque actif a fait l'objet d'une étude visant à déterminer son niveau de classification.

5. Sécurité du personnel

5.1. Vérifier que les postes et les ressources sont définis :

- inclusion de la sécurité dans les responsabilités des postes ;
- sélection du personnel et politique de recrutement ;
- accords de confidentialité ;

5.2. Vérifier que les utilisateurs sont formés.

6. sécurité : gestion des communications et des opérations

6.1. Vérifier la documentation des procédures et les responsabilités opérationnelles.

6.2. Contrôler les modifications opérationnelles.

6.3. Vérifier l'établissement de procédures de gestion des incidents.

6.4. Vérifier la séparation des fonctions et des infrastructures.

6.5. Vérifier l'étude de sécurité en cas de gestion externe des infrastructures.

6.6. Vérifier les mesures de protection contre les infections logiques.

6.7. Vérifier les sauvegardes des données :

- réalisation régulière des copies de sauvegarde des données, des applications et des paramètres ;
- distinguer sauvegarde et archivage ;
- déterminer les périodes de conservation des données ;
- conserver plusieurs générations de sauvegardes ;
- stocker les sauvegarde en lieu sûr ;
- tester régulièrement les supports de sauvegarde ;
- tester régulièrement les procédures de restauration.

6.8. Vérifier les modalités de gestion des supports de données :

- tenir en lieu sûr tous les supports amovibles ;
- effacer de manière sécurisée le contenu des supports à réutiliser hors de l'organisation ;
- établir une procédure de mise au rebut des supports prévoyant leur destruction ;
- établir des procédures de manipulation des supports adaptées au niveau de sensibilité de l'information contenue.

6.9. Vérifier les mesures de sécurisation des échanges de données :

- définition d'accords portant sur les échanges d'informations et de logiciels entre les organisations ;
- sécurité du courrier électronique.

7. Conformité

7.1. Vérifier la conformité aux exigences légales et réglementaires :

- protection des données personnelles ;
- respect de la propriété intellectuelle ;
- conservation de l'information.

7.2. Effectuer des audits de sécurité réguliers :

- internes et externes ;
- revue systématique et tests empiriques (exemple : test d'intrusion) ;
- protection des outils d'audit des systèmes ;
- protection des rapports d'audit de sécurité.

8. Gestion des identifiants et des mots de passe

8.1. Vérifier qu'il y a un seul utilisateur par identifiant.

8.2. Vérifier que les identifiants inutilisés pendant un certain délai sont révoqués.

8.3. Vérifier que les règles de bases sont connues et mises en place :

- utilisation systématique ;
- le titulaire doit être le seul à connaître son mot de passe ;
- changement périodique ;
- règles de composition ;
- procédures en cas d'inactivation ou de perte.

9. Contrôle des accès

9.1. Vérifier la définition et la documentation de la politique de contrôle d'accès :

- exigences de sécurité des applications individuelles de l'organisation ;
- politiques de dissémination de l'information et d'autorisation d'accès ("besoin d'en savoir") ainsi que les niveaux de

sécurité et la classification de l'information ;

- obligations contractuelles concernant la protection de l'accès aux données ;
- profils d'accès standard des utilisateurs pour les catégories communes de travail ;
- distinction des règles obligatoires et des recommandations facultatives ;
- établissement de règles "tout est interdit sauf" plutôt que "tout est permis sauf" ;
- règles devant être validées par un responsable (séparation des fonctions).

9.2. Vérifier la gestion des accès utilisateurs :

- identification unique des utilisateurs (tous les utilisateurs) ;
- vérification que l'utilisateur a été autorisé par le propriétaire des informations ;
- suppression des droits d'accès d'un utilisateur ayant changé de poste ou quitté l'organisation ;
- contrôle périodique et suppression des codes d'identification utilisateurs redondants et des comptes qui ne sont plus utilisés ;
- non-réaffectation des codes d'identification ;
- attribution des privilèges aux individus sur la base de leurs "besoins minimum" par rapport à la fonction qu'ils remplissent ;
- examen régulier des droits d'accès utilisateur.

9.3. Vérifier l'utilisation de mots de passe et de systèmes de déconnexion automatique :

- tout compte utilisateur doit être protégé par un mot de passe ;
- engagement des utilisateurs à :
  - ne pas divulguer leur mot de passe ;
  - ne pas écrire leur mot de passe de façon trop évidente ;
  - ne pas stocker leur mot de passe dans une procédure automatique ;
  - changer leur mot de passe dès qu'ils le soupçonnent d'être compromis ;
- contrôler qu'un mot de passe temporaire est envoyé pour la première utilisation et qu'il est bien changé par l'utilisateur dès la première utilisation ;
- contrôler que les mots de passe temporaires sont transmis aux utilisateurs de manière sûre ;
- contrôler que le système impose un changement régulier du mot de passe ;
- contrôler que le système impose le choix de mots de passe robustes ;
- discipline utilisateur pour la déconnexion ;
- la déconnexion doit être automatique en cas d'inactivité prolongée.

9.4. Vérifier le contrôle des accès aux réseaux :

- authentification des utilisateurs pour les connexions externes ;
- protection des ports de diagnostic à distance et de

télémaintenance ;
- contrôle des flux (*firewalls*) ;
- cloisonnement.

9.5. Vérifier le contrôle de l'accès aux systèmes d'exploitation :
- identification / authentification des utilisateurs ;
- limitation du nombre de tentatives infructueuses ;
- enregistrement des tentatives infructueuses ;
- limitation des jours et heures de connexion ;
- affichage de la dernière connexion ;
- protection de l'accès aux utilitaires.

9.6. Vérifier le contrôle de l'accès aux applications :
- restriction des accès à l'information ;
- isolation des systèmes critiques.

9.7. Vérifier la surveillance des accès aux systèmes et leur utilisation :
- consignation des événements :
  - constitution des journaux d'audit :
    - ✓ qui, quand, quoi, d'où ;
- surveillance de l'utilisation des systèmes activités sensibles (opérations privilégiées, modification de la sécurité) ;
- alertes sur incident (violation, tentatives infructueuses, notification de *firewall* ou de sdi) ;
- utilisation anormale ou atypique des ressources ;
- auditabilité des journaux ;
- revue régulière des journaux ;
- synchronisation des horloges :
  - assure l'exactitude des journaux d'audit (éléments de preuve) ;

9.8. Vérifier la gestion de l'informatique mobile :
- contrôle d'accès aux ordinateurs portables ;
- protection des données stockées (chiffrement) ;
- protection contre les virus ;
- sauvegardes ;
- connexions automatiques à distance ;
- sensibilisation du personnel doté d'ordinateurs portables :
  - confidentialité du travail dans les lieux publics ou moyens de transport ;
  - surveillance du matériel contre le vol ;
  - espionnage industriel.

9.9. Vérifier les suites données aux incidents :
- vérifier les réactions des possesseurs des ordinateurs incidentés ;
- vérifier les modalités effectives de remontée de l'information sur l'incident, ses délais, son parcours, son format ;
- vérifier les mesures d'isolement du ou des ordinateurs incidentés ;
- vérifier l'effectivité des mesures de communication d'alerte ;
- vérifier l'effectivité des mesures d'enquête et de l'exploration menée pour identifier les failles du système ayant permis l'incident.
- vérifier les modalités et le contenu de la communication des rappels vers les utilisateurs à l'issue de la crise, ou des nouvelles consignes.

10. Développement et maintenance des systèmes

10.1. Exigences de sécurité des systèmes :

- expression des besoins, contrôle interne, piste d'audit, sécurité ;
- spécification détaillée des besoins, contrôle interne, piste d'audit, sécurité ;
- audit des spécifications ;
- recette des fonctionnalités de contrôle interne, piste d'audit, sécurité ;
- audit de la recette ;
- audit "post mise en place".

10.2. Sécurité des systèmes d'application :

- validation des données d'entrée : type, limites de valeur, liste de valeurs possibles ;
- contrôle des traitements : contrôles de sessions séquentielles, totaux de contrôle ;
- exhaustivité des traitements ;
- validation des données de sortie :
  - contrôle de plausibilité, rapprochement.

10.3. Protocole de recette :

- tests systématiques avant le passage en production ;
- utilisation d'un environnement différent de l'environnement de production ;
- participation des utilisateurs à la recette ;
- documentation de la recette et archivage ;
- séparation des fonctions développement/exploitation ;
- procédure de passage en production lors des maintenances correctives urgentes (journalisation des actions).

10.4. Sécurité des fichiers :

- contrôle des logiciels opérationnels : mise à jour uniquement par bibliothécaire, uniquement code exécutable, journal d'audit des versions ;
- protection des données d'essai des systèmes : banalisation des données de production, garder une copie pour rejouer les tests dans les mêmes conditions ;
- contrôle de l'accès aux bibliothèques de programmes sources : hors de la production, accès réservé aux développeurs autorisés, gestion des versions et conservation de l'historique des modifications.

Informations à collecter

Organisation :

- politique de sécurité ;
- normes et standards en vigueur ;
- personnes et équipes impliquées dans l'exploitation du réseau et du parc micro (administration, maintenance, sécurité, support utilisateur ; définition des responsabilités) ;
- procédures appliquées ou prévues (mode dégradé) ;
- plans (de sauvegarde, d'archivage, de secours, de reprise, etc.) ;
- interlocuteurs pour l'audit (informatique et utilisateurs).

Volumétrie :

- nombre d'utilisateurs ;
- volumes de données transmises ;
- taille des données sauvegardées.

Matériels :

- serveurs ;
- stations de travail ;
- équipements réseau (commutateurs, routeurs), firewalls ;
- matériel d'environnement (imprimantes, scanner et photocopieurs en réseau, téléphones IP).

Logiciels :

- systèmes d'exploitation ;
- middleware ;
- principales applications utilisées.

Communications :

- architecture du réseau (topologie) ;
- plan de câblage ;
- connexions avec l'extérieur.

3.3. AUDIT DE LA PRODUCTION INFORMATIQUE

Un audit de la fonction production consiste à analyser la capacité de l'organisation à exploiter les systèmes dans des conditions répondant aux besoins opérationnels définis par les directions utilisatrices. Il s'agit d'analyser l'adéquation des moyens humains, matériels, logiciels et organisationnels (procédures d'exploitation, de sauvegardes, …) mis en œuvre pour répondre aux enjeux de l'organisation en termes de disponibilité de ses applications, d'intégrité et de confidentialité de ses données et enfin de conformité aux besoins opérationnels des utilisateurs (notion de qualité de service).

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires.

Points de contrôle
1. Enjeux, engagements de service et suivi de la performance
1.1. S'assurer que les niveaux de services sur lesquels s'engage la production sont en adéquation avec les enjeux de disponibilité, d'intégrité et de confidentialité des différents systèmes.
1.2. S'assurer que les moyens organisationnels (ex : escalade), humains (ex : nombre et compétences des personnels d'astreinte), et matériels (ex : architecture redondante) permettent un respect des engagements de service.
1.3. Vérifier que les niveaux de service assurés par la production font l'objet de conventions de service comportant des indicateurs mesurables : valider le contenu des conventions de services. S'assurer que les principaux attributs de la prestation font l'objet d'indicateurs de mesure de la performance et d'objectifs quantifiés. Juger la pertinence des indicateurs et l'ambition des objectifs au regard des enjeux.
1.4. S'assurer que le suivi de la performance est un process continu : demander les derniers comptes-rendus à l'attention des utilisateurs. En cas de non-respect des objectifs de la convention de service, valider la pertinence des actions correctives entreprises.
Vérifier que les tableaux de bords de production font l'objet d'un suivi adéquat : se faire communiquer les tableaux de bords de production et juger de leur pertinence aussi bien que de leur complétude ; s'assurer de l'existence de procédures permettant à l'équipe de production de remédier aux éventuels problèmes identifiés par l'intermédiaire des tableaux de bords.
2. Organisation de la fonction production
2.1. S'assurer que la ligne de partage entre études et production est clairement définie et documentée.
2.2. Vérifier que l'organisation de la production correspond à une réponse adaptée aux besoins opérationnels de l'organisation : • comprendre la structuration du service production. Identifier les modalités de découpage des rôles et responsabilités (découpage par application, par technologie, par niveau de support …) et s'assurer qu'ils permettent de répondre de manière adéquate aux enjeux de disponibilité, de sécurité et d'intégrité ; • valider l'indépendance de la production par rapport aux études ; • vérifier l'existence de convention de service par application ;

- vérifier l'existence de moyens de communication normalisés entre production et autres acteurs de l'organisation ;

2.3. Vérifier que les technologies opérées sont suffisamment maîtrisées :

- identifier les différentes technologies utilisées, valider l'existence pour chacune d'entre elles des compétences suffisantes tant d'un point de vue qualitatif que quantitatif et, si la taille du service de production le justifie, des grilles croisées compétences / individus ;
- revoir les budgets formation et l'adéquation des formations avec les technologies actuelles et celles induites par le déroulement du plan informatique.

2.4. Vérifier qu'il existe une bonne maîtrise des différentes missions de la production :

- identifier le périmètre couvert par la production et en dériver les principales missions assumées ;
- valider la couverture de ces différentes missions dans les descriptions de postes ;
- se focaliser sur les aspects autres que l'opération des systèmes : ex : production d'indicateurs de pilotage, *capacity planning*, veille technologique, revue qualité, ...

3. Architectures matérielles et logicielles

3.1. Valider que performance et dimensionnement des composantes des systèmes de production font l'objet d'un suivi :

- étudier les tableaux de bords techniques en se focalisant sur les indicateurs de capacité réseau, CPU et média de stockage ainsi que de temps de réponse. Couvrent-ils les consommations moyennes et les pics d'activité ?
- valider la connaissance et le suivi dans le temps du déroulement de la journée de production avec ses goulets d'étranglement et ses marges de sécurité ;
- les budgets reflètent-ils des investissements nécessaires à l'augmentation de la capacité de traitement des architectures existantes ?

3.2. Valider l'évolutivité des architectures présentes. Étudier :

- la « scalabilité » des architectures ;
- la « modularité » des architectures ;
- le niveau de maturité/obsolescence des architectures opérées (date de fin de maintenance des systèmes et progiciels, versions des langages, ...).

3.3. Vérifier que le dimensionnement des architectures actuelles permet de répondre aux engagements de services (indicateurs de pilotage et de mesure de la performance).

3.4. Vérifier que les infrastructures ne sont pas manifestement surdimensionnées en regard des besoins actuels et prévisibles.

3.5. Vérifier que les configurations matérielles (redondance matérielle et réseau, architecture disques, *clustering* CPU, média de sauvegarde, …) permettent de garantir le niveau de disponibilité sur lequel la production s'engage.
Type de questions :

- les systèmes de disques ou de stockage d'information (SAN, …) prémunissent-ils contre des pertes d'information ?
- les sauvegardes, leur périmètre, et les temps de restauration sont-ils adaptés et en ligne avec les engagements de la production ?
- les accès réseaux sont-ils doublés et les architectures sont-elles doublées ?

4. Livraisons en production

4.1. Vérifier les conditions et procédures de livraisons en production. Valider la démarche de contrôle des livraisons en production et *a minima* les points de contrôles suivants :

- recette fonctionnelle entre études et utilisateurs (PV de recette) ;
- réalisation de tests d'intégration ;
- test des procédures et des packages de livraisons, y compris retour arrière ;
- sauvegarde des environnements impactés avant livraison ;
- livraison effectuée à un moment où un retour arrière est possible sans impacter le service client (le soir, le week-end, …) ;
- recette d'exploitation entre études et production (PV de recette).

4.2. Vérifier les conditions et procédures de livraisons en production. Valider le niveau de responsabilité de la production par rapport aux livraisons des études :

- la production a-t-elle un pouvoir de veto si elle estime qu'il n'y a pas de garantie quant au risque relatif à la livraison (tests non effectués, sources non fournies, livraison non packagée et non documentée, …) ;
- les études mettent-elles à disposition dans un environnement étanche les sources et la production prend-elle le relais pour les opérations ultérieures (compilations, paramétrage, …).

4.3. Vérifier la nature des tests effectués par la production. S'assurer que les machines et les environnements disponibles permettent de réaliser le cas échéant les tests suivants :

- test de montées en charge (volumétrie pour du transactionnel[2] et exploitabilité pour des traitements asynchrones) ;
- intégration technique portant non seulement sur de l'intégration au niveau du système mais aussi au niveau de l'interaction avec l'ordonnanceur de production et le système de remontée d'alerte ;
- tests d'interface avec d'autres applications ;
- intégration dans l'architecture réseau (filtrage de ports TCP/IP par un *firewall* par exemple).

[2] Traitement en temps réel

5. Exploitation et gestion des incidents

5.1. Vérifier le découpage de la journée de production en tâches clairement délimitées permettant la mise en œuvre de points d'arrêt. S'assurer que les traitements s'inscrivent dans la logique suivante :

- tout traitement impactant des données sensibles peut faire l'objet d'un retour arrière (*archivelog*, sauvegarde, *roll back*[3], *timestamp*[4]) ;
- un traitement modifiant des données commence par analyser la validité des données (syntaxe, *timeliness*, …) avant d'effectuer une mise à jour et permet de rejeter selon des règles connues les transactions ou les lots comportant des anomalies ;
- tout rejet possible par le système génère une alerte et est dûment couvert par une procédure de recyclage ;
- l'échec d'un traitement isolé n'empêche pas de respecter les délais de déroulement de la journée de production (temps de réalisation d'un traitement très inférieur aux marges de sécurité).

5.2. Vérifier la validité des assertions suivantes :

- les alertes sont remontées en temps réel à la console d'administration (système de gestion d'alerte - pull et push : la console vérifie le statut d'un système, un traitement peut remonter une alerte) ;
- les applications et les systèmes opérés génèrent des fichiers d'erreurs exploitables (*tracelog*, …) ;
- l'ordonnanceur de production ou les outils utilisés (batch d'exécution) permettent l'arrêt du déroulement des traitements en cas d'erreur grave ;
- le niveau d'automatisation de la production permet de décaler des jobs non critiques et de mesurer l'impact sur le chemin critique (i.e. le chemin critique de production et les marges de sécurité sont identifiés) ;
- les outils systèmes offrent des garanties comme intégrité et *timeliness* des fichiers intermédiaires (puits de données --> *Cortex Sink*) et capacité de retour arrière (*Roll Back* automatique de SGBD) si non pris en compte dans le chemin d'exploitation (sauvegarde intermédiaire) ou dans les traitements.

5.3. Vérifier le patrimoine documentaire utilisé par l'exploitation :
existe-t-il des guides de production par application ?

- le séquencement des tâches de production est-il correctement documenté (dans le robot ou sur papier) ?
- les différents points de reprise sont-ils clairement identifiés ?
- existe-t-il une main courante de production traçant tout événement anormal intervenu et les actions correctives entreprises ?
- existe-t-il un référentiel listant typologies d'incidents et actions de résolution à entreprendre ? (alimenté sur la base des anomalies résolues dans le passé).

[3] Annulation d'un ensemble de requêtes ou transactions réalisées sur une base de données transactionnelle

[4] Horodatage d'une donnée ou transaction

5.4. Analyser les procédures d'exploitation :

- existe-t-il une typologie claire de gravité d'incident ?
- existe-t-il une procédure d'escalade décrivant spécifiquement quels sont les moyens de résolution des problèmes (*troubleshooting*) à mettre en œuvre par chaque niveau et les délais régissant l'escalade. La procédure d'escalade permet-elle le respect des engagements de disponibilité (SLA) ?
- les actions à entreprendre en fonction du type d'incident sont-elles documentées (ex : fermer le transactionnel, faire une sauvegarde, générer un cliché (*snapshoot*) sur un environnement pour faire du débogage, vérifier un certain nombre d'éléments, …) ?
- les astreintes sont-elles explicites ? Couvrent-elles uniquement le support production ou incluent-elles les études ? Sont-elles en adéquation avec les engagements de disponibilité ?
- les compétences disponibles au sein de la production permettent-elles un support adéquat de tous les environnements ?

6. Procédure de sauvegarde et de reprise

6.1. Identifier les différentes sauvegardes effectuées et les croiser avec les besoins existants. Valider que toute sauvegarde répond à un besoin précis et que tous les besoins sont couverts :

- peut-on faire repartir l'exploitation à partir de sauvegarde sur site avec des caractéristiques de rechargement intégrant des besoins de forte réactivité (*mirroring*[5], *dump* (sauvegarde en masse) de données, …) ?
- gère-t-on un archivage spécifique pour répondre aux obligations de la loi de finances pour 1990 sur les comptabilités informatisées ?
- gère-t-on des sauvegardes externalisées permettant de se prémunir contre une perte de tout ou partie du SI ?
- les périmètres incorporés dans les sauvegardes permettent une reconstruction complète d'un système (OS, programmes, données).

6.2. Valider que les éléments suivants font partie intégrante des procédures de sauvegarde :

- plan de sauvegarde identifiant par serveur / application, le périmètre de sauvegarde (fichiers, programmes, paramètres, os,..) et la cyclicité ;
- acteurs (homme, système de sauvegarde) en charge de la réalisation et du contrôle des sauvegardes ;
- plannings prévisionnels de tests de restauration ;
- clauses de révision des procédures de sauvegardes et des

[5] Réplication en temps réel des données sur deux disques durs miroirs

périmètres (nouvelle livraison applicative, migration serveur, …) ;
- règle de remplacement et stockage des medias de sauvegarde.

6.3. Vérifier le bon suivi des procédures de sauvegarde :
- consulter les comptes rendus de sauvegardes et valider la prise en compte de tout incident mentionné ;
- vérifier les bordereaux d'entrée / sortie des media supportant les sauvegardes externalisées ;
- s'assurer que le dernier changement des media de sauvegarde est en ligne avec ce que préconise la procédure ;
- rapprocher le planning des livraisons en production et valider que les éventuelles modifications de périmètre ont bien été incorporées dans les procédures.

6.4. Se focaliser sur les aspects de restauration :
- s'assurer qu'il existe des procédures de restauration précisant les modalités selon lesquelles on peut remonter partiellement ou totalement un système en partant des sauvegardes.

6.5. Valider le suivi du planning prévisionnel de tests de restauration :
- consulter les comptes rendus des derniers tests de restauration ;
- regarder l'effectivité du plan d'action déroulant du résultat des tests de restauration ;
- rapprocher le planning de livraison applicative avec les procédures de restauration et valider que ces dernières sont à jour.

7. La maintenance du matériel et du logiciel de base

7.1. Valider la complète couverture des matériels critiques et logiciels de base par des contrats de maintenance adaptés. Vérifier les engagements de disponibilité et les contrats de maintenance hardware ainsi que les clauses d'exclusion de garantie :
- est-ce que tous les serveurs critiques sont couverts ? Si non, le fabriquant assure-t-il encore la maintenance de ce matériel ?
- en est-il de même pour les baies de disques et les éléments actifs de réseau ?
- les délais contractuels d'intervention et de réparation sont-ils en adéquation avec les engagements de disponibilité ? Les clauses de pénalités financières sont-elles réalistes et applicables ?
- les conditions physiques de stockage du matériel sont-elles susceptibles de faire appliquer les clauses de dégagement de responsabilité ? (température, poussière, hygrométrie,..) ?

7.2. Vérifier les engagements de disponibilité et les contrats de maintenance des logiciels de base ainsi que les clauses d'exclusion des garanties contractuelles :
- est-ce que tous les OS utilisés sont couverts par un contrat de maintenance ? Si non, l'éditeur assure-t-il encore la maintenance de la version utilisée et cette version est-elle compatible avec d'éventuels « *upgrades* » matériels ?
- en est-il de même pour les SGBD, robot d'exploitation et autres outils d'administration (remontée d'alerte,

administration réseau, …)

- les délais contractuels d'intervention et de réparation sont-ils en adéquation avec les engagements de disponibilité ? Les clauses de pénalité financière sont-elles réalistes et applicables ?

3.4. AUDIT DES APPLICATIONS INFORMATIQUES EN SERVICE

Une application informatique (« application software ») est un logiciel accompagnant, automatisant, ou se substituant à un processus ou une partie de processus de l'organisation. Une application comprend des programmes, des données, des paramètres, une documentation mais aussi des habilitations pour gérer les accès aux données et aux transactions de l'application.

L'audit d'une application peut avoir deux visées distinctes : l'audit de fiabilité et de sécurité ou l'audit d'efficacité et de performance. Un audit complet couvrira ces deux périmètres.

- ***L'audit de fiabilité et de sécurité*** a pour objectif d'émettre une appréciation motivée sur la fiabilité de l'outil informatique, c'est-à-dire sur la qualité du contrôle interne de l'application et la validité des données traitées et restituées. Ce type d'audit permettra de mettre en évidence d'éventuelles failles dans la chaîne de contrôle composée de contrôles programmés effectués par la machine et de contrôles manuels restant à la charge des utilisateurs.

- ***L'audit d'efficacité et de performance*** a pour objectifs d'apprécier l'adéquation de l'application aux besoins et aux enjeux de l'organisation, d'évaluer sa contribution à la création de valeur, d'évaluer sa performance et sa rentabilité et enfin d'évaluer sa pérennité et sa capacité d'évolution.

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires.

Points de contrôle
1. Audit de la sécurité et de la fiabilité : analyse des risques associés à l'organisation
1.1. Existe-t-il un comité informatique, présidé par la direction générale et au sein duquel les directions utilisatrices sont représentées et influentes (stratégie, contrôle et pilotage,..) ?
1.2. Existe-il, au sein de l'organisation, une « politique » relative aux applications, connue, partagée et mise en œuvre : • couvrant l'ensemble du cycle de vie de l'application (conception, exploitation) ; • favorisant la responsabilisation et l'appropriation par les utilisateurs de leur système d'information ? La notion de « propriété » d'application est-elle utilisée ?
1.3. Le rôle et les responsabilités des utilisateurs vis-à-vis de l'application sont-ils clairement identifiés et couvrent-ils l'analyse des risques, la définition des besoins de sécurité, la gestion des changements et des évolutions, l'administration de l'application ?
1.4. A-t-il été réalisé une analyse des risques, spécifique à l'application, qui a débouché sur la définition des besoins de sécurité (classification formelle des données et des traitements en termes de disponibilité, d'intégrité et de confidentialité) ?
1.5. Dans le prolongement de l'analyse des risques et de l'expression des besoins de sécurité, a-t-il été mis en œuvre un contrat de service (SLA) entre l'informatique et la direction utilisatrice ?
1.5. Indépendamment de l'application : • prendre connaissance et analyser le niveau de contrôle

interne et de séparation des tâches au sein de la direction utilisatrice ;

- évaluer le niveau de sensibilité des utilisateurs à la sécurité ainsi que le niveau de « maturité » de l'organisation vis-à-vis de ses systèmes d'information.

1.7. Existe-il un manuel d'administration de l'application, à jour et maîtrisé, comprenant notamment : mode d'emploi du manuel, présentation du module d'administration de l'application, droits d'accès « type » par poste, procédure de création / modification / suppression de droits d'accès, responsabilité d'autorisation, mode opératoire, documentation des pistes d'audit et nature des contrôles à réaliser, …

1.8. Vérifier l'existence de procédures formalisées imposant l'accord du « propriétaire » de l'application pour tout changement sur :

- les programmes de l'application (maintenance corrective et évolutive) ;
- la planification des traitements informatiques (batch, clôture, …) ;
- l'environnement technologique de l'application ;

Vérifier que l'administration est bien assurée par les utilisateurs.

1.9. Le « propriétaire » dispose-t-il d'un compte-rendu (*reporting*) mensuel « intelligible » de la performance de l'application, dans le respect du contrat de service ?

1.10. Existe-il un guide utilisateurs / manuel de procédures, diffusé, à jour et maîtrisé, comprenant notamment :

- mode d'emploi du manuel, présentation de l'application, mode opératoire, règles de gestion, écrans et zones de saisie, liste des messages d'erreurs, états de contrôle et d'exception, documentation des pistes d'audit ;
- description des contrôles programmés et des contrôles manuels compensatoires à chaque phase du traitement (mode opératoire, procédure d'escalade et/ou de recyclage des anomalies, délais de mise en œuvre, …).

2. Audit de la sécurité et de la fiabilité : Analyse des risques associés à l'application

2.1. L'accès aux ressources de l'application (données et transactions) est-il restreint par un système de gestion d'accès ?

2.2. Existe-t-il une procédure de gestion des profils utilisateurs de l'application placée sous la responsabilité du propriétaire de l'application (procédure de création / modification et suppression des droits d'accès) ? Un dispositif de SSO est-il mis en œuvre ?

2.3. Chaque utilisateur possède-t-il un identifiant qui lui est propre ? Vérifier qu'il n'existe pas de compte « générique » et que l'informatique (chef de projet) n'a que des accès en lecture au même titre que d'éventuels sous-traitants et éditeurs.

2.4. Le mot de passe associé à l'identifiant permet-il d'assurer une protection d'accès efficace (7 caractères minimum, gestion de l'historique des mots de passe sur 2 ans, contrôle de « trivialité », changement trimestriel des mots de passe, etc.) ?

2.5. Les tentatives de connexions infructueuses à l'application sont-elles enregistrées et contrôlées par le propriétaire de l'application? Sont-elles limitées ?

2.6. L'accès aux données et aux transactions de l'application peut-il être correctement paramétré en fonction des tâches des utilisateurs ou le système de confidentialité est-il basé sur le contrôle d'accès aux données ?

2.7. La séparation des tâches est-elle respectée dans le paramétrage des profils ?

- comparer les droits d'accès avec les fonctions des utilisateurs ;
- vérifier l'adéquation entre les droits et les profils ;
- vérifier que toutes les personnes ayant des droits d'accès sont toujours dans le service / l'organisation.

2.8. La piste d'audit sur le système d'administration de l'application est-elle assurée et régulièrement contrôlée ?

2.9. Tous les documents servant de base à la saisie sont-ils préparés, préformatés, complets et approuvés avant saisie ?

2.10. Les facilités de saisie, l'ergonomie de la saisie, les messages écrans et les contrôles de format sur les données permettent-ils d'éviter puis de filtrer les erreurs de premier niveau ? Y-a-t-il unicité de la saisie de l'information ?

2.11. Les contrôles de validation permettent-ils de détecter les doubles saisies, les saisies incomplètes, les incohérences (contrôle de vraisemblance et de rapprochement avec d'autres valeurs, contrôle de limite et d'étendue,…) et certaines erreurs de saisie (contrôle de sommation, totaux de contrôle pour les saisies de masse) ?

2.12. Utilise-t-on des « brouillards » de saisie pour validation par réconciliation avec les documents sources ? Cette validation est-elle indépendante ?

2.13. Les saisies des données « sensibles » et notamment les données permanentes et les paramètres de l'application sont-elles autorisées, complètes et exactes ?

2.14. Les opérations effectuées sur des données sensibles sont-elles l'objet d'une piste d'audit suffisante et régulièrement analysée ?

- identité de l'auteur de l'opération ;
- entité / fichier /donnée sur laquelle l'opération a été effectuée ;
- date et heure des événements ;
- valeur avant et après l'opération.

Objectifs de contrôle de la piste d'audit :

- évaluation de la qualité des pistes (couverture, exploitabilité, …) ;
- évaluation de la sécurité des pistes (sécurité de ses constituants : OS, SGBD, ...) ;
- évaluation de la gestion des pistes (procédures de contrôle, archivage, …).

2.15. Les procédures de transmission de fichiers en entrée assurent-elles l'exhaustivité et l'exactitude des informations transmises (contrôles systèmes) ?

2.16. Les contrôles mis en œuvre lors de l'intégration des données par fichiers à l'application sont-ils suffisants et identiques à ceux mis en œuvre dans le cadre d'une saisie transactionnelle (contrôles applicatifs) ?

2.17. Le système prévoit-il de conserver toutes les données rejetées dans un fichier d'anomalies protégé et de les éditer en vue d'un contrôle et d'un recyclage ?

2.18. Les données rejetées sont-elles analysées et corrigées dans des délais raisonnables et compatibles avec les délais de validation des traitements ?

2.19. Les corrections des données rejetées subissent-elles les mêmes contrôles que les données initiales, et jouissent-elles d'une piste d'audit suffisante ?

2.20. Toutes les opérations de mise à jour des données sensibles sont-elles journalisées (transactions, traitements batch) ?

2.21. Toutes les opérations de mise à jour des données sensibles sont-elles journalisées (transactions, traitements batch) ?

2.21. Rapproche-t-on les totaux de contrôle de fin de journée et la différence est-elle analysée au travers des transactions journalisées ?

2.22. Des contrôles automatiques périodiques, notamment de vraisemblance, sont-ils effectués afin de vérifier l'intégrité des montants gérés par l'application (niveau applicatif ou base de données) ?

2.23. La couverture, le contenu et la distribution des états de sortie de l'application sont-ils adaptés aux enjeux et à l'organisation de l'organisation ?

2.24. Effectuer une revue détaillée des états disponibles et de leur destinataire et vérifier que chaque nouvel état de sortie fait l'objet d'une procédure de recette.

2.25. Chaque utilisateur dispose-t-il du bon niveau d'information et de moyen de contrôle adapté ?

2.26. La distribution des états de sortie est-elle sous contrôle (existence d'une procédure permettant l'identification et la validation formelle des destinataires) et leur niveau de confidentialité assuré ?

2.28. Les contrôles utilisateurs des états de sortie font-ils l'objet de procédures formalisées (guide de procédures), connues et appliquées ?

2.29. Les procédures de validation des résultats (Qui, Quand, Comment), de classement et d'archivage des états produits sont-elles adaptées, formalisées, connues et appliquées ?

- existence d'une procédure, identification des responsables, délai de mise à disposition des états et délai de validation, procédures à suivre en cas d'incident.

2.30. Lorsque l'application est la juxtaposition de plusieurs modules, l'homogénéisation des codifications et des règles de gestion a-t-elle été assurée ?

2.31. L'intégrité et l'exhaustivité des données transmises entre les différents modules de l'application et/ou à des applications en aval sont-elles assurées ?

3. Audit de la sécurité et de la fiabilité : analyse des risques associés à la fonction informatique

3.1. Au sein du service informatique, les tâches relatives au développement et à l'exploitation de l'application sont-elles séparées ?

- Prendre connaissance de l'organigramme de la DSI, des descriptions de travaux (*Job description*) et de la procédure de mise en production.

3.2. L'accès aux bibliothèques de production (données et programmes) est-il interdit aux analystes-programmeurs ?

- Sans réelle étanchéité des environnements de développement et de production, la séparation des tâches reste toute théorique. Analyser les droits d'accès. Un accès en lecture pour les chefs de projets est généralement admis.

3.3. La séparation des tâches est-elle maintenue et assurée en cas d'absence d'un salarié (maladie, vacances,..) ?

3.4. L'équipe actuelle en charge de la maintenance (interne ou externe) a-t-elle une maîtrise suffisante de l'application et les moyens de la faire évoluer ?

3.5. Existe-t-il une procédure formalisée et standard de maintenance de l'application validée par l'informatique et la maîtrise d'ouvrage concernée ?

3.6. Les nouvelles versions (développement interne, progiciel) sont-elles systématiquement testées puis recettées dans un environnement dédié avant d'être livrées à l'exploitation ?

3.7. Existe-t-il une procédure formalisée de transfert des programmes entre les environnements de recette et d'exploitation ?

3.8. La documentation de l'application est-elle systématiquement mise à jour après chaque intervention de maintenance ?
3.9. Les corrections effectuées en urgence sur les programmes sont-elles effectuées dans un cadre bien défini et formalisé ? Font-elles l'objet d'un rapport systématiquement revu par la direction informatique ?
3.10. Un logiciel de contrôle de programmes sources et de programmes exécutables est-il utilisé pour identifier et tracer toute modification effectuée (piste d'audit) ?
3.11. Les travaux batch de l'application, qu'ils soient périodiques ou à la demande, sont-ils systématiquement planifiés et formellement validés par le responsable d'exploitation et par le responsable utilisateur ?
3.12. Existe-t-il une procédure de contrôle des traitements batch et d'archivage des comptes-rendus d'exécution ?
3.13. La gestion des incidents en général et les procédures d'urgence en particulier sont-elles définies et correctement documentées ?
3.14. La documentation d'exploitation est-elle à jour, dupliquée, protégée et inclut-elle les procédures de gestion des incidents et de reprise / redémarrage ?
3.15. Vérifier l'existence et l'application d'un Contrat de Service (SLA) pour l'application : • vérifier que le SLA couvre les besoins de disponibilité, d'intégrité et de confidentialité de l'application et de ses données ; • valider que les engagements de service sont en adéquation avec l'analyse des risques.
3.16. Vérifier que les moyens organisationnels (ex : escalade, astreintes, procédures et *reporting*, ...), humains (effectif, compétences des personnels), matériels et logiciels (ex: architecture redondante, outil de mesure, ...) permettent le respect des engagements de service et la mesure rigoureuse du niveau de service.
3.17. Évaluer le niveau de service par l'analyse des tableaux de bord.

3.18. Les procédures de sauvegarde et de reprise de l'application sont-elles satisfaisantes et répondent-elles aux enjeux de l'application et aux engagements de service de l'informatique ?
3.19. Une partie des sauvegardes est-elle stockée à l'extérieur de l'organisation (banque, société spécialisée) selon une périodicité adaptée aux enjeux ?
3.20. En cas de sinistre grave, existe-t-il un plan de secours en adéquation avec les besoins et les enjeux (plan d'urgence, plan de repli, plan de reprise) ? • vérifier le dimensionnement des moyens mis en place ; • déterminer les faiblesses du plan de secours existant (axes d'analyse : étude d'impact financier, sites de repli, plan de secours informatique, plan de secours télécom, sauvegardes des documents, procédures, organisation, logistique).
3.21. Ce plan est-il périodiquement testé et mis à jour ?
3.22. L'organisation dispose-t-elle d'un responsable sécurité et d'une politique formalisée en matière de sécurité informatique, conforme à la réglementation ? Cette politique couvre-t-elle la fonction informatique ?
3.23. Les accès aux commandes système, aux bibliothèques et bases de données de production sont-ils protégés (logiciel de contrôle) et limités au personnel d'exploitation ?
3.24. Les accès aux logiciels de base et utilitaires sensibles sont-ils contrôlés et systématiquement "tracés" ?
3.25. Existe-t-il des procédures de contrôle périodique des accès aux ressources de l'application (analyse des « logs[6] » par le responsable de la sécurité) ?

[6] Historique d'événement, et par extension fichier contenant cet historique

4. Audit d'efficacité et de performance: adéquation de l'application aux besoins

4.1. Le projet s'inscrit-il dans le schéma-directeur du système d'information et ce dernier est-il aligné avec le schéma directeur de l'organisation ?

4.2. Évaluation de l'alignement stratégique de l'application :

- vérifier l'existence d'une maîtrise d'ouvrage « forte » et impliquée ;
- vérifier que la direction générale a participé à l'étude préalable et a validé le projet et notamment l'analyse coûts/bénéfices ;
- vérifier que le cahier des charges de l'application prend en compte tous les aspects du problème posé et du domaine fonctionnel considéré ; dans le cas contraire, vérifier que le management avait connaissance de ces lacunes lors de la validation des spécifications ; vérifier que les choix effectués ne compromettent pas l'intégration des fonctionnalités complémentaires dans une phase ultérieure ;
- vérifier que le projet s'intègre de façon satisfaisante dans le système d'information existant (intégration technique et fonctionnelle) et que l'unicité des référentiels de l'organisation est assurée (bases clients, produits, entités, fournisseurs, référentiel comptable, …) ;
- sur la base du bilan de projet (lorsque qu'il existe), vérifier que le projet a atteint ses objectifs et couvre tous les aspects du domaine fonctionnel ; le cas échéant, analyser les écarts et vérifier qu'ils ont été portés à la connaissance de la direction générale.

4.3. Les utilisateurs ont-ils été suffisamment associés à la définition des spécifications ou au choix de la solution puis aux évolutions successives ?

4.4. Les utilisateurs réalisent-ils toutes leurs tâches dans l'application (évaluation du taux d'automatisation des opérations) ?

4.5. Sinon, maintiennent-ils des systèmes parallèles (ancien système, tableurs) en dehors de l'application ? Existe-t-il des saisies multiples ?

4.6. Adéquation aux besoins des utilisateurs :

- la totalité des fonctionnalités de l'application est-elle utilisée et maîtrisée par les utilisateurs ?
- l'ergonomie de l'application est-elle satisfaisante ? Par exemple, la saisie d'une transaction récurrente est-elle suffisamment productive (nombre d'écrans optimisé, saisie assistée, temps de réponse acceptable, …) ?
- les rapports issus du système répondent-ils convenablement aux besoins des utilisateurs ? En particulier chaque niveau de management dispose-t-il de l'information qui lui est nécessaire (adéquation à l'organisation) ?
- le support utilisateur (technique et fonctionnel) est-il satisfaisant et adapté aux utilisateurs et aux enjeux ?
- la documentation utilisateur est-elle adaptée, complète, accessible et permet-elle une utilisation optimale de l'application ?
- la formation des utilisateurs est-elle suffisante, adaptée et périodique, notamment pour une activité où le « turn-over » est important ?
- existe-t-il des enquêtes périodiques de satisfaction auprès des utilisateurs ? À l'aide ou non de ces enquêtes, évaluer le

niveau de satisfaction des utilisateurs (performance de l'application, appropriation et maîtrise, qualité de la formation et du support, absence de phénomène de rejet, ...) ?

5. Audit d'efficacité et de performance : analyse de la performance et de la rentabilité

5.1. Une évaluation de la rentabilité de l'investissement a-t-elle été établie préalablement au développement ou à l'acquisition de l'application ?

5.2. Cette évaluation a-t-elle intégré les coûts de déploiement mais aussi les coûts d'exploitation/charges récurrentes ?

5.3. A-t-on étudié sérieusement les offres du marché (progiciel) avant de se lancer dans un développement spécifique ?

5.4. Les délais de mise en œuvre de l'application sont-ils « raisonnables » (impact d'un éventuel « effet tunnel ») et conformes au planning initial ?

5.5. Un bilan post-projet a-t-il été effectué afin de mesurer l'atteinte des objectifs ?

5.6. La réduction des charges (notamment de personnel et d'exploitation) et/ou des délais (délais de traitements, délais de clôture, …) est-elle conforme à la réduction attendue lors de l'étude préalable ?

5.7. A-t-on constaté des améliorations non quantifiables, définies ou pas lors de l'étude préalable (amélioration de la sécurité, du service client, ...) ?

5.8. A-t-on réalisé une réingénierie des processus (*Business Process Reengineering* (BPR) ou une étude d'organisation préalablement à la rédaction du cahier des charges ?

5.9. Les processus métiers sont-ils performants et optimisés (rechercher toute source d'amélioration possible) ?

5.10. Les traitements sont-ils performants et les données cohérentes et fiables (voir guide d'audit « Fiabilité et Sécurité d'une application ») ?

5.11. L'architecture technique est-elle adaptée et optimisée, notamment les bases de données (bon dimensionnement des configurations, gestion des évolutions techniques, personnalisation (*tuning*) des bases de données, …) ?

5.12. A-t-on mis en place des indicateurs de performance et un contrat de service adaptés aux enjeux entre l'informatique et les utilisateurs :

- disponibilité de l'application, le cas échéant par plage horaire ;
- temps de réponse, le cas échéant par transaction et traitement sensibles ;
- gestion des incidents et du support utilisateurs, fiabilité des traitements par lots (*batch) ;*
- gestion des demandes de maintenance et gestion des droits d'accès ;
- continuité d'exploitation et site de back-up.

5.13. Les outils de mesure de la performance et les tableaux de bord sont-ils adaptés aux besoins et aux indicateurs, sans contestation possible ?

6. Audit d'efficacité et de performance : analyse de l'évolutivité/pérennité de l'application

6.1. Les technologies utilisées sont-elles conformes aux standards de l'organisation ?

6.2. Le logiciel est-il de conception récente et fondé sur des technologies portables, non obsolètes et évolutives (matériel, OS, SGBD, outils de développements, …) ?

6.3. Les technologies utilisées sont-elles matures et suffisamment répandues sur le marché (Linux, J2EE, .net,..) ? Les compétences existent-elles sur le marché notamment dans le contexte d'un déploiement à l'international ?

6.4. Les technologies utilisées ont-elles suffisamment de marge pour faire

face à un nombre croissant d'utilisateurs et de transactions (cf. Business Plan) ?
6.5. L'application est-elle techniquement et fonctionnellement intégrée dans le SI ?
6.6. L'application est-elle modulaire, paramétrable et conceptuellement adaptée aux éventuelles évolutions de l'activité, notamment : • capacité d'adaptation à une internationalisation (multilingue, multidevise et multiprotocole, ...)? • capacité d'intégrer une nouvelle entité juridique, un nouveau produit, un nouveau métier, … ? • capacité de « filialiser » un métier de l'Organisation ou de décentraliser certaines activités ? • capacité d'un déploiement massif (client léger versus client lourd, ...) ?
6.7. L'application évolue-t-elle régulièrement par versions successives ?
6.8. Le volume des demandes de maintenance évolutive est-il « normal » (en fonction de l'âge de l'application) et de maintenance corrective « raisonnable » (20-25% max de la maintenance dans les 2 premières années) ?
6.9. Si l'application est de conception ancienne, la structure en charge de la maintenance (interne ou externe) offre-t-elle des garanties suffisantes de pérennité de l'application (niveau de documentation, taille, ancienneté et compétence des équipes, solidité financière du sous-traitant, ...) ?
6.10. Le niveau de dépendance vis-à-vis de cette structure est-il raisonnable ?
6.11. L'éditeur a-t-il des références significatives dans le même secteur d'activité et dans des organisations de taille et de complexité équivalente ?
6.12. La version du progiciel installée dans l'organisation est-elle mature et utilisée dans un nombre significatif d'organisations ?
6.13. A-t-on procédé à des développements spécifiques limités qui ont respecté les points d'interface et les normes préconisées par l'éditeur ? En particulier, les sources du progiciel, n'ont-ils pas été modifiés ?
6.14. Existe-il un club utilisateurs où l'Organisation est présente et influente ?
6.15. A-t-on souscrit un contrat de maintenance avec l'éditeur ?
6.16. Les redevances de maintenance sont-elles régulièrement payées ?
6.17. Le contrat prévoit-il une clause dite d' « *Escrow Agreement* » permettant de disposer des sources, auprès d'un tiers de confiance, en cas de défaillance de l'éditeur ?
6.18. Les montées de versions sont-elles régulièrement effectuées ?
6.19. Dispose-t-on d'un engagement ou d'une visibilité suffisante de la pérennité du progiciel (notamment en cas de gel des évolutions ou de l'état technique) ?

3.5. AUDIT DU SUPPORT UTILISATEURS ET DE LA GESTION DU PARC

La mission de la fonction support est orientée autour de deux axes :

- fournir l'assistance et le support aux utilisateurs des systèmes d'information et améliorer en permanence leur niveau de satisfaction ;
- améliorer la performance globale des systèmes.

La performance d'un centre d'assistance (*help-desk*) ainsi que ses répercussions sur la productivité des utilisateurs doivent être évalués. Elle doit permettre d'identifier les domaines sur lesquels il semble possible d'accroître la productivité des utilisateurs, notamment les besoins en formation.

Il est nécessaire que la fonction de support d'une part anticipe ses besoins et dimensionne convenablement ses équipes et, d'autre part, contribue à la mise en place de règles de gestion du matériel et des applications informatiques de l'organisation en analysant le retour d'expérience.

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires.

Points de contrôle
1. Fonction support : audit fiabilité et sécurité
1.1. Quelle structure de centre d'assistance (*help-desk)* (HD) est mise en place ?
1.2. Existe-t-il une procédure de gestion des demandes, diffusée et connue des utilisateurs ?
1.3. Quelle est la procédure d'escalade mise en place ?
1.4. Quelle est la couverture géographique du HD ?
1.5. Quelle est la couverture fonctionnelle du HD ?
1.6. Un outil est-il implémenté pour la prise d'appel et le suivi des tickets ?
1.7. Quelles sont les critères à renseigner pour la qualification des tickets ?
1.8. Existe-t-il une liste de questions à dérouler lors d'un appel afin d'identifier au mieux la demande de l'utilisateur ?
1.9. Les problèmes sont-ils gérés ? Si oui quel est le processus ?
1.10. Les incidents de production de nuit sont-ils saisis aussi dans l'outil ?
1.11. Quels sont les comités mis en place pour suivre les incidents et leur résolution ? Qui participe ? Comment sont suivies les actions ?
1.12. Si le HD est externalisé, existe-t-il un contrat de service ?
1.13. Quels sont les indicateurs pour suivre le contrat de service ?
1.14. Y-a-t-il un planning systématique concernant les mises en production ?
1.15. Interroger le DSI, le responsable HD, des utilisateurs, l'équipe HD – si possible, participer « à la vie du HD ».
1.16. Demander des extractions de la base de ticket : • vérifier le nombre, la complétude des critères, l'adéquation de la qualification, la description de l'incident ;

• analyser les délais de clôture ; • analyser la criticité moyenne des tickets.
1.17. Demander les *reporting* de suivi.
2. Fonction support : audit d'efficacité et de performance
2.1. Existe-t-il une aide à la saisie pour la saisie des tickets ?
2.2. Existe-t-il des revues qualité pour la saisie des tickets ?
2.3. Quelle est la procédure de mise à jour de la base de connaissance ?
2.4. Les appels sont-ils enregistrés ?
2.5. Des études de satisfaction sont-elles réalisées auprès des utilisateurs ?
2.6. Existe-t-il une évaluation de l'équipe HD ? Notamment pour les prestataires pour évaluer leur niveau de connaissance ?
2.7. Les certifications (ITIL, ISO, COBIT) sont-elles encouragées au sein de la DSI, du HD en particulier ?
2.8. Interroger le DSI, le responsable HD, des utilisateurs, l'équipe HD – si possible, participer « à la vie du HD ».
2.9. Demander la stratégie de formation des utilisateurs et de l'équipe *Help-Desk*.
2.10. Demander les *reportings* de suivi.
2.11. Demander les études de satisfaction.
3. Gestion du parc matériel et logiciel : audit fiabilité et sécurité
3.1. Quelle est la procédure de déploiement des mises à jour, d'un nouveau logiciel ?
3.2. Quels sont les outils mis en place pour gérer les versions des logiciels ?
3.3. Quels sont les outils mis en place pour gérer le matériel informatique ?
3.4. L'installation des PC / portables est-elle faite à partir d'un master (configuration minimum et standardisée) ?
3.5. Existe-t-il un processus spécifique pour le suivi des mises à jour sur les portables ?
3.6. Le déploiement de nouveaux logiciels ou mises à jour est-il possible à distance ? (utile pour les utilisateurs nomades).
3.7. Est-il possible pour le HD de prendre la main à distance ? Si oui, quelle est la procédure ?
3.8. Comment est géré le parc informatique ? Quel type de machine ? Quel outil ?
3.9. L'inventaire du parc informatique comprend-t-il la localisation des machines ?
3.10. Les logiciels "non officiels" sont-ils répertoriés et suivis ?
3.11. Les utilisateurs sont-ils sensibilisés à la sécurité informatique, notamment à l'installation de logiciel "non officiel" ?
3.12. Faire des copies d'écran ou d'extraction des outils de suivi des mises à jour/déploiement. Vérifier sur les postes utilisateurs les versions antivirus, firewall, version Windows, version IE.
4. Gestion du parc matériel et logiciel : audit d'efficacité et de performance
4.1. Comment est effectué l'inventaire des licences (logiciel, version, date de mise en production, nombre d'utilisateurs) ?
4.2. Outils de type SAM (*Software Asset Management*) sont-ils déployés ?
4.3. Existe-t-il des revues régulières des licences ?
4.4. Existe-t-il une base de données de gestion de configuration de type CMDB (*Configuration Management DataBase*) ?
4.5. La DSI est-elle sensibilisée aux enjeux de la maîtrise des licences ? (notamment en cas de contrôle) ?
4.6. Des audits sont-ils réalisés ?
4.7. Une politique logicielle existe-t-elle ?

3.6. AUDIT DE LA FONCTION ÉTUDE

Les études sont une fonction sensible de la DSI, en charge du développement et de la maintenance des applications informatiques. La fonction étude est en charge de la conception et de la réalisation des applications, de leur test, de leur mise en œuvre (avec la production) et de leur maintenance (corrective, réglementaire et évolutive).

Son audit consiste à analyser sa capacité à assurer la maintenance du patrimoine applicatif existant, conduire ou accompagner les évolutions à venir du système d'information conformément au plan ou au schéma directeur informatique. Il faut veiller à ne pas confondre audit des études avec audit de projet. L'audit d'un projet s'adresse à une organisation temporaire et sur mesure, tandis que l'audit des études s'adresse à une structure permanente de l'Organisation.

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires.

Points de contrôle
1. Activité de pilotage
1.1. La ligne de partage entre études et production est-elle clairement définie et documentée ?
1.2. Existe-t-il une cellule dédiée en charge du suivi et du contrôle des projets et des ressources (gestion des plannings et des budgets, suivi des temps et des coûts) ?
1.3. Vérifier l'existence d'une procédure de planification détaillée par projet et/ou par ressource (en fonction des besoins et des enjeux : taille des équipes, nombre et nature des projets) : • vérifier l'existence et l'utilisation d'un outil de gestion de projet (PMW, Primavera, MS-Project…) ; • vérifier l'existence d'une méthode d'évaluation des charges ; • vérifier l'adéquation des outils et procédures aux besoins et enjeux ; • vérifier que la planification offre une visibilité suffisante de la charge des études (12 mois) ; • vérifier que pour les nouveaux projets, la planification couvre l'ensemble du projet, c'est-à-dire que l'on se place dans une logique projet et non dans une simple logique d'occupation des ressources (gestion du chemin critique, engagement sur une date butoir « *deadline* », ...).

1.4. Vérifier que la procédure de planification est nominative et suffisamment détaillée pour permettre une bonne visibilité du taux prévisionnel d'occupation des ressources :

- vérifier que les projets/travaux sont découpés en tâches élémentaires gérables ;
- vérifier la cohérence transversale de la planification en fonction des ressources disponibles et s'assurer que la planification prend en compte les congés et la formation (utilisation moyenne des ressources de l'ordre de 190-200 j/an) ;
- vérifier tout particulièrement l'existence de marges de sécurité sur le chemin critique.

1.5. Vérifier l'existence d'une procédure périodique (hebdomadaire à mensuelle en fonction des enjeux), de suivi de l'activité et de mise à jour du planning, articulée autour de :

- l'utilisation de « *time sheet* » nominatif (relevé d'activité) ;
- la saisie des temps passés et du « taux de réalisation » par tâche afin d'identifier le « reste à faire » et d'anticiper toute dérive des projets (suivi du chemin critique) ;
- une procédure d'alerte en cas de dérapage du projet pour prise de décision (augmentation des délais ou affectation de ressources additionnelles) ;
- la diffusion de l'état d'avancement des travaux et du nouveau planning des Études.

1.6. Pour les travaux de maintenance, la charge de réalisation (en jours/homme) est-elle systématiquement rapprochée de l'estimation initiale afin d'une part, d'affiner les méthodes d'évaluation des demandes et, d'autre part, de mesurer la productivité relative des développeurs ?

1.6. Vérifier l'existence d'un tableau de bord mensuel de l'activité des études offrant une bonne visibilité de l'activité actuelle et à venir des études :

- situation du portefeuille des demandes de maintenance et évaluation de la charge globale prévisionnelle permettant d'anticiper les besoins de sous-traitance ;
- états d'avancement des projets, nouveaux plannings et analyse des risques ;
- suivi budgétaire (mois et année glissante (ytd)) couvrant les ressources internes et la sous-traitance ;
- taux d'occupation des ressources, absentéisme, évolution de la productivité, … ;
- suivi de l'évolution des écarts de charges de développement « estimées / constatées » et suivi des engagements de mise en production (dates), ...

1.8. Ce tableau de bord est-il communiqué et analysé par le Comité informatique ?

2. Activités opérationnelles

2.1. Valider l'existence d'une MOA forte et d'une fonction études « limitée » à la MOE :
- le rôle et les responsabilités des études sont-ils définis dans la charte informatique ou dans les plans d'assurance qualité des projets ;
- existe-t-il des « contrats de service » entre les études et les utilisateurs ?

2.2. Évaluer le rôle du Comité Informatique dans le contrôle de l'activité des études :
- gestion des priorités de développement et arbitrages entre directions ;
- suivi des projets et de l'état d'avancement des travaux, suivi de la performance.

2.3. Évaluer la qualité du « contre poids » de la production et de l'équilibre entre ces deux fonctions de la DSI :

- cet équilibre passe-t-il par une réelle séparation des tâches et l'étanchéité des environnements, rendant la production incontournable pour les mises en production ?

2.4 Vérifier que l'équipe actuelle en charge de la maintenance (interne ou externe) a la maîtrise suffisante des applications et les moyens de la faire évoluer :

- compétences techniques adaptées (analyser les curriculum vitae et les profils en fonction des technologies utilisées, vérifier la présence des concepteurs, ...) ;
- effectifs suffisants et motivés (analyser l'historique de la DSI, les rémunérations, le « turn-over », analyser le portefeuille des demandes de maintenance, ...) ;
- existence des sources et des compilateurs et de la documentation des applications ;
- évaluer le risque d'une éventuelle dépendance vis-à-vis d'une ou plusieurs personnes.

2.5. Revoir les budgets formation/recrutement et leur adéquation avec les technologies actuelles et celles induites par le déroulement du plan informatique. Les profils et compétences existants, les budgets de formation et les prévisions de recrutement sont-ils adaptés aux enjeux et à l'évolution des nouvelles technologies ?

2.6. Existe-t-il une procédure standard et formalisée de maintenance, basée sur :

- un formulaire de demande de maintenance dûment complété (besoins, priorités, ...), validé par le « propriétaire » de l'application et centralisé par les études ?
- une estimation des charges, une consolidation des demandes puis une procédure formelle de validation des priorités (implication éventuelle du comité informatique) ?
- un retour vers l'utilisateur des demandes valorisées (temps, coûts) avec une date prévisionnelle de mise en œuvre ?
- une affectation et une planification détaillées des demandes ?

2.7. Pour la maintenance évolutive, le « *versionning*[7] » (2 à 3 par an) est-il préféré à la maintenance « au fil de l'eau » ? Approche plus efficace et risque de régression réduit.

2.8. Les nouveaux programmes/versions sont-ils systématiquement testés puis recettés dans un environnement dédié avant d'être livrés à l'exploitation ?

2.9. Vérifier l'existence d'un bon niveau de séparation des tâches et des environnements entre les études et la production :

- vérifier l'existence de *job description* et le niveau de séparation des tâches ;
- vérifier que les études disposent de machines de développement et de test, dédiées et sécurisées dont les caractéristiques et états techniques sont similaires à celles des machines de production ;

[7] Regroupement d'une série d'évolutions mineures, permettant d'éviter des modifications trop fréquentes d'une application.

- vérifier l'existence d'une procédure de recette entre les études et l'exploitation ;
- vérifier l'existence et la qualité de la procédure de transfert des programmes entre les environnements de développement et d'exploitation ;
- vérifier que le niveau de séparation des tâches n'est pas dégradé en cas d'absence de membres des études et/ou de production (profil administrateur, mot de passe, …).

2.10. La documentation de l'application est-elle systématiquement mise à jour après chaque intervention de maintenance ? Vérifier dans les programmes l'existence d'historique des modifications sous forme en commentaires.

2.11. Les corrections urgentes (bug bloquant de gravité 1) sont-elles tracées (logs) et effectuées dans un cadre bien défini et font-elles l'objet d'un rapport systématique revu par la DSI (responsable des études, production, assurance qualité, …) ?

2.12. Pour les environnements obsolètes, s'assurer que les langages et compilateurs sont toujours opérationnels et maintenus (assembleurs, cobol, …).

2.13. Pour une application donnée, rechercher de façon exhaustive les éventuels programmes objets sans programmes sources correspondant.

3. Activités opérationnelles : le développement des spécifiques

3.1. Utilise-t-on des méthodes et outils de conception et de modélisation d'application ? (UML, Rational Case, ...). Ces outils et méthodes sont-ils adaptés, maîtrisés et partagés par l'ensemble des équipes concernées, la formation est-elle adaptée ?

3.2. Existe-t-il des normes de programmation et de codification dont les règles sont formalisées dans un manuel à l'attention des programmeurs ? Vérifier l'application de ces normes (revue de code).

3.3. Utilise-t-on un logiciel de gestion de version de programmes afin d'identifier et de tracer toute modification de programme et un outil de gestion des configurations logicielles afin d'en maîtriser les évolutions (*Rational Clearcase*, …) ?

3.4. Utilise-t-on une démarche standardisée d'assurance qualité couvrant les aspects suivants : organisation, méthodes, outils et procédures de développement, gestion des livrables, plannings des projets, procédures de suivi et de *reporting*, documentation ?

3.5. Existe-t-il une documentation « études » structurée, claire, tenue à jour comportant un index de la documentation, une cartographie générale et détaillée des applications, des spécifications détaillées par application, des dossiers d'architecture technique par application (MCD, tableaux croisés données/programmes, traitements de contrôle des interfaces) ?

3.6. Existe-t-il une documentation utilisateurs par application (incluse dans la recette) comportant notamment le manuel d'utilisation, la description des données saisies et mises à jour, les états de contrôle disponibles, les contrôles automatiques effectués, ...

3.7. En cas d'utilisation de progiciels, vérifier l'existence des programmes sources.
Si l'organisation ne dispose pas des sources, vérifier l'existence contractuelle d'un « *Escrow agreement* ».

3.7. AUDIT DES PROJETS

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires.

3.7.1. OBJECTIFS ET ENJEUX DU PROJET

Un projet est un ensemble de tâches interdépendantes concourant à la réalisation d'un objectif prédéfini et mesurable, avec des spécifications, des contraintes, des moyens humains, financiers et matériels, des délais (un début, une fin) et des risques.
Un projet informatique produit généralement de nouvelles applications et/ou maintien des applications existantes. Il peut aussi s'agir d'un renouvellement matériel majeur.

La conduite de projet est un ensemble de processus permettant de maîtriser la réalisation d'un projet et de la mener à terme.

Cette maîtrise passe par un découpage du projet en processus, étapes, phases, activités et tâches. Il est indispensable d'avoir une définition claire des entrées des processus, des phases et étapes, des productions attendues et des conditions de passage d'une phase à l'autre. Le rôle et les responsabilités des acteurs doivent être clairement définis.

Points de contrôle

1. Objectifs et enjeux du projet

1.1 Une étude de la valeur (ex : MAREVA 2) et des études d'opportunité et d'impacts ont été réalisées.
1.2 Un bilan critique des processus existants a été effectué.
1.3 Le choix de recourir à un nouveau système est obtenu après optimisation des processus concernés et vérification que cette optimisation ne suffit pas à apporter par elle-même les gains de performance attendus.
1.4 Les objectifs et périmètres du projet sont définis, partagés et stabilisés.
1.5 Les principales orientations du système cible ont été explicitées.
1.6 Les principaux acteurs sont identifiés.
1.7 Les coûts sont évalués.
1.8 Les liens et impacts avec des projets connexes et les infrastructures (*Datacenter*, réseaux, etc.) sont pris en compte.

Documents à récupérer

- étude de la valeur et d'opportunité ;
- liste des processus impactés ;
- manuel utilisateur ;
- manuel d'exploitation ;
- dossier d'organisation de la reprise des données ;
- bilan de qualité logiciel ;
- bilan de la satisfaction des utilisateurs.

3.7.2. ÉTUDE D'OPPORTUNITE ET EXPRESSION DES BESOINS

L'étude d'opportunité et l'expression des besoins sont les deux premières phases d'un projet. Elles font émerger les motivations et les raisons de la mise en œuvre du projet. L'étude d'opportunité est généralement suivie d'une étude d'impacts.

Il s'agit d'analyser les dysfonctionnements du système actuel pour, au final, disposer d'une description unique et partagée par tous, de la description de l'ensemble des besoins à satisfaire (évolutions de l'existant ou nouveaux besoins). Les différents scénarios de solution ainsi que des fourchettes de coûts associés doivent être élaborés.

Points de contrôle
2. Étude d'opportunité et expression des besoins
2.1 L'expression détaillée des besoins est formalisée dans un cahier des charges fait par la MOA.
2.2 Le cahier des charges préconise une solution fonctionnellement et techniquement pertinente au regard des besoins exprimés.
2.3 Les exigences utilisateurs, les populations ciblées, les options et principes de gestion retenus sont précisés et priorisés.
2.4 Le projet est cohérent avec le plan directeur informatique.
2.5 Le projet est cohérent avec le SI actuel ou futur.
2.6 La direction est bien impliquée dans le projet.
2.7 Les acteurs de l'équipe projet et leurs responsabilités sont bien identifiés.
2.8 Les compétences du personnel sont en adéquation avec les tâches.
2.9 Une étude d'opportunité est validée.
2.10 Ce document comprend les objectifs du projet.
2.11 Ce document comprend l'analyse des déficiences des systèmes existants.
2.12 Ce document comprend les enjeux et la faisabilité du projet.
2.13 Ce document comprend les bénéfices attendus et la rentabilité économique du projet.
2.14 Ce document comprend les contraintes relatives au projet.
2.15 Ce document comprend la liste des acteurs concernés.
2.16 L'étude d'opportunité a été revue par les directions utilisatrices et par la direction informatique.
2.17 L'approbation de l'étude d'opportunité a été formalisée par écrit par une personne ayant autorité pour le faire.

3.7.3. PLANIFICATION

L'organisation doit être en mesure d'évaluer, d'organiser et de planifier la réalisation des travaux à venir. La mutualisation des ressources, tant au sein de la DSI que pour les entités métiers, est devenue une nécessité.
Il est nécessaire de contrôler si l'organisation est en mesure de planifier de manière cohérente l'utilisation de ses ressources.

Points de contrôle
3. Planification
3.1 Il existe un planning directeur commun à tout le projet.
3.2 Il existe un plan de projet initial.
3.3 Ce plan de projet a été révisé.
3.4 Il existe des plans détaillés.
3.5 Ces plans ont été révisés.
3.6 Les plans intègrent une gestion optimale des ressources.
3.7 Il existe une évaluation des risques liés à la nature du projet.
3.8 Il existe une évaluation des risques liés à la technologie utilisée.
3.9 Il existe une évaluation des risques liés aux projets en cours.
3.10 Il existe une évaluation des risques liés aux délais.
3.11 Il existe une évaluation des risques liés à la synchronisation des activités.
3.12 Les acteurs se sont engagés à respecter le planning général du projet.
3.13 Les lots sont bien identifiés et suivis dans le planning.
3.14 La notion de reste à faire est bien comprise par tous les acteurs.
3.15 Une estimation périodique du reste à faire est effectuée.
3.16 Il existe des "capteurs" d'alerte.
3.17 Il existe des procédures pour traiter les alertes urgentes.
3.18 Un méthode d'estimation des charges est appliquée.
3.19 Cette méthode est cohérente.
3.20 La mise en adéquation des moyens humains est cohérente.
3.21 La mise en adéquation des moyens techniques est cohérente.
Documents à récupérer
• macro planning du projet ; • plan de projet détaillé ; • documents de suivi des risques.

3.7.4. INSTANCES DE PILOTAGE

Différentes instances de pilotage sont mises en place pour accompagner un projet. Le choix des indicateurs et le formalisme du *reporting* jouent un rôle important lors des prises de décision. Les comités de suivi de projet sont généralement au nombre de trois comités :

- **Comité de pilotage** (parfois appelé comité directeur) :
  Instance de décision et de pilotage stratégique du projet (lancement, suivi du développement de la solution, conduite du changement et mise en œuvre, management du projet, arbitrage, allocation de ressources…) ;

- **Comité de projet** (parfois appelé comité de pilotage) :
  Instance de pilotage opérationnel du projet agissant pour le compte du comité de pilotage, comprenant des représentants de la maîtrise d'œuvre (y compris prestataires) ;

- **Comité des utilisateurs** :
  - instance chargée de l'expression détaillée des besoins et des règles de gestion ;
  - de la validation des dossiers de conception présentés par l'équipe projet ;
  - de la participation aux tests du système, à l'élaboration de la documentation « utilisateurs », aux actions de formation ;
  - de la réception définitive du logiciel.

Points de contrôle
4. Les instances de pilotage
4.1 La structure de pilotage est formalisée et connue de tous les acteurs.
4.2 Les différentes instances de pilotage connaissent leurs niveaux de délégation.
4.3 Les objectifs des délégations sont atteints.
4.4 Il existe un comité de pilotage.
4.5 Il existe un comité de projet.
4.6 Il existe un comité des utilisateurs ou, a minima, une participation des utilisateurs.
4.7 Les participants aux différents comités sont représentatifs et ont le bon niveau de décision.
4.8 Les participants ne sont pas trop nombreux.
4.9 Les gestionnaires de la production sont intégrés dans les structures de pilotage.
4.10 La fréquence des comités est appropriée.
4.11 Il existe une réunion périodique de revue du projet pour suivre son avancement.
4.12 La traçabilité des évolutions de périmètre, coût et délai est assurée.
4.13 Il existe des indicateurs de suivi du projet.
4.14 Les indicateurs sont adaptés à l'étape en cours.
4.15 Les indicateurs sont mis à jour.
4.16 Les indicateurs sont pertinents par rapport aux objectifs du projet (contraintes de délais, de qualité, de coût, …).
4.17 Il existe un formalisme de *reporting* (tableau de bord par exemple).
4.18 La fréquence du *reporting* est correcte.
Documents à récupérer
• liste des instances de pilotage ;

- liste des participants avec leurs fonctions ;
- comptes-rendus des derniers COPIL / COPROJ ;
- tableaux de bord ou indicateurs du projet.

3.7.5. METHODES ET OUTILS

L'utilisation d'une méthode précise, connue et partagée impose un découpage du processus de développement en sous-ensembles maîtrisables, identifie les tâches et produits associés ainsi que les points de contrôle et, enfin, fournit un vocabulaire commun pour l'ensemble des parties prenantes.

L'auditeur doit veiller à l'utilisation par l'équipe projet d'un cadre de référence méthodologique. Les principales difficultés rencontrées sont le manque d'homogénéité des livrables, la difficulté d'utilisation de la méthode et l'incompatibilité des outils en place avec la méthode.

Points de contrôle
5. Méthodes et outils
5.1 Il existe une méthode de conduite de projet et celle-ci est appliquée.
5.2 La méthode repose sur un découpage des projets en tâches.
5.3 La méthode repose sur une attribution formelle des responsabilités par tâche.
5.4 La méthode repose sur une identification précise des points de contrôle et des livrables.
5.5 La méthode repose sur un reporting des temps à travers une feuille de temps.
5.6 La méthode repose sur un outil de planification.
5.7 La méthode repose sur des outils.
5.8 Les outils de suivi des délais et des coûts sont adaptés.
5.9 La plan général du projet est suffisamment précis.
5.10 Les tâches identifiées constituent des unités gérables.
5.11 Les membres de l'équipe projet ont été formés à la méthode et aux outils.

Documents à récupérer
• manuel de la méthode appliquée ; • liste des outils utilisés.

3.7.6. PLAN ASSURANCE QUALITE

Le plan assurance qualité (PAQ) est un document décrivant les dispositions spécifiques prises en matière d'assurance de la qualité par un organisme pour répondre aux exigences relatives à un produit et/ou service particulier.

Points de contrôle
6. Qualité
6.1 Il existe un dispositif d'assurance qualité documenté.
6.2 Il existe un manuel d'assurance qualité de l'entité.
6.3 Il existe un plan d'assurance qualité du projet.
6.4 Les objectifs qualité du produit sont formalisés.
6.5 Les objectifs qualité du service attendu sont formalisés.
6.6 Le groupe assurance qualité est indépendant des équipes de développement du projet.
6.7 Une procédure de suivi des revues d'assurance qualité est formalisée.
6.8 Les conclusions des revues d'assurance qualité sont prises en compte par l'équipe projet.
6.9 Il existe un circuit d'approbation des livrables.
6.10 Ce circuit d'approbation est pertinent.
6.11 Il existe un audit de la qualité du projet par une personne extérieure.
Documents à récupérer
• manuel d'assurance qualité ; • plan d'assurance qualité ; • procédure de suivi des revues qualité.

3.7.7. CONCEPTION GENERALE ET ANALYSE

Le dossier de conception générale informatique définit les scénarios d'évolution du système d'information avec :

- une description générale de la solution conceptuelle des flux/traitement et des données ;
- une description générale de la solution organisationnelle ;
- une description générale de l'architecture technique de la solution (centralisé, décentralisé, …) ;
- et une orientation générale des actions de conduite du changement et de mise en œuvre.

Il fournit les éléments nécessaires à la prise de décision en termes d'architecture, de lotissement, de coûts, de risques et de délais.

Points de contrôle
7. Conception générale et analyse
7.1 Il existe une analyse des différents scénarios possibles en termes de solution retenue.
7.2 Tous les scénarios ont été envisagés, même celui de ne rien faire.
7.3 Les contraintes liées aux technologies (besoins en matériels, en formation, en RH, contraintes juridiques, faisabilité opérationnelle, …) ont été prises en compte.
7.4 Une analyse économique (bénéfices attendus, coûts de développement, de formation, de maintenance, …) a été intégrée au choix de la solution.
7.5 Une analyse des risques a été mise en place pour chaque alternative.
7.6 Le choix de la solution a été fait en toute objectivité en se basant sur des critères d'évaluation pertinents.
7.7 Les aspects de contrôle interne et de sécurité ont été pris en compte dans le cahier des charges.
7.8 Les contrôles d'exploitation ont été identifiés.
7.9 La conception générale du futur système s'inscrit dans les objectifs généraux de contrôle en vigueur, dans l'environnement.
7.10 Les besoins spécifiques en matière de contrôles ont été pris en considération.
7.11 Les besoins en matière de contrôles programmés ont été identifiés et décrits.
7.12 Les études de faisabilité ont été revues par les membres du comité adéquat.
7.13 Les différentes solutions possibles ont été présentées au comité adéquat.
7.14 La poursuite du projet a été approuvée par écrit par une personne compétente.

Documents à récupérer
• comparaison des différentes solutions ; • liste des contrôles d'exploitation.

3.7.8. CONCEPTION DETAILLEE

La phase de conception détaillée est ponctuée par un dossier de conception détaillée informatique. Ce dossier spécifie de façon détaillée (architecture et modèles informatiques) les composants logiciels à mettre en œuvre ainsi que les interfaces, selon le scénario, les « modalités » et la « route » de développement retenus.

Points de contrôle
8. Conception détaillée
8.1 Il existe une méthode d'analyse et de conception.
8.2 Cette méthode est correctement utilisée.
8.3 Cette méthode est maîtrisée par l'équipe projet.
8.4 Les spécifications détaillées sont exhaustives par rapport au cahier des charges.
8.5 Il existe des contrôles adaptés à chaque point critique du système (préventifs et correctifs).
8.6 Le responsable de la sécurité est impliqué dans le projet.
8.7 Il existe des pistes d'audit permettant de suivre la totalité des transactions.
8.8 Les acteurs concernés sont impliqués dans le projet (utilisateurs, administrateurs de données, responsable sécurité, …).
8.9 La conception détaillée a été revue par les membres du COPROJ.
8.10 La poursuite du projet a été approuvée par écrit par une personne compétente.

Documents à récupérer
• dossier de spécifications détaillées (ou de conception détaillée) ; • manuel utilisateur ; • manuel d'exploitation ; • dossier d'organisation de la reprise des données ; • bilan de qualité logiciel ; • bilan de la satisfaction des utilisateurs.

3.7.9. DEVELOPPEMENT, REALISATION OU PARAMETRAGE

La phase de réalisation consiste à produire un ensemble de codes exécutables (programmes) structuré et documenté correspondant aux spécifications et respectant les dispositions du plan d'assurance qualité à partir du dossier de spécifications détaillées et des normes et standards de production du logiciel.

Cette phase inclut le développement des interfaces internes et externes, la spécification des tests et l'élaboration des scénarios de reprise des données.

On distingue deux cas de figure lors de la phase de réalisation : soit il existe déjà sur le marché une solution répondant au besoin (progiciel) qu'il faut alors paramétrer, soit il faut développer une solution sur mesure. Paramétrer consiste à adapter un progiciel au contexte organisationnel et technique cible pour répondre aux besoins exprimés par les utilisateurs.

Points de contrôle
9. Développement, réalisation ou paramétrage
9.1 Il existe une méthode de développement.
9.2 Cette méthode est correctement utilisée.
9.3 Cette méthode est parfaitement maîtrisée par les développeurs.
9.4 Il existe des normes de documentation.
9.5 Ces normes sont appliquées par les développeurs.
9.6 Les développements sont bien documentés.
9.7 La documentation est revue par le responsable du service des études.
9.8 Il existe un programme général de tests formalisé.
9.9 Il existe un plan de mise en place.
9.10 Le plan de mise en place définit la nature des travaux à réaliser et leur ordonnancement.
9.11 Le plan de mise en place définit les charges de travail correspondantes et la durée de travaux.
9.12 Le plan de mise en place définit les acteurs concernés.
9.13 Le plan de mise en place définit les rôles et les responsabilités des acteurs.
9.14 Le plan de mise en place est approuvé et diffusé.
9.15 Il existe un plan de migration.
9.16 Les normes de développement et de vérification du programme de conversion sont respectées.
9.17 Les procédures de contrôle en matière de passage en production sont respectées.
9.18 Il existe une image des systèmes et des données avant et après conversion.
9.19 Les résultats du processus de conversion sont approuvés par écrit par les directions concernées.
9.20 Il existe un dossier de spécification de paramétrage.
9.21 Ce dossier consigne les options retenues sur le produit.

Documents à récupérer
• programme général de tests ; • plan de mise en place des tests ; • plan de migration/reprise des données ; • dossier de spécification de paramétrage.

3.7.10. QUALIFICATION : TEST/RECETTE

Toute application informatique doit être testée avant de passer en production, dans un premier temps par la maîtrise d'œuvre, puis par la maîtrise d'ouvrage (test utilisateur).

Une procédure formalisée encadre l'acceptation ou le rejet d'une livraison.

Un procès-verbal doit systématiquement être dressé en fin de recette (période de test).

La qualité de la reprise des données peut être incluse dans cette phase de test.

Points de contrôle
10. Tests et recettes
10.1 La MOE réalise des tests.
10.2 La MOE s'assure que chacun des composants de l'application fonctionne tel qu'il a été décrit dans le dossier de spécifications.
10.3 La MOE réalise des tests sur l'ensemble des composants de l'application sur le plan fonctionnel et technique.
10.4 La MOE réalise des tests sur les interfaces de l'application dans le SI.
10.5 Des tests utilisateurs sont réalisés.
10.6 Les tests portent sur l'adéquation de l'application livrée par la MOE avec les besoins exprimés par la MOA.
10.7 Les tests portent sur l'acceptation technique du système (ergonomie, performance, qualité des entrées/sorties,…).
10.8 Il existe des tests de pré-exploitation.
10.9 Ces tests s'assurent de la bonne intégration de l'application dans l'environnement de production.
10.10 L'application est recettée.
10.11 L'application s'intègre bien dans l'ensemble du SI.
10.12 Il existe une procédure formalisée de recette finale destinée à accepter formellement l'application.
10.13 Tous les acteurs concernés participent activement à la phase de recette.
10.14 Les personnes impliquées dans la recette ont une maîtrise suffisante du système.
10.15 Les jeux d'essais sont pertinents et assurent l'étendue des tests.
10.16 Les résultats des jeux d'essais et de la recette finale sont formalisés par la direction du département utilisateur.
10.17 Il existe un dossier d'organisation de la reprise des données.
10.18 Le niveau de qualité des données d'origine est bien maîtrisé.
10.19 Il existe des contrôles automatiques de la qualité des données obtenues après reprise (exhaustivité et exactitude).
10.20 Les utilisateurs devant participer à la reprise des données ont été mobilisés le plus tôt possible.
10.21 Il existe un bilan de qualité du logiciel.
10.22 Le bilan de qualité prend comme référence les exigences qualité fixées par la MOA et traduites par la MOE en objectifs et critères à respecter.
10.23 Le logiciel est conforme aux besoins fonctionnels exprimés par le cahier des charges.
10.24 Le logiciel est conforme au niveau de performance attendu.
10.25 Le logiciel est conforme au niveau de sécurité attendu.
10.26 Le logiciel est conforme au niveau de convivialité attendu.
10.27 L'appréciation du logiciel est exprimée par les utilisateurs à travers un questionnaire.

Documents à récupérer

- plan de tests ;
- comptes-rendus des tests ;
- plan de recettes ;
- comptes-rendus des recettes ;
- manuel utilisateur ;
- manuel d'exploitation ;
- dossier d'organisation de la reprise des données ;
- bilan de qualité logiciel ;
- bilan de la satisfaction des utilisateurs.

3.7.11. CONDUITE DU CHANGEMENT ET MISE EN ŒUVRE

Enjeu capital dans la réussite ou l'échec d'un projet, le changement vécu par les organisations lors d'une évolution du système d'information doit être maîtrisé et géré comme un processus à part entière.

Il s'agit de l'ensemble de moyens, ressources, méthodes pour transférer la connaissance de l'application de l'équipe projet vers les utilisateurs et les exploitants de l'application.
Ce processus doit aboutir à une réelle appropriation du nouveau système d'information par tous les utilisateurs dès la phase de démarrage. La démarche de conduite du changement/mise en œuvre est habituellement structurée en 6 phases :

- identification et évaluation des changements ;
- plan de communication ;
- plan de formation ;
- élaboration définitive de la documentation ;
- organisation du soutien ;
- dans les cas simples, la reprise des données peut être incluse dans cette phase.

Points de contrôle
11. Conduite du changement et mise en œuvre
11.1 Il existe une synthèse de l'évaluation des changements.
11.2 L'évaluation des changements a été validée.
11.3 Les entretiens réalisés sont représentatifs.
11.4 Les utilisateurs participent à l'évaluation des changements.
11.5 Il existe un plan de communication complet.
11.6 Les messages sont clairs et simples.
11.7 La communication évolue et progresse par rapport au développement du projet.
11.8 La communication est fortement soutenue par la MOA.
11.9 Il existe un plan de formation.
11.10 La hiérarchie des personnes à former est impliquée.
11.11 Les profils types des personnes à former sont identifiés.
11.12 La population à former est pertinente.
11.13 Les objectifs de chaque formation sont identifiés et affichés.
11.14 Les sessions de formations sont évaluées et repensées selon l'évaluation.
11.15 Le planning de formation est cohérent avec le planning du projet.
11.16 La durée du programme de formation est pertinente.
11.17 Les formateurs et le contenu de la formation sont de qualité.
11.18 Il existe une procédure d'évaluation des formés et des formateurs.
11.19 Une organisation de soutien aux utilisateurs a été mise en place dans la phase d'exploitation du nouveau système.
11.20 Son organisation générale est bien anticipée.
11.21 Les différents niveaux de soutien sont coordonnés et cohérents.
11.22 Il existe un dossier d'organisation de la reprise des données.
11.23 Le niveau de qualité des données d'origine est bien maîtrisé.
11.24 Il existe des contrôles automatiques de la qualité des données

obtenues après reprise (exhaustivité et exactitude).

11.25 Les utilisateurs devant participer à la reprise des données ont été mobilisés le plus tôt possible.

Documents à récupérer

- plan de communication ;
- plan de formation ;
- planning de formation avec liste des formés ;
- comptes-rendus des évaluations des formés et des formateurs.

3.7.12. DOCUMENTATION

Pour que l'application soit pérenne et puisse évoluer, il est important de produire de la documentation. Ces documents contribuent à la transmission du savoir pour maintenir, faire évoluer et utiliser l'application.

Points de contrôle
12. Documentation
12.1 Il existe un manuel d'utilisation.
12.2 Le manuel utilisateur est conforme aux normes en vigueur.
12.3 Le manuel utilisateur est disponible et compréhensible par l'ensemble des utilisateurs.
12.4 Le manuel utilisateur comprend les objets du système et la description des dessins d'écran et des commandes disponibles.
12.5 Le manuel utilisateur comprend les responsables concernant le redressement des erreurs ou anomalies.
12.6 Le manuel utilisateur comprend la description des sorties et leur mode de diffusion.
12.7 Le manuel utilisateur comprend les responsabilités en matière de sauvegarde/archivage/purge.
12.8 La manuel utilisateur fait l'objet d'une procédure de mise à jour.
12.9 Il existe un manuel d'exploitation.
12.10 Le manuel d'exploitation est accessible et compréhensible pour les opérateurs.
12.11 Le manuel d'exploitation a été testé lors des tests finaux.
12.12 Le manuel d'exploitation comprend la fonction des programmes.
12.13 Le manuel d'exploitation comprend le libellé exact des fichiers concernés.
12.14 Le manuel d'exploitation comprend la liste des messages opérateurs et les réponses attendues.
12.15 Le manuel d'exploitation comprend les actions à suivre en cas d'anomalies.
12.16 Le manuel d'exploitation comprend la liste des états générés et leurs destinations.
12.17 Le manuel d'exploitation comprend les procédures de reprise.
12.18 Le manuel d'exploitation comprend les responsabilités de l'exploitation en matière de contrôles généraux.
12.19 Le manuel d'exploitation fait l'objet d'une procédure de mise à jour.

Documents à récupérer
• liste des indicateurs ; • tableau de bord ; • manuel utilisateur ; • manuel d'exploitation ; • dossier d'organisation de la reprise des données ; • bilan de qualité logiciel ; • bilan de la satisfaction des utilisateurs.

3.7.13. ROLES ET RESPONSABILITES

Il est important de définir les rôles et les responsabilités de l'ensemble des parties prenantes lors de la conduite d'un projet, et ce, pour l'ensemble des phases de son existence (de l'étude d'opportunité au retrait de service).

Points de contrôle
13. Structures mises en place à l'occasion du projet
13.1 Les rôles et les responsabilités respectifs de la MOA et de la MOE sont clairement définis.
13.2 Les prérogatives du chef de projet sont clairement définies.
13.3 Le chef de projet dispose de l'autorité suffisante pour résoudre les éventuels conflits.
13.4 La MOA et la MOE disposent des compétences et des ressources managériales, techniques et fonctionnelles suffisantes.
13.5 Les principales décisions et orientations du projet sont prises par le niveau de management adéquat.
13.6 Les principaux intervenants sur le projet sont 100% dédiés au projet avec suppression, pendant la durée du projet, des anciens liens hiérarchiques.
13.7 La MOA ou la MOE ont bénéficié d'une assistance extérieure au cours du projet.
13.8 La consultation et l'implication des utilisateurs a été suffisante au cours des différentes phases du projet.
13.9 Il existe un contrat de prestation entre la MOA et la MOE.
13.10 Si oui, il existe un engagement de résultat.
Documents à récupérer
• organigramme du projet avec définition des fonctions ; • contrats d'assistance, de sous-traitance, d'infogérance, …

3.7.14. GESTION DES EVOLUTIONS

Le terme « évolution » désigne les modifications apportées à un système après sa mise en service. La gestion des évolutions doit faire l'objet d'une organisation et de procédures clairement définies.

Points de contrôle
14. Gestion des évolutions
14.1 Les demandes d'évolution du périmètre sont fréquentes.
14.2 Les demandes d'évolutions sont formalisées.
14.3 Il existe une procédure de gestion des évolutions du périmètre.
14.4 Une mesure d'impact est effectuée.
14.5 Il existe une gestion des versions.
14.6 Les décisions sont prises avec un délai satisfaisant.
14.7 Les décisions sont prises sur la base d'un niveau d'information pertinent.
14.8 Le manuel utilisateur fait l'objet d'une procédure de mise à jour.
14.9 Le manuel d'exploitation fait l'objet d'une procédure de mise à jour.
14.10 L'organisation de soutien aux utilisateurs est informée des évolutions et les a anticipées.
14.11 Les différents niveaux de soutien restent coordonnés et cohérents.
14.12 Il existe un bilan de qualité de l'évolution.
14.13 Le bilan de qualité prend comme référence les exigences qualité fixées par la MOA et traduites par la MOE en objectifs et critères à respecter.
14.14 L'évolution est conforme aux besoins fonctionnels exprimés par le cahier des charges.
14.15 L'évolution est conforme au niveau de performance attendu.
14.16 L'évolution est conforme au niveau de sécurité attendu.
14.17 L'évolution est conforme au niveau de convivialité attendu.
14.18 L'appréciation de l'évolution est exprimée par les utilisateurs à travers un questionnaire.

Documents à récupérer
• procédure de demande d'évolution du périmètre ; • liste des demandes d'évolution ; • manuel utilisateur ; • manuel d'exploitation ; • bilan de qualité logiciel ; • bilan de la satisfaction des utilisateurs.

3.7.15. MISE EN PRODUCTION

La phase de mise en production est celle de la mise à disposition des utilisateurs. Elle doit se faire de manière ordonnée, en respectant strictement les procédures internes lors de la bascule de responsabilité entre la direction chargée des projets et la direction chargée de la production.

Cette étape soulève souvent des problèmes que les environnements de tests n'ont pas pu simuler. Il est donc primordial d'assurer la reprise d'activité le plus rapidement possible après la mise en production de l'application, pour ne pas gaspiller la période de garantie.

Points de contrôle
15. Mise en production
15.1 Les responsabilités respectives des directions des projets et de la production sont clairement établies et les périmètres décrits respectent les principes de séparation des tâches.
15.2 Il existe un document décrivant les responsabilités respectives des projets et de la production lors d'une mise en production.
15.3 Les équipes projet et de production connaissent et respectent ce document.
15.4 Les opérations de mise en production sont tracées et conformes.
15.5 Les obligations respectives de l'organisation et de ses fournisseurs lors de la mise en production sont clairement indiquées dans les documents contractuels.
15.6 Les membres de l'organisation et les fournisseurs respectent leurs obligations lors de la mise en production.
15.7 La bascule de la garantie vers la maintenance est organisée à travers des documents contractuels clairs.
Documents à récupérer
• dossier d'organisation de la direction informatique ; • procédure de mise en production.

3.8. AUDIT DES MARCHES SPECIFIQUES AU DOMAINE INFORMATIQUE

Ce paragraphe est consacré aux marchés spécifiques au domaine informatique. Il a vocation à compléter le guide des bonnes pratiques des achats de services informatiques du service des achats de l'État (SAE), qui reste la référence.

Les risques propres à ces marchés sont notamment :

- l'imprécision des responsabilités des acteurs étatiques et privés, en raison de l'utilisation dans les marchés des notions de MOA, MOE, AMOA, etc. sans accord explicites des parties sur la portée de ces notions ;
- la complexité opérationnelle et juridique des prestations, notamment pour les fonctions partiellement externalisées ;
- la nature des prestations, qui peuvent aisément dériver vers un positionnement illicite des agents du prestataire vis-à-vis de l'administration ;
- l'insuffisante définition des livrables et l'imprécision – voire l'inexistence – des critères d'évaluation permettant d'attester objectivement la réalité du service fait.

3.8.1. ÉTUDE DES MARCHES D'ASSISTANCE TECHNIQUE

L'assistance technique (qui se retrouve fréquemment en conduite de projets sous la forme d'AMOA) est un besoin pour les services du ministère qui ne disposent pas de toutes les compétences pour mener à bien toutes les missions qui leur sont confiées. Néanmoins, les marchés passés dans ces domaines présentent différents risques :

- risque de perte de compétence pour les services ;
- risque de coût prohibitif pour les finances publiques ;
- risque pénal car ces marchés, s'ils sont mal rédigés, mal passés ou mal exécutés, courent le risque d'être requalifiés, par le juge, en prêt illégal de main d'œuvre ou en délit de marchandage.

Points de contrôle
1. Marchés d'AMOA
1.1 Les responsabilités respectives de l'administration et du titulaire sont clairement établies et le marché ou un document qui lui est annexé les précise.
1.2 Les équipes du titulaire et les représentants de l'administration connaissent et respectent ce document.
1.3 L'objet du marché est régulier : • la prestation, objet du marché, n'est pas irrégulière par nature (liquidation de factures, rédaction de marchés, …) ; • le marché n'a pas pour seul objet le prêt de main d'œuvre (ex : prix calculé selon un montant exprimé en hommes/jour).
1.4 Les obligations des parties sont conformes au droit : • les pièces du marché (CCTP, acte d'engagement) font apparaître des obligations de résultats du titulaire et non des obligations de moyens (ex : pas de jalons, pas ou peu de livrables, aucun résultat réellement exigé).
1.5 Les documents du marché ne montrent pas que le service a voulu s'attacher une personne précise (CV, nom de l'intervenant cité, …).
1.6 L'exécution du marché ne fait pas apparaître une rupture du lien hiérarchique entre l'employé et sa hiérarchie : • les agents du titulaire ne sont pas intégrés dans les équipes de l'administration ; • les agents du titulaire ne reçoivent pas leurs ordres de la hiérarchie du service prescripteur.
1.7 L'exécution du marché ne fait pas apparaître une intégration des agents du titulaire au sein de l'administration : • les agents du titulaire n'apparaissent pas nominativement dans les documents de l'administration (organigrammes, annuaires, PV de réunions, …) ; • les agents du titulaire n'utilisent pas abusivement les moyens de l'administration (accès au restaurant de l'administration au tarif "usager", utilisation d'une adresse de messagerie de l'administration, accès aux réseaux de l'administration, …) ; • les agents du titulaire ne sont pas répartis dans les locaux des services de l'administration sans séparation manifeste et identification précise (absence de badges et de locaux particuliers) ; • les agents du prestataire ne sont pas en poste depuis plus de 3

ans (durée indicative).

3.8.2. ÉTUDE DES MARCHES D'ACQUISITION DE PRESTATIONS INFORMATIQUES SUR LA BASE D'UN FORFAIT

Le marché peut avoir pour objet la prestation de services dont le prix est fixé forfaitairement, à la date de conclusion du contrat. Même dans le cadre d'un forfait, le contrat peut détailler les sommes allouées au titre des redevances de licences, de maintenance, ou du prix de la formation éventuelle, des développements spécifiques…

Si le client a l'avantage de bénéficier d'un prix forfaitaire, il faut tenir compte d'un certain nombre de risques. Par exemple, le calendrier peut dériver, la charge de travail du prestataire peut être sous-évaluée, ou le référentiel trop imprécis peut enfermer l'administration dans un périmètre excessivement restreint.

Points de contrôle
2. Marchés de prestation sur la base d'un forfait
2.1 S'agissant des licences, le marché prévoit les droits concédés par l'éditeur et les conditions d'accès au code source en cas de résiliation.
2.2 Le contrat précise quels documents constituent le référentiel des spécifications afin de déterminer le champ des prestations entrant dans le montant du marché fixé forfaitairement.
2.3 Le marché distingue le traitement des évolutions qui pourront entraîner une facturation complémentaire, dans des conditions prévues entre les parties, et celles, simples précisions ou adaptations, qui resteront incluses dans le prix établi forfaitairement.
2.4 Un mécanisme de pénalités de retard sanctionne le non-respect du calendrier (y compris les jalons intermédiaires), ou un bonus est prévu si le prestataire atteint ses objectifs dans des délais plus courts que prévu.
2.5 Les jalons intermédiaires ne sont pas artificiels.
2.6 Le marché précise bien quels sont les prérequis (disponibilité du personnel du client, configuration matérielle, …).

3.8.3. ÉTUDE DES MARCHES D'ACQUISITION DE PRESTATIONS INFORMATIQUES SUR LA BASE D'UN FORFAIT HORAIRE

Le marché peut avoir pour objet la prestation de services à caractère informatique dont la rémunération est calculée sur la base d'un forfait horaire ou journalier. Cette formule présente l'avantage de la souplesse et de la simplicité mais elle est risquée, notamment sur le plan juridique (sanctions pénales et requalification du contrat).

L'administration peut, en effet, perdre le contrôle du coût final de l'opération : la rémunération au temps passé fait supporter par le seul client le risque économique de l'opération.

Le marché peut être requalifié en prêt illicite de main-d'œuvre (article L.125-3 du Code du travail) ou marchandage (article L.125-1 du Code du travail). Sont alors pénalement responsables autant l'auteur du prêt illicite de main-d'œuvre (la SSII) que son bénéficiaire (l'administration). De plus, la relation entre l'employé de la SSII et le client peut être requalifiée en contrat de travail (avec les conséquences fiscales et sociales très lourdes induites).

Bien que n'étant pas a priori irrégulier, ce mode de contractualisation est très déconseillé et doit chaque fois que possible être remplacé par un marché à forfait.

Points de contrôle
3. Marchés de prestation sur la base d'un forfait horaire
3.1 La nature de la mission confiée au prestataire est matérialisée et définie précisément. Le recours à des personnes extérieures (expertise particulière par exemple) est justifié.
3.2 Le marché attribue explicitement la responsabilité de l'exécution des travaux incombant au prestataire et précise que le lien de subordination du personnel n'est en rien transféré à l'administration. Les relations sont formalisées dans les pièces constitutives du marché.
3.3 La durée du marché est clairement limitée à la mission décrite dans l'objet du contrat, ou un terme précisément fixé dans le temps est prévu.
3.4 Les clauses du marché prévoient (et l'exécution montre) que lorsque le personnel de la SSII intervient dans les locaux de l'administration, il doit respecter les règles d'hygiène et de sécurité ainsi que les règles générales et permanentes relatives à la discipline, issues du règlement intérieur du client (il n'est toutefois pas soumis aux mêmes contraintes horaires et de congés).
3.5. Le prestataire est, dans la mesure du possible, isolé dans un local qui lui est confié pendant la durée de la prestation (rédaction d'un protocole). Cette disposition peut être contraire à l'objet même du marché, notamment dans le cas d'une plateforme commune au cœur de la méthode AGILE. Dans ce cas, l'attention doit être portée sur la stricte limitation des ressources accessibles aux agents du prestataire.

3.8.4. ÉTUDE DES MARCHES D'INFOGERANCE OU DE TIERCE MAINTENANCE APPLICATIVE (TMA)

La norme AFNOR Z67 801-1 définit l'infogérance comme étant un service défini comme le résultat de l'intégration d'un ensemble de ressources élémentaires, visant à confier à un prestataire informatique tout ou partie du système d'information du client dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de service et une durée définis.

Une TMA consiste, comme pour le SaaS, en l'externalisation d'une infrastructure et/ou d'une application. Il ne s'agit pas de l'externalisation d'un processus (BPO, pour *Business Process Outsourcing*, en anglais). Ainsi, dans une TMA, l'utilisateur étatique demeure responsable de l'utilisation qui est faite des matériels et logiciels externalisés, et du résultat de leur emploi.

Aux intérêts stratégiques (optimiser la gestion de son système d'information, réduire les coûts, gagner du temps) répond le risque de dépendance vis-à-vis du prestataire.

Points de contrôle
4. Marchés d'infogérance ou de TMA
4.1 Le marché notifié précise convenablement l'opération projetée et sa délimitation. Un audit technique et juridique des caractéristiques des applications de l'entreprise cliente pourra avoir été réalisé en phase préalable.
4.2 Le marché inclut un engagement du prestataire sur des performances et une qualité du service. Une clause du CCAP fixe les indicateurs de qualité, par exemple par une référence à un PAQ (qui peut être le premier livrable du marché) ou à l'offre du fournisseur, avec des pénalités associées en cas de non-respect.
4.3 Le marché prévoit l'obligation pour le prestataire, quelle que soit la cause du terme du contrat, de prendre toutes les dispositions utiles ou d'apporter à son client son concours pour assurer la réversibilité de la mise en infogérance de son système informatique (soit parce qu'il souhaite l'exploiter lui-même, soit parce qu'il souhaite en confier l'exploitation à un tiers de son choix). Le contrat précise les conditions d'application et les modalités pratiques de cette réversibilité.
4.4 Les dispositions du marché organisant la réversibilité sont mises en œuvre de manière démontrable, à la fois par le prestataire et par les services de l'administration qui en sont bénéficiaires.
4.5 La TMA ne camoufle pas du développement.

3.8.5. ÉTUDE DES MARCHES AYANT POUR OBJET LA FOURNITURE D'UNE APPLICATION HEBERGEE

Le principe d'un FAH (fournisseur d'application hébergée, ou en anglais ASP pour *Application Service Provider*), consiste à proposer à un client d'accéder aux fonctionnalités de son choix et/ou à des services associés.

Un contrat de fourniture d'application hébergée peut être scindé en deux parties, un volet forfaitaire correspondant à un droit d'entrée ou d'accès, et une autre partie proportionnelle à l'utilisation.

À l'optimisation du prix (notamment sélection des seules fonctionnalités nécessaires) et l'évolutivité associée des fonctionnalités choisies, s'ajoute pour le client l'avantage de disposer d'un interlocuteur unique.

Il faut, cependant, veiller à bien cerner les besoins et le prix à payer et, comme pour tout contrat informatique, à bien définir les niveaux de service attendus.

Points de contrôle
5. Marchés FAH
5.1 Le marché prévoit l'obligation, pour le prestataire, d'assurer la sécurité des données traitées, et ce d'autant plus si celles-ci sont sensibles (données comptables, fiscales, sociales ou de paie notamment). Cette obligation de sécurité concerne tant le traitement de données que leur conservation, voire leur archivage.
5.2 S'agissant des licences, le marché prévoit les droits concédés par l'éditeur et les conditions d'accès au code source en cas de résiliation. Il prévoit également la possibilité de transférer le savoir-faire du prestataire relatif à un produit, qui est également une condition de la réversibilité.
5.3 Le contrat prévoit l'étendue des prestations fournies par le prestataire (les conditions d'accès aux services, les niveaux du service et les causes d'exclusion du service).
5.4 Le contrat précise les niveaux de service attendus par le client tant en termes de performances qu'en termes de disponibilité des applications.

4. DICTIONNAIRE DES EXPRESSIONS SPECIFIQUES ET ACRONYMES

4.1. DICTIONNAIRE DES EXPRESSIONS SPECIFIQUES DU DOMAINE

Ces définitions rapides doivent permettre aux auditeurs de vérifier qu'ils partagent avec les audités une même compréhension de certaines notions spécifiques et complexes. Cette vérification est particulièrement nécessaire lorsqu'une tierce partie – un prestataire – est impliquée, par exemple lors de l'examen des conditions de réalisation d'un marché.

4.1.1. GOUVERNANCE DU SI

La « Gouvernance des Systèmes d'Information » ou « Gouvernance informatique » désigne le dispositif mis en place par une organisation pour contrôler et réguler son SI. À ce titre, la gouvernance du SI fait partie intégrante de la gouvernance de l'organisation et consiste d'abord à fixer au SI des objectifs découlant de la stratégie de l'organisation.

Les référentiels et fournissent des éléments permettant de mettre un système d'information sous contrôle et de le faire évoluer en fonction de la stratégie de l'organisation

4.1.2. SCHEMA DIRECTEUR ET PLAN STRATEGIQUE INFORMATIQUE

Le schéma directeur est un plan stratégique destiné à piloter le développement de l'informatique dans l'organisation, en cohérence avec sa stratégie générale.

Un schéma directeur informatique décrit le système informatique actuel et futur, dans une logique d'objectifs et de services attendus. Il offre donc une vue globale de l'état présent du système, un inventaire et une spécification des besoins et définit des orientations.

Il est approuvé par le plus haut niveau de l'organisation. Il doit faire l'objet d'arbitrages clairs portant sur les finalités visées, les adaptations de processus opérationnels, les ressources humaines et financières affectées et les étapes et le calendrier de réalisation.

Sa durée de vie est généralement comprise entre deux et six ans.

4.1.3. PLAN D'OCCUPATION DES SOLS (POS)

La multiplication des applications présentant des recoupements fonctionnels a conduit à la notion d'urbanisation du système d'information.
Il s'agit, par analogie avec les outils du développement urbain, de fixer des règles régissant le développement applicatif pour améliorer la couverture fonctionnelle de certaines activités de l'organisation, éviter la duplication des outils informatiques, fournir une vision prospective de l'évolution du patrimoine applicatif, etc.

Le patrimoine applicatif est ainsi réparti sur un plan d'occupation des sols, en zones, quartiers, ilots et blocs fonctionnels. Les applications actuelles et futures sont censées être réparties entre chacune des subdivisions. En

pratique, ce découpage n'est pas toujours aisé, ce qui peut amener à la création de zones fonctionnelles dites transverses et à l'affectation d'une application à la zone correspondant à sa fonction principale, voire « historique », au détriment parfois d'une vision d'ensemble des services qu'elle rend.
Cette démarche d'urbanisation encourage le développement d'un SI constitué de modules fonctionnels à l'échelle de l'organisation. Il faut alors porter une attention particulière au socle technique commun (la pile logicielle) et à la gestion des nombreuses interfaces et des données de références.

Chaque subdivision du plan d'occupation des sols doit posséder un responsable effectif chargé de son pilotage, de son interaction avec les autres zones (échange de données, interfaces applicatifs, etc.) et de l'entretien d'une vision prospective, généralement sous la forme d'un schéma directeur. Faire vivre l'urbanisme du SI est un défi pour toute organisation, quelle que soit sa taille.

4.1.4. MAITRISE D'OUVRAGE (MOA) ET MAITRISE D'ŒUVRE

La maîtrise d'ouvrage est le commanditaire du projet informatique. Il s'agit soit d'une direction métier, à l'origine du besoin fonctionnel et sponsor du projet, soit (par exemple au ministère de la défense) d'une direction générale spécialisée dans le co-pilotage (avec les directions fonctionnelles) et la conduite des projets.

La MOA :

- constitue une équipe projet adaptée et disposant des moyens financiers, humains et techniques nécessaires ;
- spécifie les besoins fonctionnels et établit le cahier des charges ;
- définit les moyens et les contraintes (délais, coûts, qualité, ...) ;
- définit et fait vivre le portefeuille des risques du projet ;
- sélectionne la MOE et rédige ; notifie et pilote les marchés correspondants ;
- pilote la MOE par une comitologie adaptée aux enjeux et méthodes retenues (ex : AGILE) ;
- valide les solutions proposées par la MOE et suit leur réalisation ;
- réceptionne l'application conformément aux besoins exprimés ;
- administre l'application jusqu'à son retrait.

L'assistance à maîtrise d'ouvrage (AMOA) soulage le travail de la MOA en la déchargeant des tâches de pilotage de nature technique (assistance à la spécification, assistance à la sélection de la MOE et à la contractualisation de la prestation, secrétariat de la comitologie, etc.). Les principaux défauts observés sont :

- AMOA remplaçant dans les faits la MOA, ce qui conduit rapidement à un défaut de maîtrise du projet par le commanditaire, avec toutes les dérives associées ;
- AMOA palliant les lacunes de l'équipe projet au lieu de l'assister ;
- AMOA mal sélectionnée et manquant d'indépendance vis-à-vis de la MOE, ce qui peut, par exemple, avoir un impact sur le contenu de la spécification et la conduite de l'appel d'offres ;
- AMOA ne pouvant être remise en concurrence en raison de son emprise sur le projet.

La partie « études » de la direction informatique joue fréquemment le rôle de MOA déléguée. Ce schéma, qui permet de faire piloter l'AMOA ou la MOE par des spécialistes des projets informatiques, n'exonère pas la direction métier de ses responsabilités de MOA.
La maîtrise d'œuvre est le garant technique du bon déroulement d'un projet.

La MOE :

- propose des solutions techniques sur la base des besoins, moyens et contraintes définis par la MOA ;
- assure ou supervise le développement de l'application ;
- contrôle et teste le résultat (tests unitaires et tests d'intégration) ;
- livre l'application pour la recette puis, le cas échéant, l'exploite.

4.1.5. PROPRIETAIRE (*BUSINESS OWNER*) D'UNE APPLICATION OU DE DONNEES

Un propriétaire d'application est chargé de veiller à la bonne adaptation d'une application ou d'un portefeuille d'applications aux besoins du métier (notion d'alignement stratégique) et à son environnement logiciel et matériel.
Il est, à ce titre, l'interlocuteur du responsable des processus et métiers utilisant l'application, de l'urbaniste du système informatique, du gestionnaire des budgets informatiques (maintenance, évolution et nouveaux projets), du responsable de la sécurité informatique et du responsable des plans de continuité et de reprise de l'activité de l'organisation.

Il est responsable vis-à-vis d'eux de la correcte prise en compte de l'ensemble de ces problématiques. Il veille à ce que les utilisateurs bénéficient d'une formation et d'un soutien adéquats.
Cette fonction ne doit pas être confondue avec celle de responsable d'application(s), qui désigne généralement celui qui, au sein de la DSI, est chargé de la gestion du portefeuille applicatif de l'organisation.

Un propriétaire de données est responsable vis-à-vis de la direction, des processus opérationnels et des utilisateurs de la qualité, de l'intégrité, de la sécurité et de la disponibilité d'un ensemble de données. Notamment, il attribue et surveille les droits de création, de modification, de lecture et de suppression des données. Il est également responsable, autant que possible, de l'unicité des donnés, c'est-à-dire de leur non réplication, notamment locale, par les utilisateurs. Cette fonction de propriétaire de données est d'autant plus importante que les données sont sensibles et transverses.

Un propriétaire d'application ou de données est un responsable opérationnel.

Au sein d'une organisation, chaque application et chaque donnée devrait avoir un propriétaire désigné, y compris pour les applications et processus externalisés.

4.1.6. BASE DE DONNEES MAITRESSE

Lorsque des données sont partagées entre plusieurs acteurs (directions fonctionnelles, applications informatiques, etc.) au sein d'une organisation, il faut mettre en place un dispositif visant à garantir l'existence, pour chacune de ces données, d'une référence incontestable.

La base de données maîtresse est cette référence. Elle peut être dupliquée en des bases de données réparties, créées pour répondre à un

besoin de proximité géographique ou fonctionnelle. Par exemple, les coordonnées clients ou la liste des agents identifiés dans le SI sont des informations sensibles utilisées par de nombreuses applications : leur exactitude, leur mise à jour et surtout leur unicité doivent être garanties.

L'une des tâches importantes d'un propriétaire de données est de veiller à la qualité des processus de réplication entre les bases de données maîtresse et réparties.

4.1.7. POLITIQUE DE SECURITE

Elle couvre l'ensemble des orientations suivies par une entité en matière de sécurité. À la lumière des résultats de l'analyse de risques, elle :

- définit le cadre d'utilisation des ressources du SI ;
- précise les rôles et responsabilités en la matière ;
- identifie les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation ;
- sensibilise les utilisateurs à la sécurité informatique.

La sécurité informatique résulte d'un compromis entre la protection des actifs numériques et informatiques et la possibilité pour les utilisateurs de développer les usages légitimes qui leur sont nécessaires. À ce titre, la politique de sécurité informatique relève de la responsabilité de la direction de l'organisation concernée.

4.1.8. CHARTE D'UTILISATION

Une charte d'utilisation est un document validé par la direction générale de l'organisation, déclinant aux utilisateurs la politique de sécurité du SI. Elle est obligatoirement signée par tous les utilisateurs des ressources informatiques.

Elle peut être établie sur le modèle suivant :

- les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition. Par exemple :
    - le poste de travail ;
    - les équipements nomades ;
    - l'espace de stockage individuel ;
    - le réseau local ;
    - internet ;
    - la messagerie électronique ;
    - le téléphone.
- les règles de sécurité auxquelles se conformer, ce qui peut inclure par exemple :
    - les moyens d'authentification ;
    - les modalités d'intervention du service de l'informatique interne ;

- signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;

- de ne jamais confier son identifiant/mot de passe à un tiers ;

- de ne pas modifier les paramétrages du poste de travail ;

- de ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;

- de verrouiller son ordinateur dès que l'on quitte son poste de travail ;

- de ne pas accéder, tenter d'accéder, ou supprimer des informations qui ne relèvent pas des tâches incombant à l'utilisateur ;

- les modalités de copie de données sur un support externe.

- les conditions d'administration du SI et l'existence, le cas échéant, de systèmes automatiques de filtrage ou de traçabilité ;

- les responsabilités et sanctions encourues en cas de non-respect de la charte.

4.1.9. ENVIRONNEMENTS DE DEVELOPPEMENT (ETUDES), D'INTEGRATION ET DE PRODUCTION (EXPLOITATION)

La ségrégation des environnements et des fonctions de développement et de production informatique est un élément essentiel de la sécurité informatique et de la lutte anti-fraude. Elle joue en matière informatique un rôle équivalent à la séparation entre ordonnateurs et comptables en matière de dépense publique, et revêt la même sensibilité.

Toute modification des applications informatiques, depuis les grands projets applicatifs jusqu'à la mise à jour d'une composante du système d'exploitation, doit respecter cette ségrégation. Elle est développée sur un environnement SI spécifique (qui peut être celui d'un prestataire), sur lequel elle est testée une première fois.

Elle est ensuite qualifiée par les équipes de la production, dans un environnement distinct de l'environnement de production (l'environnement accessible aux utilisateurs, sur lequel sont réalisées les activités réelles de l'organisation) mais aussi représentatif que possible de ce dernier.
Cette qualification inclut les tests de bon fonctionnement, mais aussi la revue du code (ou, à défaut, des spécifications détaillées) et de la documentation.
Cette acceptation par la production est un prérequis indispensable au transfert de la modification sur l'environnement de production.

Les interventions directe des études sur l'environnement de production doivent être limitées au strict minimum et parfaitement tracées et encadrées.

4.1.10. RECETTE

En informatique, la recette (ou test d'acceptation) est une phase du projet visant à assurer formellement que le produit est conforme aux spécifications.
Elle s'inscrit dans les activités plus générales de qualification. Cette étape implique le déroulement rigoureux de procédures de tests préalablement décrits, et l'identification de tout écart fonctionnel ou technique. Dans ses phases de tests fonctionnels, elle nécessite une forte disponibilité des utilisateurs (directions métiers).

Ce terme renvoie à des notions différentes dans les marchés : vérification de bon fonctionnement, vérification de fonctionnement régulier, service fait. Dans le cas d'un marché informatique, les parties doivent s'accorder sur la portée de ces expressions, ce qui peut nécessiter leur explicitation.

4.1.11. CONVENTION ET CONTRATS DE SERVICE (SLA / OLA)

Le contrat de service, appelé aussi convention de service, souvent désigné par l'acronyme anglais « SLA (pour *service level agreement*) », est un document qui définit la requise entre un prestataire d'un service informatique et les usagers de ce service, ou « clients ».

Un SLA est la formalisation d'un accord négocié entre deux parties. Il met donc par écrit un niveau de service, exprimé par l'attente des parties sur le contenu des prestations, leurs modalités d'exécution, les responsabilités des parties, et des garanties, notamment en termes de continuité ou de rétablissement de service.

Par exemple, le SLA peut spécifier les niveaux de disponibilité ou de performance d'un service informatique (matériel, y compris réseau, logiciel, soutien utilisateurs, délais d'intervention, etc.).
Tout engagement quantitatif doit être mesurable, effectivement mesuré, et faire l'objet d'un dialogue de gestion.

4.1.12. PLAN DE CONTINUITE DE L'ACTIVITE ET PLAN DE REPRISE DE L'ACTIVITE

Ces deux notions sont distinctes.

- Un Plan de Reprise d'Activités (PRA) est un ensemble de mesures qui permettraient à une organisation de reprendre son activité après un sinistre, par exemple une panne qui paralyserait son SI au-delà du supportable.

- Un Plan de Continuité d'Activité (PCA) est un ensemble de mesures qui permettraient à une organisation de poursuivre son activité pendant un sinistre. La différence est notable car, dans ce dernier cas, l'activité ne cesse pas. L'organisation est donc contrainte, pour la totalité ou pour une partie de son activité, de faire travailler différemment de son fonctionnement habituel.

Les PRA et PCA vont très au-delà de la seule informatique. Ils sont donc un dispositif clé de l'organisation, qui conditionne sa capacité à agir en situation de crise interne ou externe, et doivent, à ce titre, faire partie de sa stratégie de sécurité. Ils doivent toujours être en conditions opérationnelles, ce qui implique de mettre en place une politique de tests réguliers.

En raison de la forte dépendance des organisations vis-à-vis de leur SI, les PCA et PRA doivent évoluer de pair avec le SI. Ils peuvent ou non se décliner dans une notion connexe, limitée à l'informatique : les plans de reprise informatique (PCI) ou de continuité informatique (PRI).

4.1.13. INFOGERANCE ET OUTSOURCING

L'infogérance consiste à déléguer à un ou plusieurs prestataire(s) informatique(s) tout ou partie de la gestion de son système d'information. Les prestations correspondantes et le niveau de service attendu sont formalisés dans un cadre contractuel ou par un marché.

Cela peut concerner des éléments d'infrastructure (mise en place et exploitation de serveurs ou de systèmes de sauvegarde, supervision de services réseau ou de téléphonie…) et/ou des aspects logiciels (développement, maintenance…).

En infogérance dite « totale », l'organisation confie l'intégralité de la gestion de son SI à une entreprise tierce, de la conception à la maintenance, en passant par l'exploitation.
La sensibilité stratégique du SI et des actifs numériques, la qualité de la prestation et sa réversibilité sont des éléments de décision essentiels.
Les mécanismes d'infogérance et d'outsourcing connaissent un fort regain d'actualité lié à l'émergence du concept de *cloud computing*.

4.1.14. INFORMATIQUE EN NUAGE, OU CLOUD COMPUTING

L'informatique en nuage est une technologie qui consiste à s'appuyer sur les capacités des réseaux pour mettre à la disposition des utilisateurs finaux un service, fourni par des logiciels et une infrastructure informatique souvent distants.

Le plus souvent, ces utilisateurs n'ont pas connaissance de la localisation précise des matériels, logiciels et données auxquels ils accèdent par l'intermédiaire d'un réseau public ou privé. Le service peut être lui-même fourni par une entité publique, voire étatique (on parle alors parfois de « cloud souverain ») ou par un opérateur privé.

L'informatique en nuage permet de concentrer des matériels techniques et des logiciels dans des installations (« *datacenters* ») de plus grandes dimensions en nombre limité, ce qui évite de multiplier les installations locales, de petites dimensions et de standards matériels ou logiciels disparates. Cela permet la concentration des ressources humaines compétentes, une économie d'échelle, facilite la maintenance et améliore les sécurités physique et logique.

Il s'agit donc d'une disposition technique et organisationnelle, dont les conséquences juridiques et opérationnelles doivent être examinées au cas par cas par les responsables opérationnels. Notamment, les infrastructures informatiques (serveurs applicatifs et de bases de données) peuvent être situées à l'étranger, ce qui pose des questions en matière de protection des informations sensibles et de droit applicable, par exemple aux données personnelles.

L'utilisateur peut généralement bénéficier des niveaux de services suivants :

- le niveau IaaS (*Infrastructure as a Service*). Ce service consiste à offrir un accès à un parc informatique mutualisé. Il permet donc l'accès à une infrastructure matérielle sur laquelle l'usager peut installer ses machines virtuelles et leur environnement informatique d'exploitation. C'est un service d'hébergement qui permet de mutualiser les équipements ;

- le niveau PaaS (*Platform as a Service*). Ce service met à disposition de l'usager des machines virtuelles et leur environnement informatique d'exploitation dont l'usager n'a plus à assurer le fonctionnement. L'usager installe sur ces machines virtuelles ses propres applications et ses outils. C'est un service qui permet de mutualiser les systèmes informatiques ;

- le niveau SaaS (*Software as a Service*). Dans ce type de service, les applications sont mises à la disposition des usagers qui n'ont pas à se soucier de les installer, d'effectuer les mises à jour, d'ajouter des patches de sécurité et d'assurer la disponibilité du service. L'établissement qui fait appel à ce service n'achète plus de licence logicielle mais s'abonne à ce logiciel. L'application est directement utilisable via le navigateur web.

Le *cloud computing* peut donc aller du très basique au très complet (IaaS, PaaS, SaaS, etc., le contenu précis de chacune de ces notions étant en débat). Les offres IaaS et PaaS s'adressent aux services informatiques. Les offres SaaS s'adressent directement aux utilisateurs des applications.

4.1.15. DATACENTER

Un *datacenter*, ou « centre de traitement des données », est un lieu spécialisé contenant des serveurs de gestion de base de données (SGBD), des serveurs de fichiers et des serveurs applicatifs. Il peut être propre à une organisation, ou au contraire externalisé ou mutualisé (logique de l'informatique en nuage).
Il offre généralement des niveaux de services graduels, allant de la seule fourniture de l'environnement (le bénéficiaire amène ses propres serveurs) à l'administration complète d'un ensemble applicatif. Il héberge généralement, et de plus en plus, les actifs les plus précieux d'une organisation.

Ces centres se caractérisent normalement par un environnement (énergie, climatisation, protection physique et logique, virtualisation, accès aux réseaux, outils d'administration et de supervision) très soigné, destiné à garantir un très haut niveau de disponibilité, d'intégrité et de confidentialité. Il s'agit, avec la mutualisation entre tous les utilisateurs du coût financier et humain d'un tel environnement, de leur principal atout. L'insertion d'un tel centre dans une chaîne énergétique vertueuse doit aussi favoriser l'atteinte des objectifs environnementaux de l'organisation (notion d'informatique verte, ou *green computing*).

Les deux principaux enjeux actuels sont leur localisation, pour des raisons de confidentialité et de régime juridique, et la chasse aux multiples petits datacenters « historiques » (parfois un simple PC dans un bureau), qui offrent généralement un environnement très éloigné des meilleures pratiques.

4.1.16. MAINTENANCE APPLICATIVE OU CORRECTIVE, TMA, TME

La maintenance d'une application est une activité indispensable qui consiste à adapter en continu une application à l'évolution de son environnement technique, logiciel et de sécurité. Un renouvellement de matériel nécessite, en effet, le recours à de nouveaux pilotes, une modification de pile logicielle (ensemble des outils informatiques qui permettent le fonctionnement de l'application, par exemple le système d'exploitation) doit être prise en compte par les applications et la découverte d'une faille de sécurité implique la mise en place d'une protection.

Généralement, cette maintenance coûte annuellement le cinquième du prix initial de l'application. Sa bonne exécution est de la responsabilité du propriétaire de l'application. Son suivi est le plus souvent confié à la DSI, généralement par la partie « études ». La maintenance applicative est

parfois désignée par les sigles MCO (maintien en condition opérationnelle) et MCS (maintien en condition de sécurité).

La maintenance applicative diffère de la maintenance évolutive en ce que la première n'apporte aucune évolution fonctionnelle. Au contraire, la seconde ajoute des fonctionnalités, généralement de faible ampleur. Pour les évolutions fonctionnelles plus profondes, on parle davantage de nouvelle version applicative, voire de nouveau projet.

La TMA, ou tierce maintenance applicative, consiste à externaliser la maintenance applicative et/ou évolutive à un tiers.

La TME, ou tierce maintenance d'exploitation, consiste en supplément à externaliser tout ou partie de l'infrastructure (y compris son évolution) et des fonctions d'administration et de support aux utilisateurs.
Il existe un continuum entre l'externalisation de la maintenance applicative et l'externalisation complète d'un processus, chaque situation constituant un cas d'espèce régi par des dispositions contractuelles spécifiques.

4.1.17. PROGICIEL DE GESTION INTEGREE – PGI (*ERP*)

Un PGI (progiciel de gestion intégré) ou ERP (*Enterprise Resources Planning*) est « *un progiciel qui intègre les principales composantes fonctionnelles de l'entreprise : gestion de production, gestion commerciale, logistique, ressources humaines, comptabilité, contrôle de gestion. À l'aide de ce système unifié, les utilisateurs de différents métiers travaillent dans un environnement applicatif identique qui repose sur une base de données unique. Ce modèle permet d'assurer l'intégrité des données, la non-redondance de l'information, ainsi que la réduction des temps de traitement.* »

Pour être qualifié de « progiciel de gestion intégré », une solution logicielle doit couvrir au moins deux domaines fonctionnels différents de l'entreprise (par exemple, RH et finance, ou encore finance et achats…). Un PGI peut constituer le socle du SI de l'entreprise s'il couvre la quasi-totalité des processus fonctionnels clés de celle-ci.

Un ERP peut, dans certaines limites, être paramétré pour s'adapter à l'organisation. Dans la pratique, c'est surtout l'organisation qui doit s'adapter à l'ERP. Sa mise en place nécessitera donc une refonte parfois substantielle des processus et, dans tous les cas, un fort investissement initial.

4.2. DICTIONNAIRE DES ACRONYMES

Les acronymes ci-dessous sont ceux qui, cités dans le document, n'ont pas été définis ou explicités par ailleurs.

Batch Séquence de traitement automatique, également appelée « traitement par lots », généralement réalisée en temps différé

BPR Réingénierie des processus

GB : Business Process Reengineering

BSC Tableau de bord prospectif

GB : *Balanced score card*

COBIT Référentiel de contrôle interne informatique

GB : *Control Objectives for Information and related Technology*

COMEX Comité exécutif

CPU Core processing unit (processeur)

DBA Administration de base de données

GB : *Database administration*

HD Plateau d'assistance (technique)

GB : *Help desk*

IaaS Service d'infrastructure (dans le cadre d'une informatique en nuage)

GB : *Infrastructure as a service*

ITIL Référentiel pour la production informatique

GB : *Information Technology Infrastructure Library*

MCD Modèle conceptuel de données

OS Système d'exploitation (GB : *Operating system*)

PaaS Service d'hébergement

GB : *Platform as a Service*

PCA/PRA Plan de continuité de l'activité/Plan de reprise de l'activité

PCI/PRI Plan de continuité de l'informatique/Plan de reprise de l'informatique

SaaS Logiciel en tant que service (dans le cadre d'une informatique en nuage)

GB : *Software as a service*

SAN Réseau de stockage de données

GB : *Storage Area Network*

SGBD Serveur de gestion de base de données

SSO Identifiant unique (GB : *Single sign-On*)

TP Traitement en temps réel, aussi appelé « Traitement transactionnel »

GB : *Transaction Processing*

UML Langage de modélisation unifié

GB : *Unified Modeling Language*

YTD Année glissante

GB : *Year to date*

CHAI
COMITÉ D'HARMONISATION DE L'AUDIT INTERNE

SECRETARIAT GENERAL

FICHE D'EVALUATION DU GUIDE D'AUDIT DES SYSTEMES D'INFORMATION

Nous vous remercions d'avoir utilisé cette première version du ***Guide d'audit des Systèmes d'Information***.
Afin de pouvoir l'améliorer et élaborer d'autres documents à l'intention des auditeurs internes de l'Etat, nous vous demandons de prendre quelques minutes pour remplir la présente fiche d'évaluation.

1. A quelle occasion avez-vous utilisé ce guide ?
   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……

2. Aviez-vous déjà une expérience de ***l'audit des Systèmes d'information ?***
   ☐ **Oui** :……
   ……

   ☐ **Non :**……
   ……

3. Aviez-vous déjà été formé à ***l'audit des Systèmes d'information?***
   ☐ **Oui** :……
   ……

   ☐ **Non :**……
   ……

4. Globalement, ce guide vous a-t-il apporté l'aide dont vous aviez besoin ?

   ☐ **Oui** :……
   ……

   ☐ **Non :**……
   ……

5. L'avez-vous trouvé facile d'utilisation ?
   ☐ **Oui** :……
   ……

   ☐ **Non :**……

……

6. Le niveau de détail abordé vous a-t-il semblé adéquat ?

☐ **Oui** :……

……

☐ **Non :**……

……

7. Le cas échéant, quels aspects auriez-vous souhaité voir plus développés ? Quels aspects vous ont-ils parus trop développés ?

☐ **Pas assez développés** :

……

……

……

☐ **Trop développés** :……

……

……

8. Pouvez-vous évaluer l'utilité de ce guide sur une échelle de 1 (peu utile) à 5 (extrêmement utile) ?

☐ 1. Peu utile
☐ 2. Assez utile
☐ 3. Utile
☐ 4. Très utile
☐ 5. Extrêmement utile

9. Souhaitez-vous formuler d'autres commentaires ou suggestions ?

……
……
……
……
……
……
……
……
……
……

*

* *

Vous pouvez également télécharger ce formulaire au format électronique à l'adresse suivante :
http://www.action-publique.gouv.fr/files/questionnaire_guide_si.doc

Formulaire à renvoyer :
a) par voie électronique à : *sec-gen.chai@finances.gouv.fr ;*

b) ou voie postale à :

Secrétariat général du CHAI - Télédoc 659 –
139 rue de Bercy
75572 Paris Cedex 12