



GUIDE D'AUDIT DES SYSTÈMES D'INFORMATION

Sommaire

Introduction	2
I. Les systèmes d'information : enjeux et risques	2
A. Le système d'information	2
B. Les principaux risques informatiques	4
II. Périmètre des audits des systèmes d'information	5
A. L'audit des SI à l'occasion de missions « généralistes »	6
B. Les missions d'audit dont l'objet principal appartient au domaine des SI	6
III. Orientation et planification de la mission	7
A. La prise de connaissance de l'informatique dans l'entité	8
B. Description du système d'information de l'entité	8
IV. Les techniques d'audit assistées par ordinateur	11
V. Approche thématique des principaux domaines d'audit des SI	12
A. Audit de sécurité	12
B. Audit des projets	13
VI. Le contrôle interne en milieu informatique	15
A. Les contrôles généraux et applicatifs des SI	17
B. Les contrôles généraux	17
C. Les contrôles applicatifs	18
VII. Les normes internationales de références	31
Annexes	33
Annexe 1 Fiche d'audit détaillée relative à la prise de connaissance de l'informatique de l'entité	33
Annexe 2 Fiche d'audit relative à la cartographie des applications	39
Annexe 3 Fiche d'audit relative à l'identification des processus à analyser	41
Annexe 4 Fiche d'audit détaillée relative à la sécurité informatique	42
Annexe 5 Fiche d'audit relative au projet informatique	48
Annexe 6 Dictionnaire des expressions spécifiques	49
Annexe 7 Types de contrôles liés aux applications	59

Introduction

L'audit réalisé dans un environnement informatique peut poser aux auditeurs des difficultés en termes de mise en œuvre en termes d'approche, de nature des contrôles à réaliser et d'exploitation des résultats obtenus à l'issue de ces contrôles.

L'émergence des nouvelles technologies de l'information ainsi que la complexité croissante des systèmes d'information automatisés ont conduit la Cour à élaborer le présent guide. Il permet d'orienter et de faciliter les travaux de l'auditeur en charge de l'audit des systèmes d'information, quel que soit le type de l'entité concernée. L'objectif du présent guide est d'apporter à l'auditeur des solutions opérationnelles dans le cadre de la prise en compte de l'environnement informatique dans son audit.

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. Le guide est complété par des fiches d'audit figurant en annexe, elles sont présentées selon l'ordre de présentation au travers du guide.

Ce document est une première version, des adaptations peuvent s'imposer pour le rendre adéquat au système d'information de l'entité auditée.

I. Les systèmes d'information : enjeux et risques

A. Le système d'information

1. Définition

Le système d'information représente l'ensemble des ressources humaines et matérielles participant à la collecte, au stockage, à la gestion, au traitement, au transport et à la communication de l'information au sein de l'entité, il s'appuie souvent sur un système informatique.

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 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.

Un PGI (progiciel de gestion intégré) est la traduction en Français du terme ERP «Enterprise Resource Planning» qui signifie « planification des ressources de l'entreprise ». C'est un ensemble d'applications intégrées couvrant l'ensemble des activités de l'entité : gestion des commandes, gestion des stocks, gestion de la comptabilité, gestion du budget, contrôle de gestion, paie. Ces applications émanent d'un éditeur de logiciel unique. Chaque application est appelée module.

2. Les facteurs clés d'un SI

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 évolutif ;*
- *est pérenne ;*
- *est disponible ;*
- *est efficace.*

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 :*
 - *une politique de sécurité ;*
 - *le respect de la législation en matière de système d'information ;*
 - *un paramétrage correct des droits d'accès aux applications informatiques ;*
 - *une bonne gestion des projets de développements informatiques ;*
 - *la formation continue des utilisateurs et des équipes informatiques ;*
 - *un contrat de maintenance.*

- *la présence d'un SI intégré.*

B. Les principaux risques informatiques

Les principaux risques informatiques peuvent être regroupés en 3 domaines :

- *les risques opérationnels (dysfonctionnement des applications, risques d'erreurs, doublons...)* ;
- *les risques financiers (les états financiers ou les comptes traduisent une situation erronée)* ;
- *les risques légaux de non-conformité (gestion des licences, loi organique n°12-05 du 12 janvier 2012 relative à l'information, décret exécutif n°09-110 du 7 avril 2019 fixant les conditions et modalités de tenue de la comptabilité au moyen de systèmes informatiques...).*

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 entité 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 MM (Material Management) : achat et gestion des stocks ;*
- *module RE (Real Estate) : gestion immobilière.*

Les principaux avantages des PGI sont les suivants :

- *réduction des délais administratifs par une mise à jour en temps réel des données;*
- *saisie unique dans le SI de l'entité ;*
- *disponibilité immédiate de l'information ;*
- *la traçabilité des opérations est assurée, la piste d'audit est « 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;*
- *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*

II. Périmètre des audits des systèmes d'information

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.).

A. L'audit des SI à l'occasion de missions « généralistes »

1. L'audit d'une organisation

Les entités ou administrations 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'entité. Ils sont parfois au cœur de sa performance.

Pourtant, les entités 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. Elles sont parfois peu ou mal organisées pour tirer le meilleur de ces ressources.

L'audit d'une entité doit donc désormais nécessairement inclure un audit de sa relation au fait informatique et répondre aux questions suivantes :

- 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 ?*

2. Les audits de processus

Les processus peuvent être très fortement dépendants des outils informatiques. Dans le meilleur des cas, ils s'appuient sur un système informatique répondant à leurs besoins.

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.

B. Les missions d'audit dont l'objet principal appartient au domaine des SI

1. Les audits d'application

Une application 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 contribuer à l'homogénéité ou 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'entité.

L'audit d'une application informatique nécessite l'examen 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.

2. Les audits de projets informatiques

L'auditeur peut se retrouver face à un projet qui, au lieu de respecter la cohérence du système d'information, contribue au contraire à l'hétérogénéité, voire au désordre du système informatique.

L'auditeur doit donc examiner la qualité de l'expression, du recueil et de la traduction du besoin. En effet, les recommandations émises au terme de l'audit ne peuvent faire abstraction de cet environnement.

L'audit d'un projet, surtout s'il est suscité par une situation non satisfaisante, 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'œuvre informatiques, voire avec les assistants du maître d'ouvrage ;*
- de la gestion des processus au sein de l'entité, notamment du processus ayant suscité le projet audité ;*
- de l'organisation de ce processus ;*
- de l'organisation de la gouvernance de la fonction informatique.*

III. Orientation et planification de la mission

Les spécificités de l'environnement informatique sont prises en compte dans les principales étapes de la démarche d'audit, à savoir :

- *La prise de connaissance de l'informatique dans l'entité*
- *L'établissement de la cartographie des applications*

A. La prise de connaissance de l'informatique dans l'entité

La première étape de l'audit des systèmes d'information est la prise de connaissance de l'organisation informatique et des systèmes d'information de l'organisation auditée. Elle consiste à collecter des informations sur les systèmes et les processus informatiques de l'entité et à en déduire leur incidence sur les procédures internes de fonctionnement.

Il s'agit notamment de connaître et d'apprécier :

- *la structure organisationnelle chargée des systèmes d'information et ses composantes (entités, effectifs, équipements et ressources (matériels, applications, et humaines) ;*
- *les missions, objectifs et finalités de la structure en charge de l'informatique et des systèmes d'information ;*
- *le plan informatique et/ou schéma directeur en vigueur ;*
- *l'architecture informatique ;*
- *la conformité aux exigences légales ;*
- *la sécurité informatique.*

La démarche d'audit de cette première étape est décrite en Annexe 1 – Fiche d'audit relative à la prise de connaissance de l'informatique de l'entité.

La réalisation de cette étape permet à l'auditeur de comprendre l'environnement informatique de l'entité auditée ainsi que d'apprécier la maîtrise par l'entité du système d'information.

B. Description du système d'information de l'entité

La deuxième étape consiste à dresser la cartographie des applications.

La description du système d'information de l'entité consiste à :

- *Formaliser la cartographie des applications ;*
- *Apprécier le degré de complexité du SI ;*
- *Identifier les processus à analyser.*

La réalisation d'une cartographie des applications permet de comprendre et de documenter les composantes du SI. Elle permet en outre de mettre en évidence les risques potentiels liés à cette architecture.

L'établissement de la cartographie du système d'information nécessite l'identification des principales applications et interfaces et se termine par l'identification des processus à analyser.

Identification des principales applications informatiques

L'identification des applications informatiques concerne le recensement des applications qui composent le système d'information de l'entité. Pour chacune d'elles, il est nécessaire de connaître :

- *Nom de l'application ;*
- *Utilisateur ;*
- *Fonctionnalités ;*
- *Hébergement sur des serveurs interne ou hébergement externalisé sur des serveurs externes ;*
- *Type (développement interne, développement par un tiers, progiciel, fichier bureautique) ;*
- *Date de mise en place ;*
- *Prestataire pour la maintenance ;*
- *Date de la dernière modification ;*
- *Date de fin d'utilisation prévue ;*
- *OS du serveur hébergeant l'application : UNIX, Windows, AS400... ;*
- *Base de données : SQL Server... ;*

- *Projet dévolution ;*
- *Principales fonctionnalités ;*
- *Nature des sorties ;*
- *Une estimation du volume traité ;*
- *Criticité de l'application.*

Identification des principales interfaces

L'identification des principales interfaces concerne les liens qui existent entre les différentes applications. Ces liens peuvent être automatiques, semi-automatiques ou manuels. Pour chaque interface identifiée, il est nécessaire de connaître :

- *le type d'interface : automatique, semi-automatique, manuel ;*
- *les applications en amont (source) / en aval (destination) ;*
- *le type des flux : ventes, stocks, clients... ;*
- *le protocole d'échange de données ;*
- *la périodicité : quotidienne, hebdomadaire, mensuelle... ;*
- *le déclenchement ;*
- *les données échangées ;*
- *les contrôles.*

Identification des principales interfaces

L'équipe de contrôle ne s'intéresse pas à tous les processus existant au sein de l'entité, mais uniquement ceux « contribuant directement ou indirectement à la production des données financières ».

La cartographie est un outil clé pour l'environnement informatique de l'entité.

La démarche d'audit de cette étape est décrite en Annexe 2 – Fiche d'audit relative à la cartographie des applications ainsi qu'en Annexe 3 – Fiche d'audit relative à l'identification des processus à analyser.

IV. Les techniques d'audit assistées par ordinateur

Les étapes de la mise en œuvre des techniques d'audit assistées par ordinateur sont :

1. Étape 1 : récupération des fichiers informatiques

Il convient de définir avec l'entité la nature des tests à réaliser sur la base de l'analyse de la cartographie des applications. Il s'agit de :

- *identifier les logiciels présentant un risque (enjeux importants, montants substantiels, fonctions clés, etc.) ;*
- *définir les données nécessaires à exploiter ;*
- *récupérer les fichiers nécessaires à la réalisation des tests informatiques utiles à l'audit.*

Une première difficulté apparaît du fait de l'existence dans les entités de systèmes diversifiés et de progiciels d'origine différente, qui ne gèrent pas le même type de données. La récupération des fichiers à un format et sur un support adaptés est une phase essentielle mais complexe, compte tenu de la diversité des systèmes informatiques dans les entités (logiciels spécifiques, progiciels, différences de technologie...). Le format des supports de données reçus est très varié.

2. Étape 2 : Validation des fichiers

Elle s'effectue notamment par rapprochement des fichiers reçus avec la comptabilité. Il s'agit de vérifier, avant d'effectuer les tests, que les données reçues sont exhaustives et qu'elles n'ont subi aucune modification lors de l'extraction.

3. Réalisation des tests

Le lancement des tests peut alors démarrer. Il est important que les tests réalisés soient reproduits ultérieurement et que toutes les étapes intermédiaires soient sauvegardées. Ainsi, l'existence d'un journal des tests effectués dans le logiciel d'audit sélectionné peut s'avérer utile pour leur identification. Cette phase aboutit à la constitution d'un dossier contenant les différentes étapes du cycle de réalisation et de validation.

4. Analyse et synthèse

La dernière phase consiste à analyser et à interpréter les résultats, qui sont alors consignés dans un rapport de synthèse décrivant notamment les tests réalisés et les recommandations qui en découlent.

V. Approche thématique des principaux domaines d'audit des SI

Les thèmes précédents « orientation et planification de la mission » et « description du système d'information de l'entité » sont transverses. Les thèmes suivants doivent être considérés comme venant en complément.

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. Ainsi, ils peuvent ne pas être totalement applicables et appropriés pour certains modes d'organisation.

A. Audit de sécurité

L'information est un actif précieux de l'entité. 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.

L'étude de la fonction informatique donne une cartographie des risques sur les axes de vigilance majeurs : Sécurité physique des salles informatiques, Procédures de sauvegardes des applications et des fichiers de travail, Plan de secours en cas de sinistre, Sécurité des accès aux données de l'entité, Procédures du service informatique, Processus de gestion de projets informatiques.

L'obtention des documents suivants préalablement à l'intervention permettra à l'auditeur d'apprécier la stratégie de sécurité informatique :

- 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).*

La démarche d'audit de sécurité est décrite en Annexe 6 – Fiche d'audit relative à la sécurité informatique.

B. Audit des projets

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.

La conduite d'un projet comprend les étapes suivantes :

- L'étude d'opportunité et l'expression des besoins : ce 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.*
- La planification : l'entité 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 Direction des systèmes d'information (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.*
- Les instances de pilotages : il existe différentes instances de pilotage qui peuvent être 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 méthodes et les outils : 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.*

- *La conception : 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.

- *Développement, réalisation ou paramétrage : 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.

- *Tests et recettes : 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.

- *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.*
- 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.*

La démarche d'audit de sécurité est décrite en Annexe 5 – Fiche d'audit relative au projet informatique.

VI. Le contrôle interne en milieu informatique

Les technologies de l'information peuvent potentiellement éliminer les risques liés à un système manuel, mais introduire leurs propres risques. En outre, étant donné la nature des activités informatiques, ces risques peuvent également s'affecter les uns les autres :

- Pistes d'audit physiques remplacées par des pistes de données. Bon nombre de documents physiques sont éliminés pour les audits et des contrôles doivent être utilisés pour compenser.*
- Défaillance matérielle/logicielle. La perte permanente de données, par exemple, en raison de dommage environnemental, d'indisponibilités, de désorganisation ou de sinistre, a un coût élevé.*

- **Erreurs systématiques.** Les technologies de l'information réduisent les erreurs aléatoires, notamment lors de la saisie des données, mais les systèmes automatisés peuvent uniformément dupliquer les erreurs, par exemple, au moyen d'un code erroné.
- **Moins de saisies humaines / moins de séparation des fonctions.** De nombreux systèmes informatiques réduisent les coûts du travail via l'automatisation. Les contrôles d'atténuation incluent la vérification de la séparation des fonctions et la vérification par les utilisateurs finaux de leur sortie à un niveau d'agrégation suffisamment faible pour pouvoir détecter les problèmes.
- **Autorisation d'accès.** La capacité accrue d'accès à des informations sensibles à distance augmente également le risque d'accès non autorisé.
- **Autorisation de transactions automatisées.** Les transactions qui exigeaient auparavant une vérification et une autorisation peuvent être intégralement régulées par une application informatique. L'assurance d'autorisation dépend des contrôles logiciels et de l'intégrité du fichier maître.
- **Actes volontairement dommageables.** Les salariés/agents malhonnêtes ou mécontents disposant de leur propre accès ainsi que des individus extérieurs motivés par le profit ou la destruction peuvent provoquer des dommages significatifs pour une organisation. Les collègues de confiance représentent le plus grand risque.

Les défis d'un audit des technologies de l'information consistent à identifier et évaluer correctement le contrôle des risques liés aux technologies de l'information, un auditeur doit :

- *Comprendre l'objectif d'un contrôle informatique, le type de contrôle dont il s'agit et ce à quoi il est destiné.*
- *Évaluer l'importance du contrôle pour l'entité : les bénéfices qui reviennent à l'entité au moyen du contrôle (par exemple, conformité légale ou avantage compétitif) et les dommages que peut provoquer un contrôle faible ou inexistant.*
- *Identifier les individus ou postes responsables de l'exécution des différentes tâches.*
- *Équilibrer le risque posé par les exigences de création d'un contrôle.*
- *Implémenter un cadre de contrôle et un plan d'audit appropriés.*

A. Les contrôles généraux et applicatifs des SI

On peut classifier les contrôles de manière à en comprendre les objectifs et à savoir où ils s'insèrent au sein du système de contrôle interne. La compréhension de ces classifications permet à l'auditeur de mieux connaître leur position au sein du système de contrôle et de répondre aux questions cruciales, telles :

- les contrôles détectifs sont-ils adéquats pour identifier les erreurs qui pourraient échapper aux contrôles préventifs ?*
- les contrôles correctifs sont-ils suffisants pour corriger les erreurs une fois celles-ci détectées ?*

Une classification courante des contrôles des SI, est de séparer les contrôles généraux des contrôles applicatifs.

B. Les contrôles généraux

Les contrôles généraux (CGTI) s'appliquent à l'ensemble des composantes, processus et données d'une organisation ou d'un environnement système. Sans se limiter à ces domaines, les contrôles généraux incluent la gouvernance des SI, la gestion des risques, la gestion des ressources, l'exploitation, le développement et la maintenance des applications, la gestion des utilisateurs, la sécurité logique, la sécurité physique, la gestion des changements des systèmes, la sauvegarde et la restauration de données, ou la continuité d'activité.

Certains contrôles généraux sont liés aux métiers (par exemple la séparation des fonctions ou l'organisation de la gouvernance), alors que d'autres sont plus techniques (tels que les contrôles des systèmes de logiciels et les contrôles réseaux) et sont liés à l'infrastructure sous-jacente.

Les contrôles généraux sont revus par l'auditeur, car ils sont la base de l'environnement de contrôle des SI. Si les contrôles généraux sont peu fiables (par exemple le contrôle des accès et des changements), l'auditeur devra modifier son approche des tests pour les zones impactées.

Les CGTI les plus courants sont les suivants :

- Contrôles d'accès logique à l'infrastructure, aux applications et aux données ;*
- Contrôles sur la gestion des changements dans les programmes ;*

- *Contrôles de sécurité physique sur le centre de traitement informatique ;*
- *Contrôles de sauvegarde et de restauration des systèmes et des données ;*
- *Contrôles de l'exploitation.*

La revue des CGTI a été exposée dans les premières parties de ce guide, la suite du document se concentrera sur la revue des contrôles applicatifs.

C. Les contrôles applicatifs

Les contrôles applicatifs portent sur l'étendue des processus de l'organisation ou ses applications et incluent les contrôles au niveau des entrées, des traitements et des sorties des applications. Il s'agit, notamment, de la validation de données, de la séparation des tâches (par exemple : saisie et autorisation d'une transaction), balance des totaux de contrôle, journalisation des transactions et des rapports d'erreurs.

Le rôle d'un contrôle est primordial pour en évaluer la conception et l'efficacité. On peut généralement différencier les contrôles préventifs, détectifs et correctifs.

Les contrôles préventifs

Les contrôles préventifs permettent d'éviter la survenue d'erreurs, d'omissions ou d'incidents de sécurité. Il s'agit, par exemple, de simples règles de validation des données dès leur saisie, qui empêchent d'entrer des caractères alphabétiques dans des champs numériques, de contrôles d'accès grâce auxquels les données sensibles ou les ressources système deviennent inaccessibles aux individus non autorisés, ou encore de contrôles techniques dynamiques et complexes tels que les logiciels antivirus, les pare-feu et les systèmes anti-intrusion.

Les contrôles détectifs

Les contrôles détectifs visent à repérer les erreurs ou les incidents qui échappent aux contrôles préventifs. Ainsi, un contrôle détectif peut identifier le nombre de comptes inactifs ou les comptes qui ont été signalés comme devant faire l'objet d'une surveillance pour déceler des activités suspectes.

Les contrôles détectifs peuvent aussi prendre la forme d'une surveillance ou d'analyses visant à mettre au jour des activités ou des événements hors des limites autorisées ou des schémas connus pour certaines données, pouvant être sujet à une manipulation inadéquate. Pour les échanges de données sensibles, des contrôles détectifs peuvent indiquer si un message est corrompu ou si l'identité de l'expéditeur ne peut être authentifiée.

Les contrôles correctifs

Les contrôles correctifs ont pour but de corriger les erreurs, omissions ou incidents une fois ceux-ci détectés. Il peut s'agir de la simple correction d'erreurs de saisie, de l'identification et la suppression d'utilisateurs ou de logiciels non autorisés, dans un système ou un réseau, ou encore de la reprise après un incident, une panne ou un sinistre.

Généralement, il est plus efficace de prévenir les erreurs ou de les détecter à un niveau aussi proche que possible de la source pour en simplifier la correction.

Les points de contrôle interne portant sur les applications veillent à ce que :

- Toutes les données saisies soient exactes, complètes, autorisées et correctes ;*
- Toutes les données soient traitées comme prévu ;*
- Toutes les données stockées soient exactes et complètes ;*
- Tous les résultats soient exacts et complets ;*
- Le traitement des données fait l'objet de traces (logs) depuis la saisie jusqu'au stockage et à la production de données de sortie ;*

L'examen des contrôles d'application constitue le domaine des auditeurs informatiques. Cependant, ce type de contrôles représentant désormais une composante essentielle de la maîtrise des activités, tous les auditeurs (internes/externes) devraient en faire une priorité.

Différents types de contrôles courants devraient exister dans chaque application :

- Les contrôles des données d'entrée : ils servent essentiellement à vérifier l'intégrité des données saisies dans une application, qu'elles soient saisies directement par les utilisateurs, à distance par un partenaire ou à travers une application Web. Une vérification des entrées permet de s'assurer qu'elles respectent les paramètres spécifiés.*
- Les contrôles du traitement : ils procurent un moyen automatisé de s'assurer que le traitement est complet, exact et autorisé.*
- Les contrôles des données de sortie : ils portent sur ce qui est fait des données. Ils doivent comparer les résultats obtenus aux résultats attendus, et les vérifier par rapport à ce qui a été saisi.*

- *Les contrôles d'intégrité : ils peuvent s'appliquer de façon permanente sur les données en cours de traitement et/ou stockées, afin de s'assurer qu'elles restent cohérentes et exactes.*
- *La traçabilité : le fait de traiter l'historique des contrôles, ce qu'on appelle souvent une piste d'audit, permet au management de suivre les transactions depuis la source jusqu'au résultat final ou de remonter à partir des résultats jusqu'aux transactions et les événements enregistrés qui les ont générés. Ces contrôles doivent permettre de surveiller l'efficacité de l'ensemble des contrôles et de déceler les erreurs le plus en amont possible.*

1. Le plan d'audit

Les auditeurs doivent élaborer un plan pour chaque mission d'audit. Ce plan doit mentionner les objectifs, l'étendue, les ressources et le programme de travail. Les objectifs permettent à l'auditeur de déterminer si les contrôles applicatifs sont bien conçus et fonctionnent efficacement, afin de gérer les risques afférant à la communication financière, au respect de la réglementation et aux paramètres opérationnels.

Les contrôles applicatifs ont pour objectifs de vérifier que :

- *Les données d'entrée sont exactes, complètes, autorisées et correctes ;*
- *Les données sont traitées conformément aux objectifs et dans un délai acceptable ;*
- *Les données stockées sont exactes et complètes. ;*
- *Les données de sortie sont exactes et complètes ;*
- *Les processus d'entrée, de stockage et de sortie des données sont archivés.*

Nous proposons le plan d'audit suivant qui pourra être adapté en fonction de la situation rencontrée :

Exemple de plan d'audit

Un examen des données propres à l'entité ainsi que l'étendue de l'audit détermineront les étapes de la revue détaillée des activités suivantes.

Objectif 1 : Les données d'entrée sont exactes, complètes, autorisées et correctes

Contrôles	Activités liées à la revue
<i>Les contrôles portant sur les données d'entrée sont conçus et fonctionnent efficacement de manière à veiller à ce que toutes les transactions aient été autorisées et validées avant la saisie des données.</i>	<p><i>Se procurer les procédures de saisie des données, comprendre le processus d'autorisation et de validation, déterminer s'il existe un processus d'examen et de validation et s'il a été communiqué aux utilisateurs chargés d'obtenir les autorisations correspondantes.</i></p> <p><i>Vérifier que le propriétaire de l'application ou du processus veille à ce que toutes les données soient autorisées avant leur saisie. Cette assurance peut passer par la répartition des rôles et des responsabilités selon les fonctions de chaque poste.</i></p> <p><i>Se procurer une copie des niveaux d'autorisation et déterminer si quelqu'un a été chargé de vérifier que les autorisations correspondantes sont toujours respectées.</i></p>
<i>Les contrôles portant sur les données d'entrée sont conçus et fonctionnent efficacement de manière à veiller à ce que toutes les transactions saisies soient traitées correctement et intégralement.</i>	<p><i>Se procurer les procédures de saisie des données et vérifier que les individus responsables de la saisie des données ont été formés à l'élaboration, à la saisie et au contrôle des données d'entrée.</i></p> <p><i>Déterminer si les routines d'édition sont intégrées dans l'application qui vérifie puis rejette les informations entrées qui ne satisfont pas à certains critères : dates incorrectes, caractères incorrects, longueurs de champ non valides, données manquantes et entrées/numéros de transactions en double (la liste n'est pas exhaustive).</i></p> <p><i>Vérifier l'existence et le fonctionnement de contrôles manuels pour éviter les saisies en double. Les contrôles manuels peuvent comporter la prénumérotation des documents sources et l'apposition de la mention « entré » après saisie.</i></p> <p><i>Vérifier que les données ajoutées proviennent d'une source acceptable et soient rapprochées de cette source à l'aide de totaux de contrôle, de nombres d'enregistrements et d'autres techniques, comme les rapports de sources indépendantes.</i></p> <p><i>Déterminer si la séparation des fonctions est suffisante pour éviter que les utilisateurs saisissent et autorisent des transactions.</i></p> <p><i>Vérifier que la séparation des fonctions soit suffisante entre les individus qui saisissent les données et ceux qui sont chargés du rapprochement et de la vérification de l'exactitude et de l'exhaustivité des données de sortie.</i></p> <p><i>Vérifier que des contrôles sont en place pour éviter les changements non autorisés.</i></p>

<p><i>Les contrôles portant sur les données d'entrée sont conçus et fonctionnent efficacement pour veiller à ce que toutes les transactions rejetées aient été identifiées et retraitées correctement et intégralement.</i></p>	<p><i>Se procurer les procédures de saisie des données pour le traitement des transactions rejetées et la correction ultérieure des erreurs et vérifier que le personnel responsable de la correction des erreurs et de la ressaisie des données a reçu la formation adéquate.</i></p> <p><i>Vérifier qu'un mécanisme est en place permettant d'avertir le propriétaire du processus que des transactions ont été rejetées ou que des erreurs se sont produites.</i></p> <p><i>Vérifier que les éléments rejetés sont retraités correctement et dans les délais, conformément aux procédures.</i></p>
<p><i>Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce que les données envoyées automatiquement depuis un autre système soient traitées correctement et intégralement.</i></p>	<p><i>Se procurer les procédures et vérifier l'existence d'informations détaillées sur la procédure d'autorisation des interfaces automatisées et sur les éléments déclenchant un traitement automatisé.</i></p> <p><i>Vérifier que les calendriers de traitement sont consignés dans un document et que les problèmes sont identifiés et corrigés rapidement.</i></p> <p><i>Déterminer si les comptages des enregistrements de système à système et le total des valeurs monétaires sont systématiquement vérifiés pour les interfaces automatisées et si l'on empêche les éléments rejetés de s'afficher et si on les a marqués en vue d'un suivi et d'un retraitement.</i></p> <p><i>Vérifier que tous les fichiers et toutes les données créés pour être utilisés par d'autres applications ou qui sont transférés à d'autres applications sont protégés contre toute modification non autorisée pendant tout le processus de transfert.</i></p>
<p><i>Les contrôles sont conçus et fonctionnent efficacement pour faire en sorte que les bons fichiers de données et bases de données soient utilisés lors du traitement.</i></p>	<p><i>Confirmer que les données et programmes d'essais sont séparés de la production.</i></p>
<p><u>Objectif 2 : Les données sont traitées conformément aux objectifs et dans un délai acceptable</u></p>	
<p>Contrôles</p>	<p>Activités liées à la revue</p>
<p><i>Les contrôles sur le traitement sont conçus et fonctionnent efficacement pour que toutes les transactions soient traitées rapidement et durant la période comptable correspondante.</i></p>	<p><i>Vérifier que les données de sorties sont examinées ou rapprochées avec les documents sources pour en confirmer l'exhaustivité et l'exactitude, notamment par la vérification des totaux de contrôle.</i></p> <p><i>Déterminer si l'application contient les routines, qui assurent que toutes les opérations correctement saisies sont bien traitées et enregistrées comme prévu pour la période comptable correspondante.</i></p>

<p><i>Les contrôles sur le traitement sont conçus et fonctionnent efficacement pour que toutes les transactions rejetées soient identifiées et rapidement retraitées.</i></p>	<p><i>Se procurer les procédures de traitement des transactions rejetées et de correction des erreurs et déterminer si le personnel chargé de la correction des erreurs et de la ressaisie des données a reçu la formation adéquate.</i></p> <p><i>Vérifier qu'un mécanisme avertit le propriétaire du processus lorsque des transactions ont été rejetées ou que des erreurs sont survenues.</i></p> <p><i>Vérifier que les éléments rejetés sont traités correctement et rapidement, conformément aux procédures, et que les erreurs sont corrigées avant la ressaisie dans le système.</i></p>
---	---

Objectif 3 : Les données stockées sont exactes et complètes

Contrôles	Activités liées à la revue
<p><i>Les contrôles d'accès logique sont conçus et fonctionnent efficacement pour prévenir l'accès, la modification ou la divulgation non autorisés de données système.</i></p>	<p><i>Se procurer la configuration et les procédures d'utilisation des mots de passe et vérifier la présence de critères obligatoires concernant les mots de passe, le renouvellement des mots de passe, le verrouillage du compte et la réutilisation des mots de passe.</i></p> <p><i>Vérifier que les dispositions décrites ci-dessus sont bien appliquées aux applications examinées.</i></p> <p><i>Vérifier que des contrôles d'accès à distance sont conçus et fonctionnent efficacement.</i></p> <p><i>Vérifier que les utilisateurs ne peuvent exécuter que des fonctions spécifiques, conformément aux responsabilités inhérentes à leur poste (accès fondé sur les rôles).</i></p> <p><i>Vérifier que des numéros d'identification utilisateur uniques ont été attribués à tous les utilisateurs, y compris les utilisateurs privilégiés, et que les comptes utilisateurs et administrateurs ne sont pas partagés.</i></p> <p><i>Vérifier que la création et la modification des comptes utilisateurs sont dûment autorisées avant d'accorder ou de modifier l'accès. (Les utilisateurs sont les utilisateurs privilégiés, les salariés, les sous-traitants, les fournisseurs et les intérimaires).</i></p> <p><i>Vérifier que l'accès est supprimé immédiatement après la fin du contrat de travail.</i></p> <p><i>Vérifier que le propriétaire de l'application veille à ce qu'un examen semestriel des comptes utilisateurs et système soit effectué pour confirmer que l'accès aux données financières, applications et systèmes opérationnels critiques est correct et à jour.</i></p>
<p><i>Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce que la sauvegarde des données soit</i></p>	<p><i>Vérifier que la création et la modification des comptes utilisateurs sont dûment autorisées avant d'accorder ou de modifier l'accès. (Les utilisateurs sont les utilisateurs privilégiés, les salariés, les sous-traitants, les fournisseurs et les intérimaires).</i></p>

<i>rigoureuse, complète et rapide.</i>	<p><i>Vérifier que l'accès est supprimé immédiatement après la fin du contrat de travail.</i></p> <p><i>Vérifier que le propriétaire de l'application veille à ce qu'une revue semestrielle des comptes utilisateurs et système est effectuée pour confirmer que l'accès aux données financières, applications et systèmes opérationnels critiques est correct et à jour.</i></p>
<i>Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce que les données soient physiquement stockées dans un lieu sécurisé, hors site et à environnement contrôlé.</i>	<i>Vérifier que des mécanismes sont en place pour stocker des données hors site dans un lieu sécurisé et à environnement contrôlé.</i>
<u>Objectif 4 : Les données de sortie sont exactes et complètes</u>	
Contrôles	Activités liées à la revue
<i>Les contrôles sur les sorties sont conçus et fonctionnent efficacement pour veiller à ce que tous les résultats issus des transactions soient complets et précis.</i>	<p><i>Se procurer les procédures de sortie des données, comprendre le processus d'examen et vérifier que les individus responsables de la saisie sont formés à l'analyse et à la vérification des sorties de données.</i></p> <p><i>S'assurer que les données de sortie sont examinées ou rapprochées avec les documents source pour en vérifier l'exhaustivité et l'exactitude, y compris en vérifiant les totaux de contrôle.</i></p>
<i>Les contrôles sur les sorties sont conçus et fonctionnent efficacement pour veiller à ce que tous résultats issus des transactions soient diffusés au personnel approprié et que les informations sensibles et confidentielles soient protégées durant leur diffusion.</i>	<i>Examiner les procédures existantes sur les sorties de données et déterminer si elles précisent quel personnel les reçoit et comment ces données sont protégées lors de leur diffusion.</i>
<i>Les contrôles sur les sorties de données sont conçus et fonctionnent efficacement pour veiller à ce qu'un rapport de sortie soit créé au moment indiqué et couvre la période indiquée.</i>	<p><i>Vérifier qu'un rapport de sortie a été créé et que la date et l'heure du rapport correspondent bien au moment indiqué.</i></p> <p><i>Vérifier que le rapport couvre la période indiquée par un rapprochement avec les documents sources pour cette période.</i></p>

Objectif 5 : Les processus d'entrée, de stockage et de sortie des données sont archivés

Contrôles	Activités liées à la revue
<i>Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce qu'une piste d'audit soit générée et actualisée pour toutes les données relatives aux transactions.</i>	<i>Vérifier l'existence de pistes et journaux d'audit qui confirment que tous les dossiers ont été traités et permettent de suivre la transaction de la saisie des données à leur stockage et à leur sortie. Vérifier l'existence de rapports d'audit qui retracent l'identification et le retraitement des transactions rejetées. Ces rapports doivent contenir une description claire de la transaction rejetée, de la date et de l'heure indiquées</i>

2. Contrôles applicatifs courants et propositions de tests

Les paragraphes qui suivent décrivent les contrôles applicatifs (cf. Annexe 7) communs avec les tests proposés pour chaque contrôle.

a. Contrôles des entrées

Ces contrôles sont conçus pour apporter une assurance raisonnable que les données reçues pour un traitement informatique sont dûment autorisées et converties dans une forme assimilable par une machine, et que des données ne sont pas perdues, supprimées, ajoutées, dupliquées ou indûment modifiées. Les contrôles des entrées informatisés comprennent des procédures de vérification et de validation des données telles que les chiffres clés, le nombre d'enregistrements, les totaux de contrôle et les totaux financiers de contrôle, tandis que les routines d'édition informatisées, conçues pour détecter les erreurs de données, regroupent des contrôles de la validité des caractères, des contrôles des données manquantes, des tests de séquence et des contrôles de vraisemblance.

Le tableau ci-après présente les contrôles des entrées et les tests préconisés.

Contrôles des entrées et des accès		
<i>Ces contrôles permettent de vérifier que toutes les données d'entrée sont exactes, complètes et autorisées.</i>		
Domaine	Contrôle	Tests possibles
<i>Vérification et validation des données</i>	<ul style="list-style-type: none"> • Contrôles de vraisemblance sur les valeurs financières. • Contrôles des formats et des champs requis, écrans d'entrée standardisés. • Contrôles de séquence (p. ex. éléments manquants), contrôle des limites et chiffres clés. • Contre-vérification (certaines politiques ne sont valides qu'avec certains codes de table premium). • Validations (p. ex. table en mémoire et menu déroulant des éléments valides). 	<ul style="list-style-type: none"> • Tester des échantillons pour chaque scénario. • Observer les tentatives d'entrer des données incorrectes. • Déterminer qui peut passer outre les contrôles. • S'ils sont gérés par tables, déterminer qui peut altérer les modifications et les niveaux de tolérance.
<i>Autorisation et agrément automatisés et contournement (Override)</i>	<ul style="list-style-type: none"> • Des droits d'autorisation (p. ex. pour les dépenses, le paiement des créances ou les crédits au-delà d'un certain seuil) sont accordés à des utilisateurs sur la base de leurs rôles et de leur besoin d'utiliser l'application. • Le pouvoir de passer outre (p. ex. l'autorisation de créances d'un montant inhabituellement élevé) est réservé à certains utilisateurs, sur la base de leurs rôles et de leur besoin d'utiliser l'application. 	<ul style="list-style-type: none"> • Procéder à des tests sur la base des droits d'accès des utilisateurs. • Vérifier les privilèges d'accès pour chaque fonction ou transaction sensible. • Examiner les droits d'accès qui établissent et modifient des limites configurables d'agrément ou d'autorisation.
<i>Séparation automatisée des fonctions et des droits d'accès</i>	<ul style="list-style-type: none"> • Les individus qui décident qui sont les fournisseurs agréés ne peuvent pas engager de transactions d'achat. • Les individus qui ont accès au traitement des créances ne doivent pas être en mesure de définir ou d'amender une politique. 	<ul style="list-style-type: none"> • Procéder à des tests sur la base des droits d'accès des utilisateurs. • Examiner les droits d'accès qui établissent et modifient des rôles configurables ou des structures de menu.

<p><i>Éléments en attente</i></p>	<ul style="list-style-type: none"> • Les superviseurs vérifient tous les jours ou une fois par semaine les rapports chronologiques faisant apparaître des nouveaux éléments des politiques dont le traitement est incomplet. • Les fichiers en attente pour lesquels les informations disponibles sont insuffisantes pour permettre un traitement de la transaction. 	<ul style="list-style-type: none"> • Examiner le résultat du classement chronologique et la preuve des procédures d'examen par les superviseurs. • Cheminer dans un échantillon vers et depuis le rapport chronologique ou le fichier en attente.
-----------------------------------	--	---

<p>Contrôles de la transmission des fichiers et des données</p>		
<p><i>Ces contrôles permettent de vérifier que les fichiers et les transactions transmis en interne ou à l'extérieur par voie électronique ont été envoyés par une source identifiée et traités exactement et complètement.</i></p>		
Domaine	Contrôle	Tests possibles
<p><i>Contrôles des transmissions des fichiers</i></p>	<ul style="list-style-type: none"> • Contrôle de l'exhaustivité et de la validité du contenu, y compris la date et l'heure, la taille des données, le volume des enregistrements et l'authentification de la source. 	<ul style="list-style-type: none"> • Observer les rapports de transmission et d'erreur. • Observer les paramètres de validité et d'exhaustivité et les réglages. • Examiner les droits d'accès à la définition et à la modification des paramètres configurables pour le transfert de fichiers.
<p><i>Contrôles des transmissions des données</i></p>	<ul style="list-style-type: none"> • Application de certains contrôles des entrées afin de valider les données reçues (p. ex. principaux champs, vraisemblance, etc.). 	<ul style="list-style-type: none"> • Tester des échantillons pour chaque scénario. • Observer les tentatives d'entrer des données incorrectes. • Déterminer qui peut passer outre les contrôles. • S'ils sont gérés par tables, déterminer qui peut modifier les éditions et les niveaux de tolérance.

b. Contrôles du traitement

Ces contrôles sont conçus pour apporter une assurance raisonnable que le traitement des données s'est déroulé comme prévu, sans omission ni double décompte. Les

contrôles du traitement sont en grande partie les mêmes que les contrôles des entrées, particulièrement pour les systèmes de traitement en ligne, ou en temps réel, mais sont appliqués pendant les phases de traitement. Ces contrôles sont les totaux intermédiaires, les rapports des totaux de contrôle, les contrôles des fichiers et des opérateurs, tels que les labels externes et internes, les journaux système des opérations informatiques et les tests de vraisemblance.

Contrôles du traitement		
<i>Ces contrôles permettent de vérifier que les données d'entrée valides ont été traitées exactement et complètement.</i>		
Domaine	Contrôle	Tests possibles
<i>Identification et validation automatique des fichiers</i>	<ul style="list-style-type: none"> • <i>Les fichiers à traiter existent et sont complets.</i> 	<ul style="list-style-type: none"> • <i>Examiner le processus de validation et le fonctionnement du test.</i>
<i>Fonctionnalité automatique et calculs</i>	<ul style="list-style-type: none"> • <i>Calculs spécifiques effectués sur une ou plusieurs entrées et éléments de données stockés qui produisent d'autres éléments de données.</i> • <i>Utilisation des tables de données existantes (p. ex. fichiers maîtres ou données de référence telles que les barèmes).</i> 	<ul style="list-style-type: none"> • <i>Comparer les valeurs d'entrée et de sortie pour tous les scénarios par cheminement et re-exécution.</i> • <i>Examiner les contrôles de la maintenance des tables et déterminer qui peut modifier les éditions et les niveaux de tolérance.</i>
<i>Pistes d'audit et contournements / Overrides</i>	<ul style="list-style-type: none"> • <i>Suivi automatisé des changements apportés aux données, attribuant le changement à un utilisateur précis.</i> • <i>Suivi automatisé et mise en évidence des contournements des procédures normales.</i> 	<ul style="list-style-type: none"> • <i>Examiner les rapports et les preuves des vérifications.</i> • <i>Examiner les droits de contourner les procédures normales.</i>

<p><i>Extraction, filtrage et communication des données</i></p>	<ul style="list-style-type: none"> • <i>La vraisemblance et l'exhaustivité des sorties des routines d'extraction sont contrôlées.</i> • <i>Allocation automatisée des transactions (p. ex. à des fins de réassurance, d'autres processus actuariels ou l'allocation des fonds).</i> • <i>Évaluation des données utilisées pour procéder aux estimations à des fins de communication financière.</i> 	<ul style="list-style-type: none"> • <i>Examiner la conception de la routine d'extraction par rapport aux fichiers de données utilisés.</i> • <i>Examiner l'évaluation par les superviseurs du résultat de la routine d'extraction pour vérifier qu'un examen régulier est effectué et s'il existe des problèmes.</i> • <i>Examiner le bien-fondé d'un échantillon d'allocations.</i> • <i>Examiner le processus d'évaluation de l'exhaustivité et de la validité des données extraites.</i>
<p><i>Équilibre à l'interface</i></p>	<ul style="list-style-type: none"> • <i>Vérification automatique des données reçues depuis les systèmes en amont (p. ex. données sur les paies, les créances, etc.) par les entrepôts de données ou les grands livres.</i> • <i>Vérification automatique de la correspondance entre les soldes des deux systèmes. En cas de non-correspondance, un rapport d'exception est généré et utilisé.</i> 	<ul style="list-style-type: none"> • <i>Inspecter les rapports d'erreur à l'interface.</i> • <i>Inspecter les paramètres et les réglages de la validité et de l'exhaustivité.</i> • <i>Examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les interfaces.</i> • <i>Examiner les preuves des rapports de correspondance, des vérifications et du traitement des fichiers contenant des erreurs.</i>
<p><i>Fonctionnalité automatique et classement chronologique</i></p>	<ul style="list-style-type: none"> • <i>Extraits de fichiers des listes de débiteurs afin de procurer à la direction des données sur les transactions par ordre chronologique.</i> 	<ul style="list-style-type: none"> • <i>Tester des échantillons de transactions sur ces listes afin de valider le bien-fondé du processus de classement chronologique.</i>
<p><i>Contrôles des doublons</i></p>	<ul style="list-style-type: none"> • <i>Comparaison de chaque transaction aux transactions précédemment enregistrées afin de mettre les champs en correspondance.</i> • <i>Comparaison de chaque fichier avec les dates, heures, tailles... attendus.</i> 	<ul style="list-style-type: none"> • <i>Examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les transactions ou les fichiers dupliqués.</i> • <i>Examiner le processus de manipulation des fichiers ou des transactions rejetés.</i>

c. Contrôles des sorties

Ces contrôles sont conçus pour apporter une assurance raisonnable que les résultats du traitement sont exacts, et diffusés exclusivement au personnel habilité. Il convient de comparer et de rapprocher les totaux de contrôle sortis pendant le traitement, aux totaux de contrôle d'entrée et intermédiaires produits en cours de traitement. Il convient de comparer les rapports de modification générés par ordinateur pour les fichiers maîtres, aux documents sources originaux afin de vérifier que l'information est correcte.

Contrôles des sorties		
<i>Ces contrôles permettent de vérifier que les données de sortie sont complètes, exactes et diffusées à qui de droit.</i>		
Domaine	Contrôle	Tests possibles
<i>Report dans le grand livre général</i>	<i>• Tous les reports des transactions individuelles et synthétisées dans le grand livre.</i>	<i>• Remonter jusqu'au grand livre général un échantillon de transactions synthétisées d'entrée et du grand livre auxiliaire.</i>
<i>Report dans le grand livre auxiliaire</i>	<i>• Tous les reports de transactions réussis dans le grand livre auxiliaire.</i>	<i>• Remonter jusqu'au grand livre auxiliaire un échantillon de transactions d'entrée.</i>

Contrôles des fichiers maîtres et des données de référence		
<i>Ces contrôles permettent de vérifier l'intégrité et l'exactitude des fichiers maîtres et des données permanentes.</i>		
Domaine	Contrôle	Tests possibles
<i>Autorisation des mises à jour</i>	<i>• Droits d'accès aux mises à jour attribués aux utilisateurs seniors sur la base de leurs rôles et de leur besoin d'utiliser l'application.</i>	<i>• Examiner les droits d'accès au réglage et à la modification des fichiers maîtres et des données de référence.</i>

VII. Les normes internationales de références

Les cadres de référence Contrôle interne et management des risques de l'entreprise du Committee of Sponsoring Organizations of the Treadway Commission (COSO) constituent des sources d'information fréquemment consultées, mais ils ne sont pas spécifiquement axés sur les SI. L'environnement de contrôle reposant sur le COSO devrait être complété par des objectifs de contrôle des SI plus détaillés, qui permettront d'évaluer plus efficacement l'environnement de contrôle des SI.

Il existe un certain nombre de possibilités à cet égard, les normes citées ci-après peuvent être prises en considération :

1. Le CobiT (Control Objectives for Information and related Technology)

Initialement publié en 1994 par l'ISACA (Information Systems Audit and Control Association), le CobiT est l'un des référentiels de contrôle et de gouvernance des SI couramment utilisés.

La version 5.0 du CobiT a été publiée en décembre 2013. Le CobiT n'a pas pour vocation de concurrencer le COSO ou d'autres référentiels, il peut être utilisé pour les compléter en les enrichissant avec des objectifs de contrôle des SI plus ciblés.

Un référentiel comme le CobiT propose une série d'objectifs de contrôle des SI communément admis, qui aide l'auditeur à concevoir une politique d'évaluation et de gestion des risques liés aux SI.

2. ISO 27001 – ISO 27001

L'Organisation internationale de normalisation (ISO) a édité une norme générique sur la sécurité des SI reconnue à l'échelle internationale. Il s'agissait au départ d'une norme britannique (BS 7799), qui a été transformée en norme ISO et qui est désormais connue sous l'appellation ISO 27001 - Techniques de sécurité – Systèmes de gestion de la sécurité de l'information.

Elle présente les bonnes pratiques communément admises concernant la gestion de la sécurité des SI et constitue un document de référence utile à partir duquel les auditeurs des SI peuvent mener à bien leurs missions.

<http://www.iso.org>

3. ISSAI 5310 – Directives sur le contrôle de la sécurité du système d'information - Seulement en anglais (Information System Security Review Methodology)

Les directives sur le contrôle de la sécurité du système d'information (SSI) sont rédigées en 3 volumes :

- Le Volume 1 propose aux instituts supérieurs de contrôle (ISC) une méthode de révision facile et manuelle du système d'information, en particulier lorsque les ressources sont limitées ou si un contrôle plus détaillé n'est pas nécessaire.*
- Le Volume 2 est une méthode plus sophistiquée fondée sur la valeur monétaire des risques auxquels sont exposés les systèmes d'information. Elle adopte une perspective allant « du sommet vers la base » en ce qui concerne l'information et de ce qu'elle représente en termes de valeur pour l'institution, les risques, les risques de sécurité et elle formule des recommandations.*
- Le Volume 3 montre des méthodologies détaillées pour assurer la sécurité du système d'information. Elles tentent de mesurer l'impact monétaire net des risques de sécurité et des contre-mesures mises en place.*

4. Manuel de vérification informatique 2014 WGITA IDI

Le manuel de vérification informatique (IT Audit Handbook) est établi par le INTOSAI Working Group on IT Audit (WGITA) et le INTOSAI Development Initiative (IDI), il a pour objectif essentiel d'aider l'auditeur à planifier et à effectuer des audits informatiques.

Il fournit un outil de travail adapté aux ISC qui suit les principes généraux d'audit énoncés dans les Normes internationales des Institutions Supérieures de Contrôle des finances publiques (ISSAI). Il peut compléter les cadres de référence prévus dans les autres modèles tels que le modèle ISACA CobiT, celui de l'Organisation internationale de normalisation (ISO) ou des normes, des guides et des manuels de certaines ISC.

Un outil a été élaboré par M. Cardoso dans le cadre de l'activité A.2.2.4. Il est basé sur le « IT Audit Handbook » et utilise l'environnement de Excel : à partir d'un questionnaire basé sur l'évaluation des risques, cet outil propose des tests à réaliser par les auditeurs. L'outil a été remis par M. Cardoso aux membres du groupe de travail de la Cour des comptes algérienne.

Annexes

Annexe 1. Fiche d'audit détaillée relative à la prise de connaissance de l'informatique de l'entité

Préambule

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 (Direction des systèmes d'information) avec les enjeux de l'entité.

Les documents à demander sont :

- L'organigramme de la structure en charge des systèmes d'information ;*
- Les fiches de fonctions des différents responsables des systèmes d'information ;*
- Les informations ayant trait aux objectifs, politiques et orientations en matière de systèmes d'information et d'informatique ;*
- Les plans informatiques et schémas directeurs ;*
- L'architecture et la cartographie des systèmes d'information ;*
- La liste des équipements informatiques (matériels, logiciels, applications ;*
- La charte informatique ;*
- Les procédures et politiques de sécurité informatique ;*
- Budget informatique des trois dernières années, ainsi que les budgets prévisionnels ;*
- Une communication des projets en cours ou prévus ;*
- Contrats conclus avec les opérateurs téléphoniques et les fournisseurs d'accès à Internet.*

Les personnes à rencontrer dans le cadre de l'audit de l'organisation informatique et systèmes d'information sont :

- La direction de l'entité auditée ;*
- Les responsables informatique et système d'information de l'organisation auditée ;*

- *Un échantillon représentatif des utilisateurs et gestionnaires concernés (utilisateurs clés représentatifs).*



Audit des systèmes d'information	Fiche n° : 1
Prise en compte de l'environnement informatique	Version : 1.0 Approuvé le : Novembre 2016 Par :

Question déterminante

	Réponses	Incidence sur la fiabilité du système d'information			Notation (sur 3)	Commentaires
		F	M	E		
1. Rôle et positionnement de l'informatique dans l'entité					2,08	
Quelle est la structure organisationnelle de la Direction des systèmes d'information (DSI) de l'entité ?		X			1	
A qui est rattachée la DSI ? Est-elle rattachée à la Direction générale ? (Évaluer le degré d'implication et de maîtrise de la DG dans les systèmes d'information de l'entité).				X	3	
Existe-t-il des Comités «informatique» (stratégique, pilotage...) regroupant les différentes directions de l'entité en charge de recenser les besoins et les opportunités, gérer les priorités et suivre les projets, évaluer le rôle et le poids de ces comités.						
2. Organisation et structure de la DSI					2,33	
Vérifier l'existence d'une charte informatique ou de tout autre document définissant le rôle et le périmètre de responsabilité de la DSI.						
Si ce document n'existe pas, expliquer comment est défini le champ d'intervention de la DSI.			X		2	
Décrire brièvement les responsabilités, missions et attributions à la DSI.						
Vérifier l'existence d'un organigramme à jour de la DSI.						
Existe-t-il une définition des fonctions et des responsabilités						

pour chaque poste figurant sur l'organigramme ?						
Vérifier que l'ensemble des composantes d'une fonction informatique (exploitation, la veille technologique, la sécurité informatique, le support utilisateurs, l'administration des serveurs...) est convenablement défini dans la charte informatique.						
Quel est l'effectif alloué à la DSI ?						
Cet effectif vous paraît-il suffisant eu égard aux enjeux de l'informatique dans l'entité ? (adéquation des effectifs aux besoins et aux enjeux).				X	3	
Le personnel de la DSI possède-t-il les compétences techniques requises ?						
Évaluer le caractère « raisonnable » du turn-over de la DSI (5 à 15% / an) et évaluer la stabilité de l'équipe.						
L'entité a-t-elle recours aux prestataires informatiques ? (nombre de prestataires, degré de dépendance vis-à-vis des prestataires, fonctions exercées).						
Évaluer la dépendance de l'entité vis-à-vis d'une ou plusieurs personnes.			X		2	
Les informaticiens sont-ils dispensés de préavis en cas de rupture brutale du contrat de travail?						
Existe-t-il un plan de formation nominatif pour l'ensemble des informaticiens ?						
L'effort de formation est-il adapté, suffisant et s'inscrit-il dans la durée?						
Existe-t-il des documentations utilisateurs et de gestion des différentes applications informatiques ? Sont-elles diffusées ?						

3. Planification stratégique						
Prendre connaissance du schéma directeur de l'entité et analyser le plan informatique et la feuille de route du SI (analyse de la pertinence du plan et de son alignement stratégique ; analyse de l'adéquation des compétences et des ressources aux objectifs du plan).						
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).						
Décrire (succinctement) et analyser les objectifs à court et moyen terme.						
4. Budgets et coûts informatiques						
Prendre connaissance du budget, est-il suffisamment détaillé ?						
Comprend-il les budgets acquisitions de matériels et logiciels ?						
Comprend-il les budgets de maintenance informatique ?						
Établir des ratios et des éléments de comparaison (ratio coûts/CA, ratio budget informatique/budget global).						
5. Cadre législatif et réglementaire						
Les exigences légales et réglementaires en vigueur sont-elles documentées au niveau de l'entité ? (décret 09-110 du 7 avril 2009).						
Certification du système d'information par un organisme externe (décret XXX).						
Respect de la confidentialité des données.						

6. Importance de l'informatique dans l'entité						
Quel est le degré d'incidence de l'informatique sur la production des informations comptables et financières ? (fort, moyen, faible ou inexistant) ?						
Décrire l'architecture fonctionnelle des systèmes d'information.						
Quels sont les domaines d'activité couverts par l'informatique ?						
Quel est le degré d'automatisation ?						
Quels sont les traitements automatisés ? nombre de traitements automatisés ?						
Quels sont les traitements non automatisés ? (les procédures et les règles de gestion sont-elles formalisées).						
Taille des systèmes, nombre d'opérations traitées.						
Quelles sont les caractéristiques du système d'information (besoins de l'activité, volume de transactions important, utilisation importante de technologies (échanges de données dématérialisés, Internet), exploitation en temps réel, génération automatique d'opérations...).						
Quel est le temps d'indisponibilité maximale tolérable ? (estimation)						
Quels sont les impacts et conséquences (opérationnelles et financières) d'une interruption du SI au-delà de la durée maximale tolérable.						



Fiche audit - Prise
connaissance environ

Annexe 2. Fiche d'audit relative à la cartographie des applications

Travail à réaliser

Liste des applications

Application	Utilisateur	Fonctionnalités	Hébergement (lieu si hébergement en propre et/ou nom du tiers si applicable)	Hébergement (Local, externalisé)	Type 1-Développ-ements internes 2- Développ-ements par un tiers 3- Progiciel 4- Fichier bureautique	Date de mise en place	Prestataire pour la maintenance	Date de fin d'utilisation prévue (si applicable, sinon laisser la case vide)	Date de la dernière modification	OS du serveur hébergeant l'application	Base de données	Projet d'évolution	Nature des sorties	Volume traité	Criticité (1 à 5)
<i>Exemple</i>															
FINANCE +	Contrôle de Gestion	Comptabilité générale Comptabilité analytique	Salle Serveur	Local	Progiciel	11/04/2001	XX Informatique	31/10/2016		Windows Server 2003	SQL Server	Montée de version en v8.2 en janvier 2013	Établissement des comptes	500 enregistrements par jour	1
Applications financières critiques															
Autres applications significatives															

Liste des principales interfaces internes et externes

ID	Source	Destination	Type de flux	Protocole	Périodicité	Déclenchement	Données échangées	Contrôles



Fiche audit -
Cartographie des ap

Annexe 3. Fiche d'audit relative à l'identification des processus à analyser

Travaux à réaliser

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

Selon l'importance du rôle joué par les applications et les interfaces dans chaque processus, l'équipe de contrôle sélectionne le ou les processus à analyser. La première étape prévoit une revue du concept de la procédure (test de design) permettant de vérifier la cohérence du processus avec la couverture des risques.

Suite à la revue du concept, l'auditeur pourra effectuer les contrôles de réalité et d'efficacité de l'application du processus.

Résultat

Le résultat peut être formalisé sous forme du tableau suivant :

	<i>Appli. 1</i>	<i>Appli. 2</i>	<i>Appli. 3</i>	<i>Appli. 4</i>	<i>Appli. 5</i>	<i>Appli. 6</i>	<i>Appli. 7</i>	<i>Appli. 8</i>
<i>Processus 1</i>	X	X				X		
<i>Processus 2</i>			X	X	X			
<i>Processus 3</i>		X	X	X				
...	X				X	X		

Annexe 4. Fiche d'audit détaillée relative à la sécurité informatique



Audit des systèmes d'information	Fiche n° : 1
Prise en compte de l'environnement informatique	Version : 1.0 Approuvé le : novembre 2016

Question déterminante

	Réponses	Incidence sur la fiabilité du système d'information			Notation	Commentaires
		F	M	E		
POLITIQUE DE SÉCURITÉ AU NIVEAU DE L'ENTITÉ						
<i>La politique de sécurité informatique (physique et logique) est-elle formalisée au niveau de l'organisation ?</i>						
<i>La structure en charge de l'informatique et des systèmes d'information a-t-elle élaboré un document officiel ou charte sur la sécurité qui décline cette politique en actions et procédures concrètes ?</i>						
<i>La communication de la charte sur la sécurité se fait à tous les utilisateurs</i>						
<i>Il existe un service dédié à la gestion de la sécurité de l'information : un comité, un responsable de la sécurité du système d'information</i>						
<i>Il existe des procédures d'autorisation de nouveaux matériels ou logiciels.</i>						
SÉCURITÉ PHYSIQUE						
Accès à la salle informatique						
<i>Il existe une salle informatique dédiée</i>						
<i>Les portes des locaux informatiques sont maintenues verrouillées</i>						
<i>Il existe un dispositif de détection des intrusions (alarmes, caméra...)</i>						
<i>Seules les personnes autorisées accèdent à ces locaux</i>						
<i>Il existe une gestion des visiteurs (personnes autorisées temporairement à accéder aux locaux informatiques) assurant la traçabilité des entrées/sorties</i>						
<i>Toutes les entrées et sorties sont enregistrées</i>						
<i>Les heures d'accès pour toutes les personnes sont réglementées</i>						
Dispositifs anti-incendie						
<i>Il existe au sein du local un dispositif de détection des fumées</i>						
<i>Il existe au sein du local un dispositif</i>						

<i>d'extraction des fumées</i>						
<i>Un extincteur en cours de validation est présent dans le local</i>						
<i>Le dispositif d'éradication du feu est à base de gaz. sont audités par des sociétés spécialisées et à intervalles régulier</i>						
Dispositifs contre les surtensions et coupures électriques						
<i>Il existe un dispositif de protection (serveurs et postes de travail) contre les surtensions et coupures électriques (onduleur)</i>						
<i>Des tests sont effectués régulièrement</i>						
Autres dispositions de sécurité						
<i>Les locaux sont tenus propres, aucun papier n'est présent près des serveurs</i>						
<i>Les locaux des serveurs sont ventilés et climatisés</i>						
<i>Il existe un dispositif de contrôle de l'hygrométrie</i>						
<i>Les serveurs ne sont pas posés à même le sol</i>						
<i>Les serveurs ne sont pas situés dans les locaux de l'entité, mais chez un prestataire extérieur certifié</i>						
<i>La salle informatique n'est pas localisée dans une zone présentant un risque potentiel d'inondation (sous-sol, local sous les toits, canalisations d'eau au-dessus des serveurs, etc.)</i>						
<i>Il existe un système d'évacuation des eaux dans le plancher de la salle informatique</i>						
SÉCURITÉ LOGIQUE						
Sécurité du réseau						
<i>Il existe une procédure définissant la sécurité du réseau (architecture technique, gestion des données sensibles et profils d'accès, gestion des utilisateurs: création, modification, suppression)</i>						
<i>La procédure est formalisée (écrite)</i>						
<i>Les accès au réseau sont sécurisés contre les intrusions extérieures : ex. : Internet par un Proxy, réseau local par firewall</i>						
<i>Les connexions à distance sont sécurisées (VPN, MPLS...)</i>						
<i>Les accès au réseau sont protégés par mots de passe</i>						
<i>Il n'existe pas de compte générique</i>						
<i>Le premier mot de passe est affecté individuellement à chaque utilisateur (mot de passe non connu)</i>						
<i>Le premier mot de passe doit être automatiquement modifié à la première connexion par l'utilisateur</i>						
<i>Les mots de passe font l'objet d'un renouvellement régulier</i>						

<i>L'utilisateur n'a pas le droit d'utiliser plusieurs fois de suite le même mot de passe</i>						
<i>Les mots de passe comportent au moins 8 caractères alphanumériques et caractères spéciaux</i>						
<i>Après plusieurs tentatives d'accès infructueuses, le compte de l'utilisateur est bloqué</i>						
<i>Il existe des profils pour chaque type d'utilisateur</i>						
<i>Une revue régulière des droits d'accès des utilisateurs est réalisée</i>						
<i>Après un délai donné d'inactivité, le poste se met en veille (déconnexion automatique et/ou protection par mot de passe)</i>						
<i>Les accès et les échanges WIFI sont cryptés</i>						
Sécurité des applications avec impact financier						
<i>Il existe une procédure de gestion des utilisateurs (profils utilisateurs, création, modification, suppression)</i>						
<i>La procédure est formalisée (écrite)</i>						
<i>Il existe un profil pour chaque utilisateur</i>						
<i>L'entité a mené une réflexion sur la séparation des fonctions et déduit des profils d'utilisateurs avec l'identification des droits associés formalisés dans un document approuvé par la direction</i>						
<i>Une revue régulière des droits d'accès des utilisateurs est réalisée</i>						
<i>Les accès aux applications sont protégés par mots de passe</i>						
<i>Il n'existe pas de compte générique</i>						
<i>Le premier mot de passe est affecté individuellement à chaque utilisateur (mot de passe non connu)</i>						
<i>Le premier mot de passe doit être automatiquement modifié à la première connexion par l'utilisateur</i>						
<i>Les mots de passe font l'objet d'un renouvellement régulier</i>						
<i>L'utilisateur n'a pas le droit d'utiliser plusieurs fois de suite le même mot de passe</i>						
<i>Les mots de passe comportent au moins 8 caractères alphanumériques</i>						
<i>Après plusieurs tentatives d'accès infructueuses, le compte de l'utilisateur est bloqué</i>						
Autres						
<i>Les postes et les serveurs sont équipés d'antivirus</i>						
<i>Les logiciels antivirus sont présents et mis à jour régulièrement</i>						
<i>Le système d'exploitation (Windows, autres...) est à jour</i>						
<i>La détection des virus s'effectue sur tous les types de fichiers (programmes,</i>						

<i>fichiers système et documents)</i>						
<i>Les logiciels antivirus sont activés sur tous les postes et ne peuvent être déconnectés par l'utilisateur</i>						
<i>Les messages et les pièces jointes font également l'objet de décontamination</i>						
<i>Il existe un système anti-spam</i>						
Gestion des sauvegardes						
<i>Il existe une procédure définissant la gestion des sauvegardes</i>						
<i>La procédure est formalisée (écrite)</i>						
<i>La procédure indique le type de données sauvegardées</i>						
<i>La stratégie de sauvegarde permet-elle de garantir une perte limitée de données supportable par l'entité?</i>						
<i>Les serveurs sont équipés de dispositifs de sauvegarde ou utilisent un moyen de sauvegarde mutualisé</i>						
<i>Les sauvegardes sont automatisées (au moins une fois tous les 24h)</i>						
<i>Les rapports sont contrôlés systématiquement</i>						
<i>Les sauvegardes sont conservées suffisamment longtemps et assurent une perte de données limitée</i>						
<i>Il existe une procédure de sauvegarde pour les ordinateurs portables</i>						
<i>Un jeu de sauvegarde est conservé à l'extérieur de l'entité</i>						
<i>L'usure des bandes est vérifiée, les bandes sont changées le cas échéant</i>						
<i>Il existe un classement et un référencement des supports de sauvegarde</i>						
<i>Des tests de restauration complets sont effectués régulièrement</i>						
<i>Les tests de restauration intègrent les utilisateurs métiers</i>						
<i>Tous les incidents de sauvegarde sont documentés</i>						
<i>Les sauvegardes sont conservées dans un endroit protégé (type coffre ignifugé)</i>						
<i>Le lieu de stockage des sauvegardes (bandes, disque dur, etc.) est extérieur au local des serveurs</i>						
<i>En cas d'externalisation des sauvegardes, le contrat a défini l'engagement du prestataire sur chacun des points précédents (Plan de sauvegarde, nombre et cycle de vie des générations, sécurité physique des supports, procédures de restaurations, procédure d'actualisation du plan de sauvegarde, procédure de reporting)</i>						
<i>En cas d'externalisation, les applications et/ou serveurs critiques ont fait l'objet de tests de restauration complète sur un nouveau matériel dans le cadre d'une procédure standard</i>						

PLAN DE SECOURS						
<i>Il existe un plan de secours défini et formalisé</i>						
<i>Un matériel de secours est prévu</i>						
<i>Un site de secours est prévu</i>						
<i>Un test du plan de secours est réalisé au minimum annuellement</i>						
<i>Un compte rendu des tests est formalisé</i>						
<i>L'entité dispose d'un contrat de maintenance sur les serveurs</i>						
CONTRÔLE INTERNE DE LA FONCTION INFORMATIQUE						
<i>Les principes de séparation des fonctions sont respectés au sein du service informatique (Fonctions Back Office (développement) et Front Office (exploitation) séparées)</i>						
<i>Séparation du service informatique avec les opérationnels</i>						
<i>Les expertises sont partagées et documentées au sein du service des systèmes d'information</i>						
<i>Il existe un plan de formation spécifique pour le service informatique</i>						
<i>Il existe une procédure de gestion des incidents</i>						
<i>La procédure est formalisée (écrite)</i>						
<i>Les incidents sont tracés, analysés, corrigés et leur résolution est suivie</i>						
<i>Il existe une charte informatique signée par les utilisateurs, validée juridiquement et annexée au règlement intérieur</i>						
<i>La charte informatique définit les règles d'utilisation du SI (applications, données), des postes de travail et/ou des serveurs, du courrier électronique, de l'Internet.</i>						
GESTION DES CHANGEMENTS						
<i>Il existe une procédure de gestion des évolutions</i>						
<i>La procédure est formalisée (écrite)</i>						
<i>La procédure prévoit le cas particulier de la montée en version des applications et/ou des logiciels de base qui doivent être gérés comme un projet</i>						
<i>Les demandes d'évolutions fonctionnelles sont validées par le management</i>						
<i>Les demandes et les développements sont documentés</i>						
<i>Il existe un plan de test de non-régression pour les évolutions (y compris les montées en version des applications)</i>						
<i>Les jeux et comptes rendus de test sont réalisés par le demandeur (utilisateur pilote) et validés pas le demandeur avant</i>						

<i>la mise en production</i>						
<i>Il existe une procédure définie pour les changements en urgence</i>						
<i>La création des profils suit le processus de gestion des changements</i>						
<i>Il existe une séparation de fonctions entre les environnements de production et de développement en termes d'accès logique</i>						



Fiche audit - sécurité
informatique.xlsx

Annexe 5. Fiche d'audit relative au projet informatique



Audit des systèmes d'information	Fiche n° : 1
Audit des projets informatiques	Version : 1.0 Approuvé le : Novembre 2016

		<i>Commentaires</i>
<i>Objectifs et enjeux du projet</i>		
<i>Étude d'opportunité et expression des besoins</i>		
<i>Planification</i>		
<i>Les instances de pilotage</i>		
<i>Méthode et outils</i>		
<i>Conception</i>		
<i>Développement, réalisation ou paramétrage</i>		
<i>Tests et recettes</i>		
<i>Conduite du changement et mise en œuvre</i>		
<i>Documentation</i>		

Annexe 6. Dictionnaire des expressions spécifiques

Ces définitions rapides doivent permettre aux auditeurs de vérifier qu'ils partagent avec les audités une même compréhension de certaines notions spécifiques et complexes.

A. Dictionnaire des expressions spécifiques des SI

a. 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.

b. Schéma directeur et Plan stratégique 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.

c. Maîtrise d'ouvrage (MOA) et maîtrise d'œuvre (MOE)

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 nationale) 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.*

d. Propriétaire (Business owner) d'une application ou de données

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 données, 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.

e. Base de données maîtresse

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.

f. Politique de sécurité

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.

g. 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 paramètres 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.*

h. 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.

i. 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.

j. Plan de continuité de l'activité et plan de reprise de l'activité

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).

k. Infogérance 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.

1. 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'utilisateur 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'utilisateur des machines virtuelles et leur environnement informatique d'exploitation dont l'utilisateur n'a plus à assurer le fonctionnement. L'utilisateur 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.

m. 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.

n. 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.

Annexe 7. Types de contrôles liés aux applications

On distingue les types de contrôles applicatifs suivants :

- 1. Création et autorisation*
- 2. Saisie et enregistrement des données*
- 3. Traitement des données*
- 4. Sortie des données (Output)*
- 5. Interfaces*

1. Création et autorisation

Les principaux objectifs relatifs à la création et à l'autorisation sont les suivants:

- minimiser les erreurs et les omissions ;*
- identifier, documenter, communiquer et corriger les erreurs et les irrégularités dès leur apparition ;*
- vérifier l'exactitude de la correction des erreurs par un service / une personne indépendante ;*
- les opérations commerciales (transactions) ne sont effectuées que par des personnes habilitées et/ou selon des procédures autorisées ;*
- les personnes responsables de la saisie des transactions commerciales sont identifiées dans le système ;*
- les justificatifs de saisie délivrés sont exhaustifs et exacts et sont transmis en temps utile ;*
- les justificatifs de saisie sont conservés pendant la période légale et sous la forme prescrite ou peuvent être reconstitués par l'organisation ;*
- Les contrôles typiques concernant la création et l'autorisation sont les suivants :*
 - profils des compétences pour l'établissement de pièces comptables (par ex. règlement sur les signatures) et mise en œuvre à travers un contrôle des autorisations par des systèmes de gestion des accès ;*

- *séparation des fonctions de création et de validation de pièces comptables ;*
- *visa ou signature sur les justificatifs de saisie ;*
- *formulaire de saisie compréhensibles et utiles (par ex. avec des champs préimprimés) ;*
- *processus d'identification précoce et de traitement des erreurs et des irrégularités ;*
- *collecte systématique des pièces comptables (par ex. dans l'ordre chronologique à l'aide d'un horodateur ou séquentiellement à l'aide d'un système de numérotation continue) ;*
- *micro filmage ou numérisation des justificatifs et conservation sur un support permettant de reconstruire les informations originales dans les délais requis.*

2. Saisie et enregistrement des données

Les principaux objectifs de la saisie et de l'enregistrement des données sont les suivants :

- *seules des personnes habilitées (ou les processus autorisés) peuvent enregistrer des données ;*
- *l'exactitude, l'exhaustivité et la validité des champs importants (par ex. numéros de compte, montants, code article) sont contrôlées dans les écrans ou programmes en amont du processus de saisie ;*
- *les erreurs et les anomalies de saisie / d'enregistrement sont identifiées, documentées, communiquées et corrigées en temps utile ;*
- *l'exactitude de la correction des erreurs est vérifiée par un service / une personne indépendante.*

Les contrôles typiques de saisie et d'enregistrement des données sont les suivants :

- *profils des compétences pour la saisie / enregistrement des transactions et mise en œuvre à travers un contrôle des autorisations par des systèmes de gestion des accès ;*

- *masques de saisie compréhensibles et conviviaux avec des contrôles de format de données intégrés (par ex. champs de date, données numériques, champs obligatoires, etc., et liste de valeurs prédéfinies et récurrentes) ;*
- *contrôle automatique approfondi des valeurs saisies (par ex. dépassements de valeurs limites, contrôle de plausibilité des contenus, synchronisation avec les données enregistrées) ;*
- *affichage des libellés de code complets après saisie du code (par ex. la désignation d'un article s'affiche à la saisie du numéro d'article) ;*
- *comparaison des données saisies, c'est-à-dire comparaison des données à saisir avec les données visibles à l'écran ou avec des journaux de saisie (compte tenu du coût, judicieux uniquement pour les transactions critiques telles que les mutations de données de base notamment) ;*
- *totaux de contrôle par lots: nombre de documents (ex nombre de factures), somme de zones de valeurs figurant sur les documents ou sommes numériques (montants, quantités), somme de contrôle (condensat, hash, addition mathématique de numéros de documents, numéros de compte) ;*
- *contrôle de l'ordre d'apparition des pièces comptables numérotées en continu au sein d'un lot pour identifier les numéros manquants ou les doublons de saisies ;*
- *comparaison des données saisies avec les valeurs enregistrées (par ex. postes ouverts avec des opérations comptables nouvellement créées) ;*
- *saisie de contrôle (appelée également double saisie, contrôle des 4 yeux); saisie à double de valeurs importantes par différentes personnes (géré par le système de gestion des accès) ou le cas échéant, par une seule et même personne (par ex. lors de la saisie masquée d'un nouveau mot de passe) ;*
- *contrôle visuel des valeurs saisies généralement par une deuxième personne ; convient pour les cas critiques et un petit nombre de transactions ;*
- *processus d'identification précoce et de traitement d'erreurs et d'anomalies, les transactions corrigées devant être à nouveaux entièrement vérifiées.*

3. Traitement des données

Les principaux objectifs du traitement des données sont les suivants :

- l'exhaustivité, l'exactitude et la validité des traitements réalisés sont vérifiées selon une procédure de routine; les erreurs de traitement sont identifiées au plus tôt, documentées et corrigées en temps utile ;*
- la correction de transactions erronées se déroule sans entraver inutilement le traitement des autres transactions ;*
- les calculs, totalisations, consolidations, analyses et affectations sont effectués correctement par le programme ;*
- la séparation des fonctions est assurée y compris pendant le traitement des données ;*
- les transactions générées automatiquement par l'application (par ex. intérêts sur crédit périodiques, commandes en cas de dépassement du seuil de sécurité des stocks) font l'objet des mêmes contrôles d'exhaustivité, d'exactitude et de validité que les transactions isolées ;*
- les décisions importantes reposant sur des calculs automatiques sont prises et vérifiées par des personnes ;*

Les contrôles typiques du traitement des données sont les suivants :

- un grand nombre des contrôles décrits précédemment pour la saisie et la création de données peuvent être appliqués pour le traitement (par ex. comparaison des champs individuels, totaux de contrôle par lots, contrôle de l'ordre d'apparition et comparaison de données, synchronisation automatique du grand livre et des livres auxiliaires). Il est cependant important que les documents et les totaux utilisés pour les contrôles correspondent aux résultats de fin de traitement ;*
- rapprochement des données traitées dans le système avec des confirmations externes (par ex. inventaires, confirmations de soldes bancaires et de soldes de comptes) ;*
- garantie de l'intégrité du traitement grâce aux quatre objectifs de processus supérieurs : atomicité (unité de travail non divisible, toutes les actions s'y rapportant sont effectuées avec succès ou aucune d'entre elles ne l'est), consistance (lorsque la transaction n'atteint aucun statut final stable, elle doit être réinitialisée dans le système), isolation (le comportement d'une transaction*

n'est pas influencé par d'autres transactions effectuées simultanément) et durabilité (à l'issue d'une transaction, ses conséquences restent durables, y compris les changements en cas de pannes de système). Ces contrôles sont souvent implémentés hors des applications (par ex. dans des systèmes de base de données). Ceci doit toutefois être vérifié au cas par cas.

4. Sortie de données (output)

Les principaux objectifs de la sortie des données sont les suivants :

- *la sortie des données s'effectue en temps utile, au bon endroit et conformément aux procédures définies ;*
- *l'exhaustivité et l'exactitude des informations éditées sont garanties par des procédures effectuées de manière systématique sur des totaux de contrôle et un rapprochement avec les totaux de contrôle correspondant du traitement ;*
- *le traitement, la conservation et la destruction d'output sont conformes aux exigences de la protection des données et de sécurité (avant et après leur diffusion auprès des utilisateurs) ;*
- *les informations imprimées sont conservées conformément aux dispositions légales.*

Les contrôles typiques de la sortie des données sont les suivants :

- *les contrôles d'envoi et de réception règlent les modalités de communication des listes et autres outputs (qui, quand, quoi, comment et en combien d'exemplaires) ;*
- *les systèmes de gestion des accès garantissent la traçabilité des accès des utilisateurs lors de consultations à l'écran ou de commandes de listes en ligne ;*
- *les contrôles de numérotation et d'exhaustivité garantissent que la gestion, l'édition, la restitution, la réception et la destruction (par ex. en cas de copie de contrôle) d'outputs critiques (par ex. chèques, bons, obligations de caisse, etc.) s'effectuent conformément aux procédures ;*
- *l'exactitude et l'exhaustivité des impressions périodiques (par ex. traitement semestriel et annuel) sont contrôlées au moyen des contrôles par échantillonnage.*

5. Les interfaces

Les principaux objectifs relatifs aux interfaces sont les suivants :

- *l'authenticité et l'intégrité des informations provenant de sources externes à l'organisation sont contrôlées soigneusement avant d'entreprendre toute action potentiellement critique, indépendamment du moyen de réception (téléphone, voicemail, papier, fax, e-mail, ou fichier) ;*
- *les informations sensibles sont protégées pendant leur transmission par des mesures appropriées contre les accès non autorisés, les modifications ou les adressages erronés ;*

Les contrôles typiques au niveau des interfaces sont les suivants :

- *un grand nombre des contrôles présentés précédemment pour la saisie et l'enregistrement des données peuvent également être utilisés pour le contrôle des interfaces (par ex. comparaison des positions individuelles, totaux de contrôle de lots, contrôle de numérotation et comparaison de données) ;*
- *authentification de chaque message à l'aide de procédures cryptographiques ;*
- *cryptage de chaque message (important) pour garantir :*
 - *la confidentialité du contenu ;*
 - *l'intégrité du contenu du message ;*
 - *l'identité de l'expéditeur.*