CIGREF

IFACI Institut de l'Audit Interne

Le contrôle interne du système d'information des organisations

Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne

SOMMAIRE

SOMMAIRE

SOMMAIRE

Remerciements

Le groupe de travail sur le **contrôle du SI de l'entreprise** a été piloté par Régis DELAYAT, DSI de SCOR. Nous tenons à remercier les personnes qui ont contribué à ces travaux :

- Samantha ANDRIAMAROHASY, DCNS
- Thierry BLANCHARD, La Banque Postale
- Carine CABALO, Groupe La Poste
- Philippe ELBAZ, Les Mousquetaires
- Jacques FASSEL, SCOR
- Jean FERRE, L'Oréal
- Jean-Claude HILLION, Banque de France
- Maher KAMAL-RIZK, SCOR
- Kacem MALTI, Rhodia
- Guy NICOLAS, Nexans
- Jean-Marie PIVARD, Nexans
- Christine SHIMODA, L'Oréal
- Isabelle TOURNASSOUD, EDF
- Jean-Brice TULASNE, St Gobain

Le groupe de travail sur le **contrôle interne de la DSI** a été piloté par Farid ARACTINGI, Directeur Audit et Management des Risques de Renault. Nous tenons à remercier les personnes qui ont contribué à ces travaux :

- Jean-Pierre BOUILLOT, Sanofi-Aventis,
- Gilles BRUNET, France Telecom
- Eric CORNAY, AXA
- Philippe ELBAZ, Les Mousquetaires
- Anne EMILIAN, Renault
- Gilbert FENEUIL, Total
- Annie GIRARD-LAOT, GDF Suez
- Henri GUIHEUX, SCOR
- Philippe HERVIAS, Sanofi-Aventis
- Jean-Marc HOSPITAL, Renault
- Alain ROGULSKI, Alcatel-Lucent
- Cyrille ROY, AGF
- Gérard VEDRENNE, Banque de France

L'étude a été coordonnée par Stéphane ROUHIER, chargé de mission au CIGREF et Béatrice KI-ZERBO, Directeur de la Recherche à l'IFACI et pilotée par Jean-François PEPIN, Délégué Général du CIGREF et Louis VAURS, Délégué Général de l'IFACI.

I. Préface

L'objectif de ce document CIGREF-IFACI est de sensibiliser les dirigeants aux enjeux du contrôle interne et de la maîtrise des systèmes d'information au sein des organisations, tant publiques que privées, tout en proposant aux managers des pistes opérationnelles (démarche, check lists, …).

Il résulte des travaux communs réalisés par le CIGREF et l'IFACI, dans le cadre de leur partenariat signé le 9 octobre 2007. Celui-ci a été décidé suite à l'élaboration début 2007 par un groupe de place d'un cadre de référence du contrôle interne, dont l'Autorité des Marchés Financiers (AMF) recommande l'utilisation.

Le système d'information est en effet devenu la colonne vertébrale d'une entreprise ou d'une administration moderne, dont il irrigue toutes les fonctions pour contribuer à la fois à leur efficacité opérationnelle et à leur transformation stratégique. Il est donc au cœur de tous les métiers, et embarque les éléments de standardisation, les besoins de spécificités et, les contrôles de sécurité et de performance. Dans une économie globalisée avec des processus de plus en plus complexes, il est devenu le garant de facto de la protection de l'information, de la sincérité des opérations, de la vitesse d'exécution et donc de l'excellence opérationnelle. Et, de simple pourvoyeur de systèmes et de technologies, la Direction des systèmes d'information a vu son rôle évoluer vers leur utilisation optimale par les métiers et les utilisateurs au service de la performance de l'entreprise.

Compte tenu de son rôle, la pertinence du contrôle interne du système d'information, c'est-à-dire sa bonne maîtrise, est un élément clé de succès des organisations. Rappelons que, selon le cadre de référence de l'AMF, un bon contrôle interne contribue à la maîtrise des activités d'une organisation, à l'efficacité de ses opérations, à l'utilisation efficiente de ses ressources, et doit lui permettre de prendre en compte de manière appropriée les risques significatifs. Le contrôle interne des systèmes d'information est donc un sujet prioritaire pour une organisation, et encore plus actuellement où l'économie mondiale subit une crise d'une rare intensité.

Dans ce contexte l'audit interne a, ces dix dernières années, renforcé continûment son positionnement et son rôle. Il est de plus en plus positionné comme partenaire des organes dirigeants pour évaluer les enjeux et les risques les plus importants et les plus complexes des organisations. Il évalue l'ensemble du système de contrôle interne et fournit des conseils précieux pour leur pilotage. Dans ce même esprit, le système d'information devient aussi un moyen du contrôle, puisqu'une mission d'audit sur un processus ou une filiale utilisera largement les données extraites des applications couvrant ce processus ou cette filiale.

Le système d'information, objet et moyen du contrôle interne de l'entreprise, est donc un sujet majeur sur lequel le CIGREF, association de Grandes Entreprises utilisatrices de système d'information et l'IFACI, association professionnelle de l'audit et du contrôle internes, ont décidé de collaborer, autour de deux thèmes : le contrôle du système d'information de l'entreprise et le contrôle interne de la Direction des systèmes d'information.

Les résultats sont très opérationnels et facilement adaptables aux caractéristiques propres à chaque organisation. Ils sont à prendre en compte dès la conception et le développement des applications et des systèmes. C'est un outil au service des auditeurs, des contrôleurs, des informaticiens, mais aussi des métiers, dont l'utilisation contribuera à l'amélioration de l'efficacité des dispositifs de contrôle interne et, fournira des réponses concrètes aux questions centrales posées par les organes de gouvernance.

Bruno Ménard
Président, CIGREF
Vice Président Systèmes d'Information, SANOFI-AVENTIS

Claude Viet
Président, IFACI
Directeur Audit Groupe, LA POSTE

2. Résumé

Le contrôle interne a acquis ces dernières années une dimension nouvelle, incontournable et consubstantielle à l'entreprise. **Le contrôle interne des organisations fait et fera de plus en plus partie du paysage des entreprises.**

Cinq grands principes peuvent se dégager :

- **C'est aux managers d'instaurer une culture et une dynamique du contrôle** par la mise en place d'une organisation appropriée et d'un système de management efficace (stratégie, politique, déploiement, ...).
- Le contrôle interne doit être **intégré dans les processus** de l'entreprise (achat, vente, production, consolidation, RH, …).
- **Les SI jouent un rôle clé** dans une bonne gouvernance d'entreprise et dans un dispositif efficace de contrôle interne. Ils sont non seulement un objet mais aussi un levier du contrôle interne des processus de l'entreprise.
- **Un principe de réalité, de proportionnalité et de granularité** doit s'appliquer dans tout dispositif de contrôle interne. Il convient de penser à arbitrer entre le coût et l'efficacité du dispositif.
- **Il faut enfin rester conscient du caractère non exhaustif, des limites intrinsèques** et des arbitrages nécessaires dans tout dispositif de contrôle.

Il est possible de formuler un certain nombre de recommandations selon une démarche PDCA (Plan Do Check Act) :

<u>Planifier</u>

- Etre clair sur la finalité, les objectifs et le périmètre du contrôle ;
- en prérequis, avoir cartographié les processus de l'entreprise et son patrimoine informationnel.

<u>Faire</u>

- Avoir une démarche de contrôle au « juste prix » ;
- **avoir une démarche de contrôle en partant des processus de l'entreprise, des risques associés et des points de contrôle ;**
- adapter la démarche à la culture et au modèle d'organisation de l'entreprise, ainsi qu'à la taille des entités contrôlées (filiales notamment) ;
- utiliser les référentiels existants (CobiT, ITIL, ISO 2700, …) ;
- coordonner les audits interne et externe ;
- travailler en étroite collaboration entre les différents acteurs « responsables » dans l'organisation : direction de l'audit interne, direction des systèmes d'information, direction des risques, direction juridique, direction de la sécurité, et fonctions de contrôle interne sans pour autant diluer les responsabilités ;
- s'appuyer sur la direction qualité et la démarche qualité quand elles existent ;
- intégrer la démarche de contrôle interne dans la construction des applications ou le pilotage du service informatique.

Vérifier

- Les failles se situent souvent aux frontières : il convient d'être attentif aux risques à la jonction de plusieurs processus ou lorsque les applications transversales sont sous la responsabilité partagée de plusieurs directions ;
- les points de contrôle applicatifs et automatiques ainsi que les points de contrôle non-applicatifs et manuels sont indispensables et complémentaires ;
- évaluer régulièrement l'efficacité des contrôles en place en fonction de l'évolution du SI et de l'entreprise ;
- arbitrer le coût de mise en place d'un contrôle avec les impacts du risque identifié.

Mettre à jour

- Exploiter les résultats des audits interne et externe et des revues ponctuelles des prestataires externes pour améliorer le système de management du contrôle interne ;
- assurer un processus continu de mise à jour de la cartographie des risques.

3. Introduction

3.1. Contexte

Le CIGREF[1] et l'IFACI[2] ont signé une charte[3] le 9 octobre 2007 visant à sensibiliser les dirigeants et à aider concrètement les praticiens sur les enjeux du contrôle interne et de la maîtrise des systèmes d'information au sein des organisations, tant publiques que privées.

Cette initiative fait suite à la publication début 2007 du cadre de référence de contrôle interne de l'AMF complété d'un guide d'application relatif à l'information comptable et financière.

Ce document précise qu'un dispositif de contrôle interne doit bénéficier de systèmes d'information adaptés aux objectifs actuels de l'organisation et capables de l'accompagner dans ses ambitions futures. La diffusion de bonnes pratiques dans ce domaine relève donc d'un impératif à la fois stratégique et opérationnel.

A cette fin, un groupe de travail commun aux deux associations professionnelles a été mis en place.

3.2. Publics cibles

Le document, coproduit par le CIGREF et l'IFACI, est destiné aux directeurs généraux, directeurs métiers, directeurs des systèmes d'information, directeurs d'audit interne, fonctions de contrôle interne, consultants et auditeurs externes, soucieux de la mise en œuvre et de l'efficacité d'un dispositif de contrôle interne.

3.3. Rappel des objectifs

L'objectif principal de ce document est le renforcement de l'efficacité du contrôle interne, en particulier :

1. Enrichir la dimension SI du cadre de référence de l'AMF et mieux le relier aux référentiels existants (CobiT, ITIL, ISO 2700x…).
2. Elaborer un guide d'application relatif au contrôle interne des systèmes d'information, incluant des listes de bonnes pratiques.
3. Aider la fonction SI et la fonction audit interne à mieux collaborer pour renforcer l'efficacité du contrôle interne de l'entreprise.

3.4. Périmètre retenu

Le CIGREF et l'IFACI ont cherché à avoir une approche sélective et réaliste des risques.

[1] *www.cigref.fr* - [2] *www.ifaci.com* - [3] *Cf. Annexe 1*

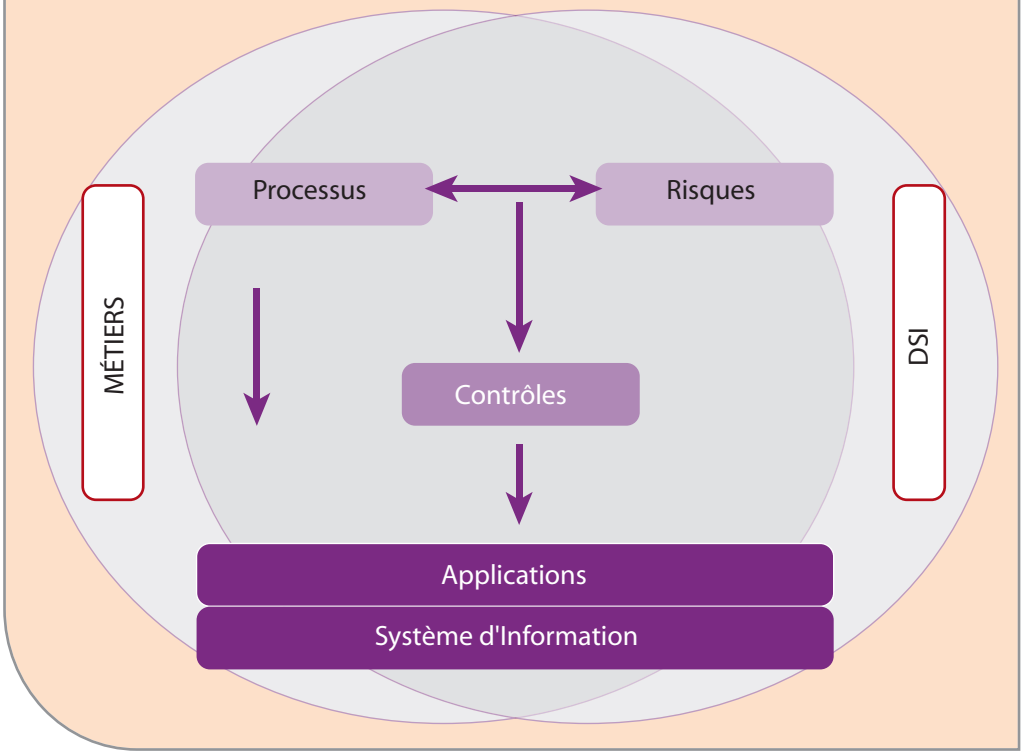
Le groupe de travail a retenu une approche structurée à partir des processus de l'entreprise, des risques associés, des objectifs et des points de contrôle.

Les équipes mobilisées ont fonctionné en deux sous-groupes mixtes, l'un traitant le **contrôle interne du SI de l'entreprise**, l'autre le **contrôle interne de la DSI.**

Les deux sujets donnent lieu à un guide opérationnel, dont la mise en œuvre devra être adaptée au contexte de chaque organisation, à l'initiative des propriétaires de processus.

Figure 1 : Démarche et périmètre du contrôle du SI de l'entreprise

Source : CIGREF - IFACI



3.5. Les livrables

- Une description des processus avec leurs principales étapes ;
- une description des acteurs et de leurs rôles (RACI) ;
- un diagramme de flux ;
- une matrice risques / contrôles ;
- quelques bonnes pratiques.

3.6. Panorama des principaux processus métiers dans l'entreprise

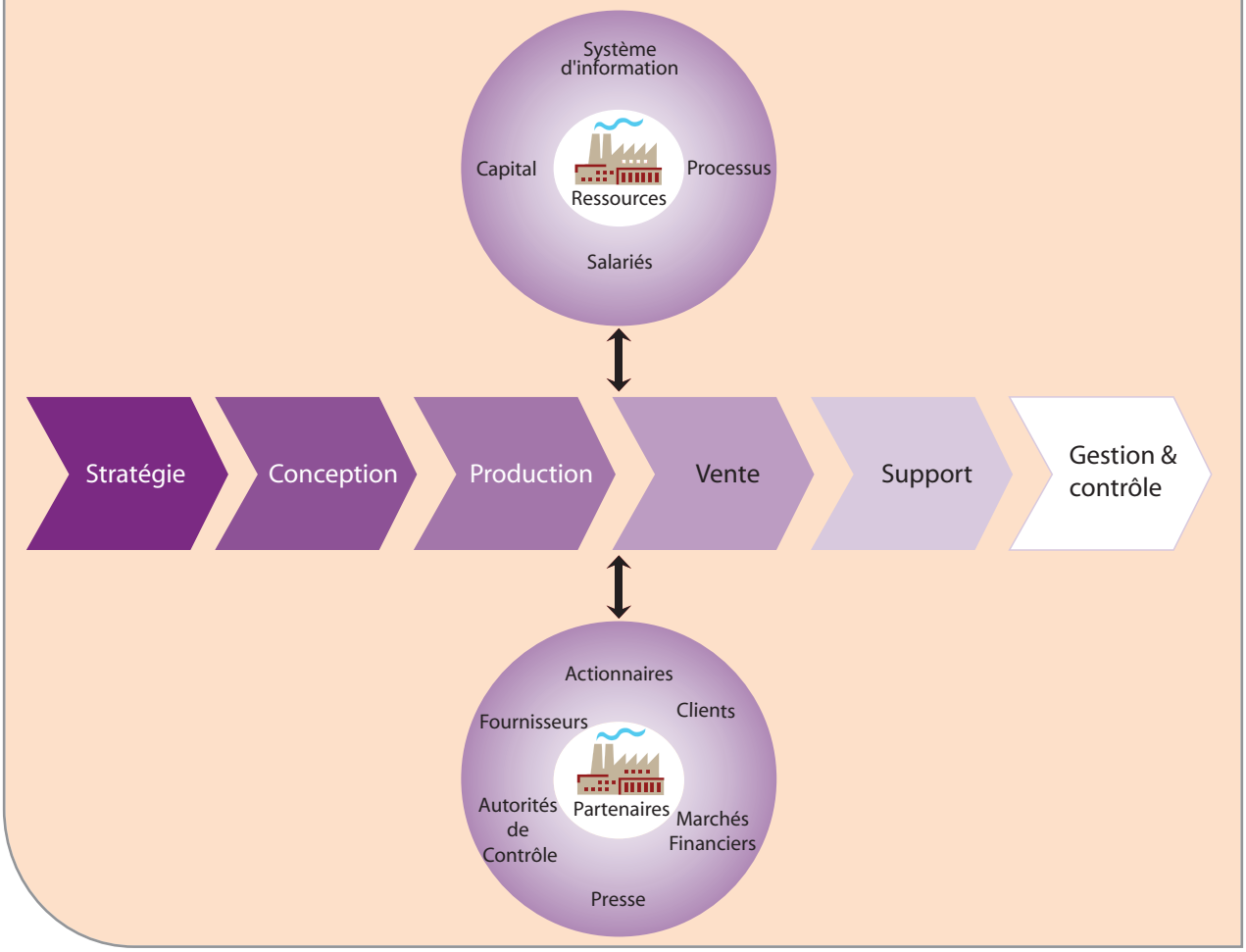
3.6.1. L'entreprise vue comme une chaîne de valeur

Avant de s'intéresser aux processus métiers de l'entreprise, on peut analyser l'entreprise de manière globale et transversale. L'entreprise peut être définie de plusieurs façons (approche structurelle, approche par les acteurs, système politique, etc.).

L'entreprise est, avant tout, une organisation dynamique qui mobilise des acteurs et des ressources, au sein d'un écosystème, le long d'une chaîne de valeur et selon des processus. La finalité de l'entreprise est de créer de la valeur pour les actionnaires et autres parties prenantes. Cette définition est intéressante car on retrouve ces éléments (acteurs, ressources, rôles) et cette finalité dans l'analyse des principaux processus de l'entreprise.

Figure 2 : Chaîne de valeur de l'entreprise

Source : CIGREF - IFACI



3.6.2. Les principaux processus de l'entreprise

On classe généralement les processus en trois grandes catégories :

- processus de direction ;
- processus opérationnels ;
- processus support.

Chaque macro-processus peut se découper en sous-processus / étapes. Il s'agit d'une typologie générique des processus : chaque entreprise peut avoir sa propre taxonomie.

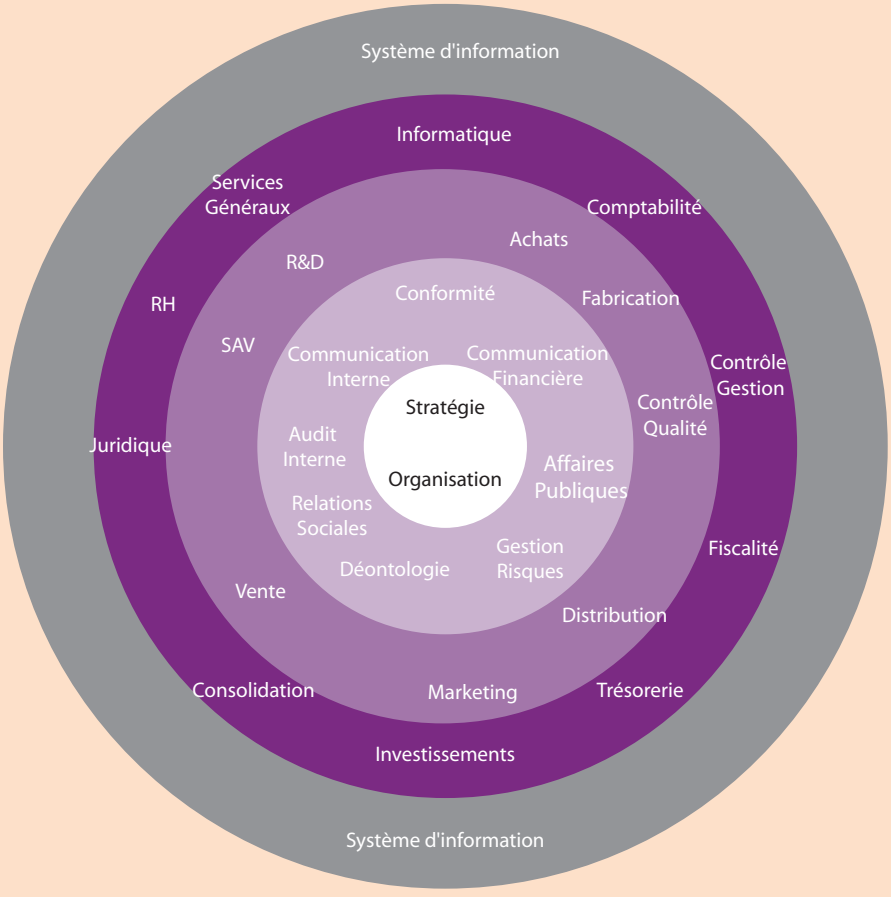
Figure 3 : Cartographie des principaux processus de direction, opérationnels et support de l'entreprise

Source : CIGREF - IFACI

Processus de direction	Processus opérationnels	Processus support
• Stratégie • Organisation • Déontologie • Conformité • Gestion des Risques • Communication financière • Audit interne • Affaires Publiques • Communication interne • Relations sociales	• Recherche & Développement • Achats • Fabrication • Contrôle qualité • Distribution / Logistique • Marketing • Vente • Après-vente	• Contrôle de gestion • Trésorerie • Comptabilité • Investissements • Consolidation • Fiscalité • Juridique • RH • Services généraux • Informatique

Figure 4 : Cartographie des principaux processus de l'entreprise

Source : CIGREF - IFACI



L'informatique est ici considérée comme un des métiers supports de l'entreprise *(Cf. figure 4)*. En revanche, dans cette représentation, le système d'information a été positionné autour de tous les processus de l'entreprise, signifiant ainsi qu'il les irrigue tous, de manière transversale. L'efficacité et la sécurité des processus dépendent directement du SI et de la pertinence des contrôles qui y sont intégrés.

Comme le précise le cadre de référence de l'AMF, le dispositif de contrôle interne assure le bon fonctionnement de l'ensemble des processus. Il permet la prise en compte appropriée des risques significatifs associés à leur mise en œuvre.

3.7. Les typologies de risques

Un des intérêts de la classification des risques dans une démarche de contrôle interne est de relier finement les processus aux risques et aux points de contrôle associés. Il convient au préalable d'utiliser une cartographie des risques de l'entreprise.

Les risques informatiques doivent être intégrés dans la démarche de gestion des risques de l'entreprise. Cette intégration passe par des méthodes communes et partagées afin de conserver une vision globale des risques.

On peut classer les risques en trois catégories :
- risques financiers ;
- risques opérationnels ;
- risques de conformité.

Figure 5 : Typologie des risques d'entreprise

Source : CIGREF - IFACI

Risques financiers	Risques opérationnels	Risques de conformité
• Risques de contrepartie • Risques de taux • Risques de change • Risques de marché • Risques de liquidité	• Risques pays • Catastrophe naturelle • Fraudes, corruption • Failles de sécurité • Accidents de travail • Arrêts de production • Dommages aux actifs corporels • Défaillances dans l'exécution et la gestion des processus et des systèmes • Autres dysfonctionnements de l'activité	• Aspects légaux et réglementaires • Risques de sanctions (administrative, judiciaire, disciplinaire) • Risques de réputation et d'image • Risques déontologiques • Risques contractuels

Il existe bien évidemment plusieurs autres formes de classification des risques.

- Le *World Economic Forum* distingue 5 catégories de risques (cf. annexe 4) : les risques économiques, sociétaux, environnementaux, technologiques et géopolitiques.

- Une autre classification (cf. annexe 4), proposée par Marsh Insurance, classe les risques en 5 catégories : les risques aléatoires, financiers, opérationnels, organisationnels et stratégiques.

- On peut également mentionner des classifications de risques sectorielles telles que celle prévue par le réglement CRBF 97-02 dans le secteur bancaire.

3.8. Les points de contrôle existants

Généralement on distingue les contrôles a priori (permettant de limiter l'occurrence d'un risque) et les contrôles a posteriori (visant à identifier et traiter les anomalies).
On peut aussi distinguer les contrôles automatiques et les contrôles manuels.

Selon le référentiel CobiT, il existe trois grands types de contrôle :
- les contrôles métiers (Business Controls) ;
- les contrôles applicatifs (IT Applications Controls) ;
- les contrôles généraux informatiques (IT General Controls).

Le contrôle du SI de l'entreprise repose sur les contrôles métiers et les contrôles applicatifs tandis que le contrôle de la DSI est basé sur la qualité des contrôles généraux informatiques.

Ce qui est important, c'est de ne pas oublier la finalité du contrôle (les objectifs) et d'être conscient de l'imperfection des outils, donc ne pas tout baser sur un seul type de contrôle. Il faut relier les contrôles aux risques. L'efficacité des contrôles doit être régulièrement appréciée dans le cadre d'un processus continu de réévaluation.

Figure 6 : Typologie des points de contrôle

Source : AFAI / COBIT

Contrôles métier

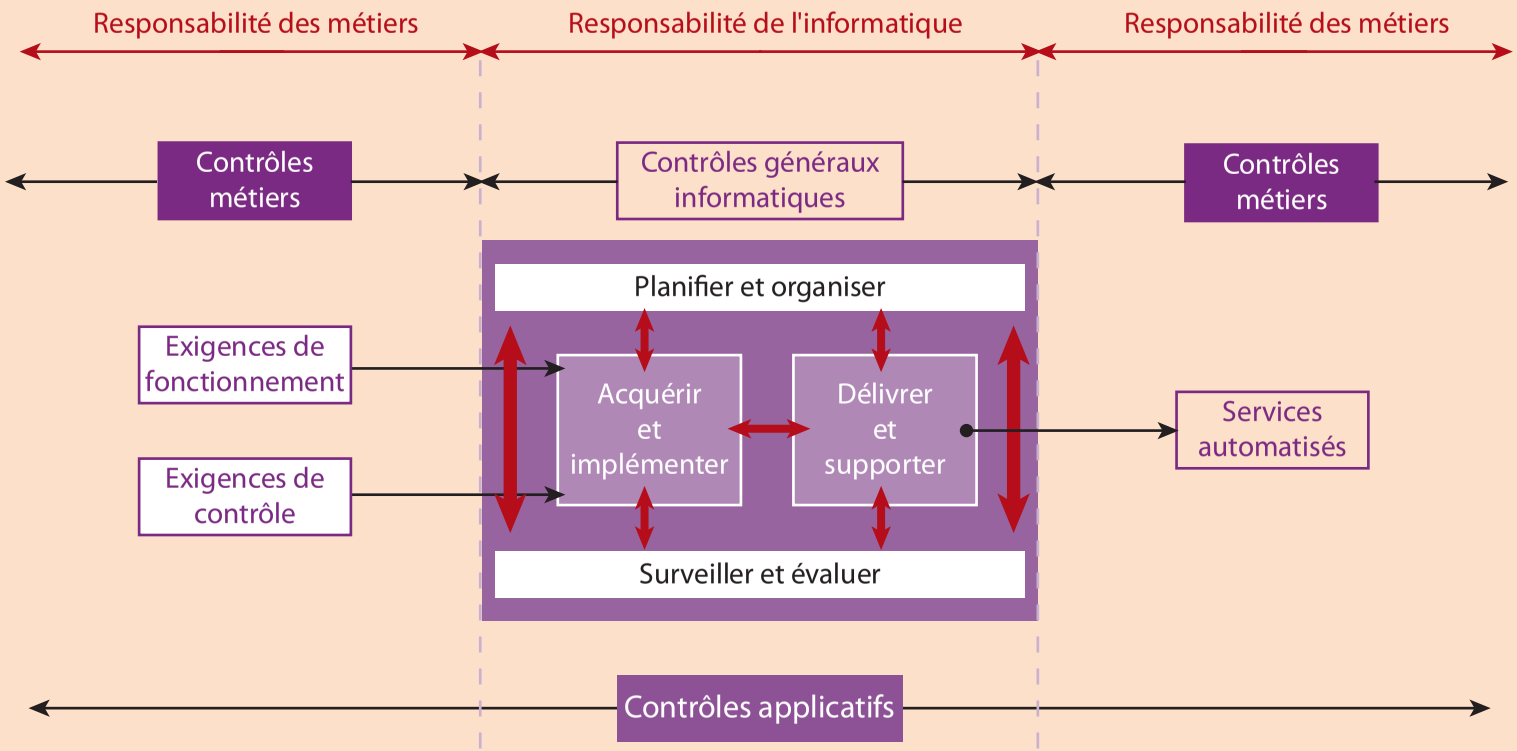
Tout contrôle (tel que les vérifications d'autorisations de transaction, les rapprochements exhaustifs ou non, ...) effectué par les entités opérationnelles dans le cadre des processus métier.
Ce sont souvent des contrôles manuels qui s'appuient sur des états produits par les applications.

Contrôles généraux informatiques

Les contrôles généraux sont ceux qui sont intégrés aux processus et aux services informatiques. Ils concernent, par exemple :
· le développement des systèmes,
· la gestion des changements,
· la sécurité,
· l'exploitation.

Contrôles applicatifs

On appelle communément "contrôles applicatifs" les contrôles intégrés dans les applications métier. Ils concernent, par exemple :
· l'exhaustivité,
· l'exactitude,
· la validité,
· l'autorisation,
· la séparation des tâches.



3.9. Les acteurs du risque

Au-delà de la démarche, ce qui importe c'est l'existence d'acteurs chargés de l'identification et du traitement de ces risques.

Pour formaliser la gestion des risques, on a adopté le modèle RACI[1] pour préciser les rôles et responsabilités des acteurs à chaque stade du cycle de gestion du risque : identification, évaluation, traitement et surveillance du risque.

Vous trouverez, ci-après, un tableau indicatif des responsabilités respectives des différents acteurs du processus de management des risques.
Ce tableau devra être adapté en fonction des spécificités de chaque organisation.

Figure 7 : Les acteurs du risque – exemple de répartition des rôles et responsabilités

Source : CIGREF - IFACI

	Identification des risques	Evaluation des risques	Traitement des risques	Surveillance
Direction générale	Approbateur	Approbateur	Informé	Approbateur
Directeur métier *	Approbateur	Approbateur	Approbateur	Approbateur
Opérationnels métier	Réalisateur	Réalisateur	Réalisateur	Consulté
Direction des systèmes d'information			Réalisateur	Consulté
Risk Manager Groupe	Réalisateur	Réalisateur / Approbateur	Informé	Informé
Responsable Sécurité SI	Informé	Informé	Réalisateur	
Responsable du contrôle interne	Consulté	Consulté	Consulté	Réalisateur
Audit interne	Informé / Réalisateur **	Informé / Réalisateur **	Informé	Réalisateur

** le DSI est considéré comme un directeur métier*
*** pour ses activités propres (plan d'audit, programme de travail des missions ...)*

L'absence de certains acteurs peut être palliée, de même que certains acteurs peuvent avoir plusieurs rôles à un stade du processus.

Un des enjeux aujourd'hui porte sur la coopération, entre acteurs du risque, au sein des organisations. Elle se fait au sein de structures de coordination et d'arbitrage à tous les niveaux de l'entreprise.

[1] *Le modèle RACI est un modèle qui permet de décrire les rôles et responsabilités des acteurs au sein d'une organisation, sur un processus donné. RACI définit 4 rôles - R: Responsible ou Réalisateur, A: Accountable ou Approbateur C: Consulted ou Consulté, I: Informed ou Informé.*

4. Le contrôle du SI de l'entreprise

4.1. Objectifs

Ce chapitre s'intéresse au contrôle interne des métiers de l'entreprise, par le prisme des SI, composant essentiel de toute activité. Il a pour but de fournir aux lecteurs les éléments suivants :

- une cartographie stratégique des principaux processus et risques au niveau de l'entreprise ;
- un guide d'application du cadre de référence AMF relatif au contrôle interne ;
- un guide méthodologique sur trois processus représentatifs et standards d'entreprise : les processus achat, vente et consolidation financière ;
- une boite à outils relative aux points de contrôle et bonnes pratiques.

4.2. Périmètre retenu

L'ensemble des macro-processus de l'entreprise et macro-risques associés a été cartographié. Au sein de ces macro-processus, les participants ont retenus trois processus clés en raison de leur caractère générique, commun aux entreprises mais aussi parce qu'ils étaient évoqués dans le cadre de référence AMF. Il s'agit des processus suivants :

- le processus achats ;
- le processus vente ;
- le processus consolidation financière ;

4.3. Démarche et rappel des principaux processus

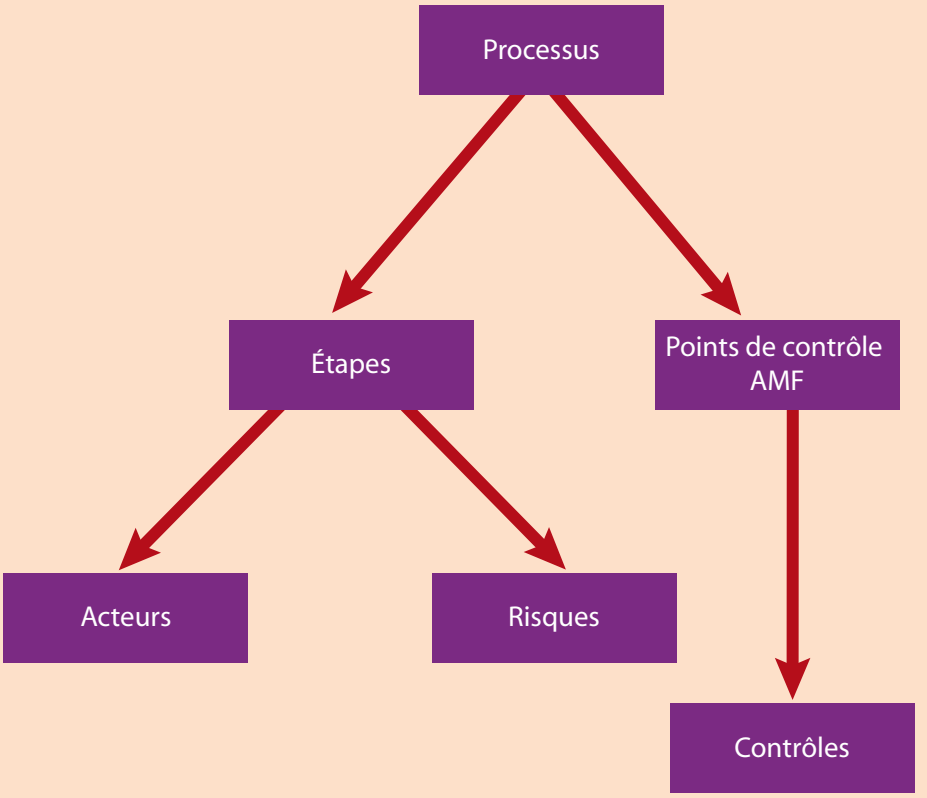
Pour chacun de ces trois processus, la démarche a porté successivement sur les points suivants :

- description du processus ;
- acteurs ;
- risques associés ;
- points de contrôles associés (en partant du cadre de référence AMF) ;
- contrôles et bonnes pratiques (le cas échéant).

En revanche la réflexion n'a pas porté sur des éléments de contexte jugés trop spécifiques ou propres à chaque entreprise, notamment le *mapping* processus / applications (spécifique), la typologie des applications, les particularismes sectoriels des organisations.

Figure 8 : Démarche suivie au sein du sous-groupe sur le contrôle du SI de l'entreprise

Source : CIGREF - IFACI



Les participants se sont attachés à lister un maximum de contrôles afin de fournir une aide opérationnelle et concrète au développement, au paramétrage ou à la maintenance des applications informatiques relatives aux trois processus étudiés. L'atteinte d'un bon niveau de contrôle des processus passe de fait par l'intégration des contrôles identifiés dans les systèmes correspondants. Ils ne peuvent néanmoins à ce stade avoir de caractère exhaustif, et pourront être étendus à loisir en fonction des besoins de chaque entreprise. C'est la raison pour laquelle le document parle d'exemples de contrôles.

L'important était de faire prendre conscience que la construction d'un système quel qu'il soit ne pouvait se limiter à l'automatisation des différentes étapes des processus métiers, mais devait aussi impérativement intégrer des routines de contrôle de leur bon fonctionnement.

A partir des 14 catégories d'opérations concourant à l'élaboration de l'information financière publiée, le groupe a retenu trois processus :

1) les achats fournisseurs et assimilés ;
2) les produits des activités ordinaires, clients et assimilés ; et
3) la consolidation.

Ces trois processus [en gras et en couleur] dans le tableau ci-après ont été étudiés dans les chapitres suivants.

Figure 9 : Les 14 catégories d'opérations concourant à l'élaboration de l'information comptable et financière publiée

Source : Cadre de référence AMF (chap 2 - p39-50)

N° de §	Nom de l'opération
2.3.1	Investissement / désinvestissement / R&D
2.3.2	Immobilisations incorporelles, corporelles et *goodwills*
2.3.3	Immobilisations financières
2.3.4	**Achats fournisseurs et assimilés**
2.3.5	Coût de revient / stocks et encours / Contrats à long terme ou de construction
2.3.6	**Produits des activités ordinaires / Clients et Assimilés**
2.3.7	Trésorerie / financement et instruments financiers
2.3.8	Avantages accordés au personnel
2.3.9	Impôts, taxes et assimilés
2.3.10	Opérations sur le capital
2.3.11	Provisions et engagements
2.3.12	**Consolidation**
2.3.13	Information de gestion nécessaire à l'élaboration des informations comptables et financières publiées
2.3.14	Gestion de l'information financière externe

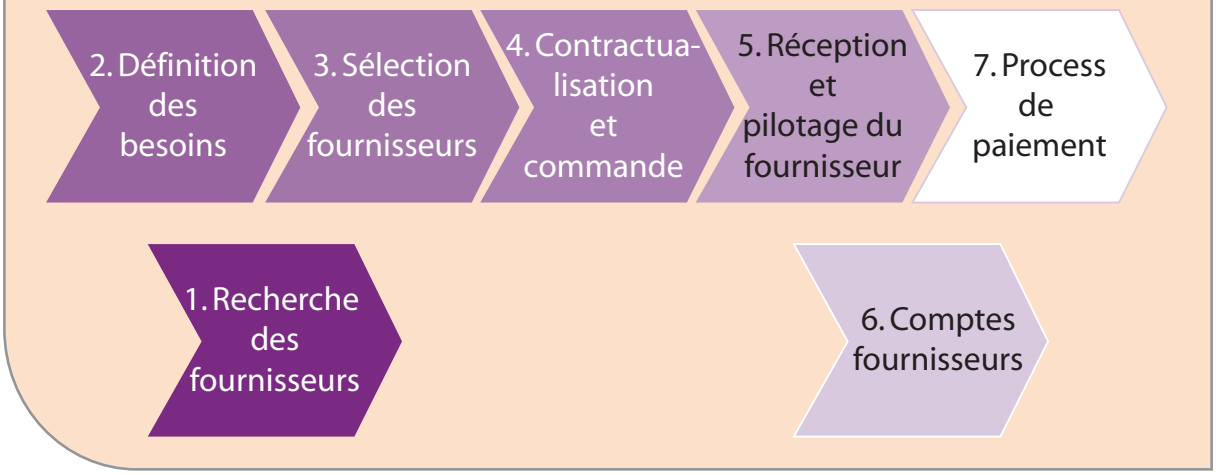
4.4. Description du processus achats

4.4.1. Processus

Le processus achats est découpé en sept étapes, résumées dans le graphique ci-dessous.

Figure 10 : Description du processus achats

Source : CIGREF - IFACI



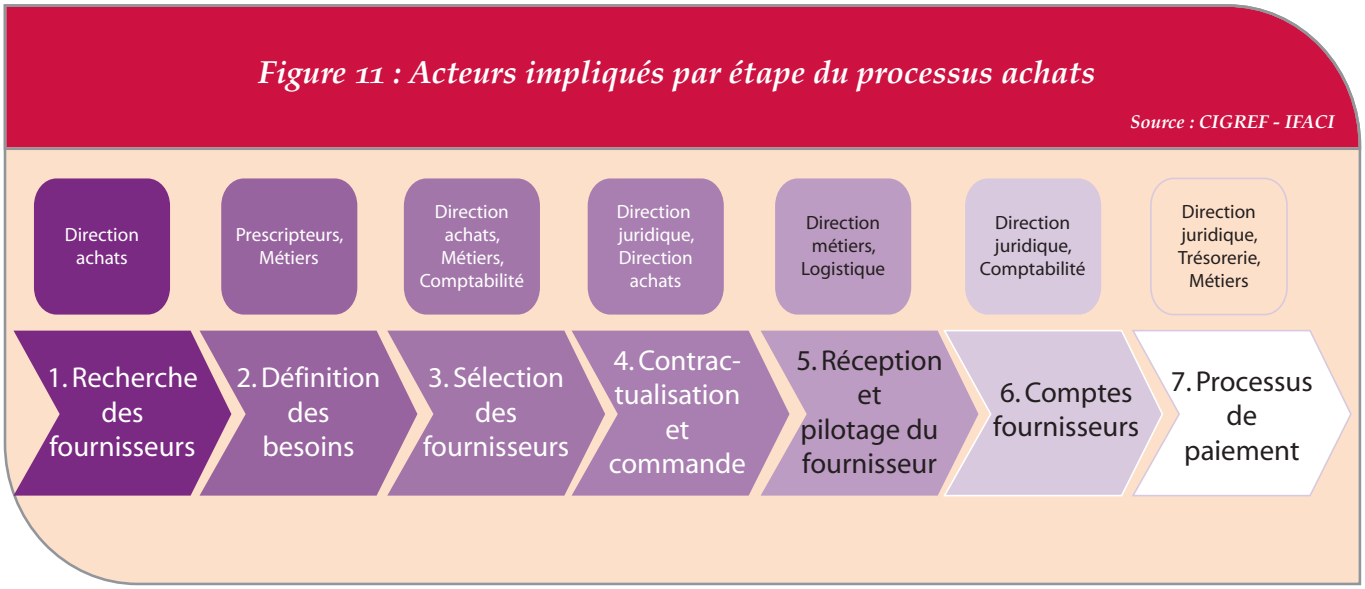
NB : le processus budgétaire a été volontairement exclu.

4.4.2. Acteurs

Les acteurs impliqués par étape sont décrits dans le schéma ci-dessous.

Figure 11 : Acteurs impliqués par étape du processus achats

Source : CIGREF - IFACI



4.4.3. Risques

Les principaux risques portent sur le non-respect des fournisseurs autorisés, le non-respect des montants autorisés, le non-respect du principe de séparation des tâches, le manque de contrôle qualité à la réception, la fraude.

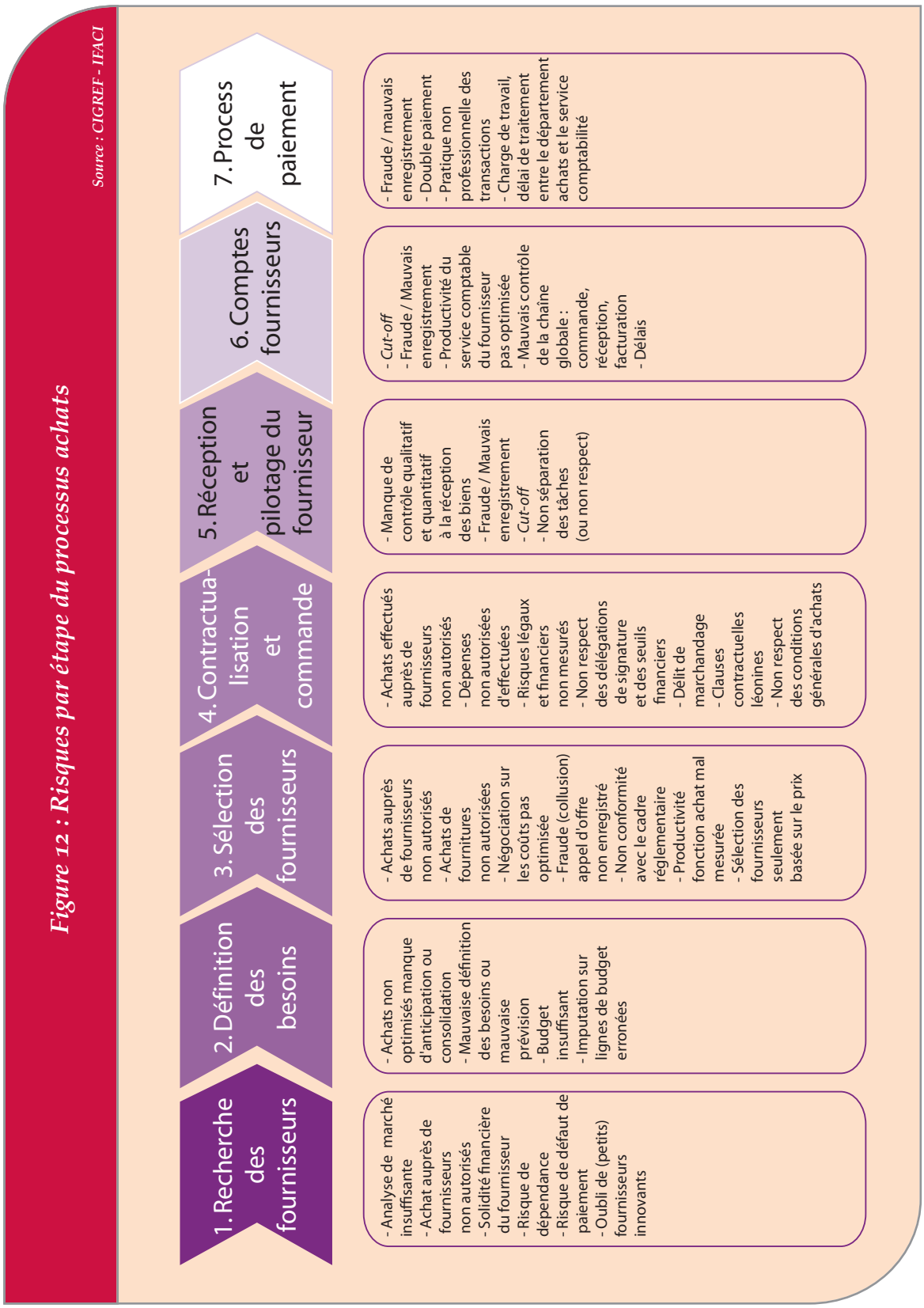


Figure 12 : Risques par étape du processus achats

Source : CIGREF - IFACI

4.4.4. Rapprochement entre risques et points de contrôles AMF

Le schéma ci-dessous relie les risques aux points de contrôle (PC, par exemple PC4.1) décrits dans le cadre de référence AMF. Chaque entreprise peut avoir une démarche spécifique et relier ses propres risques aux points de contrôles.

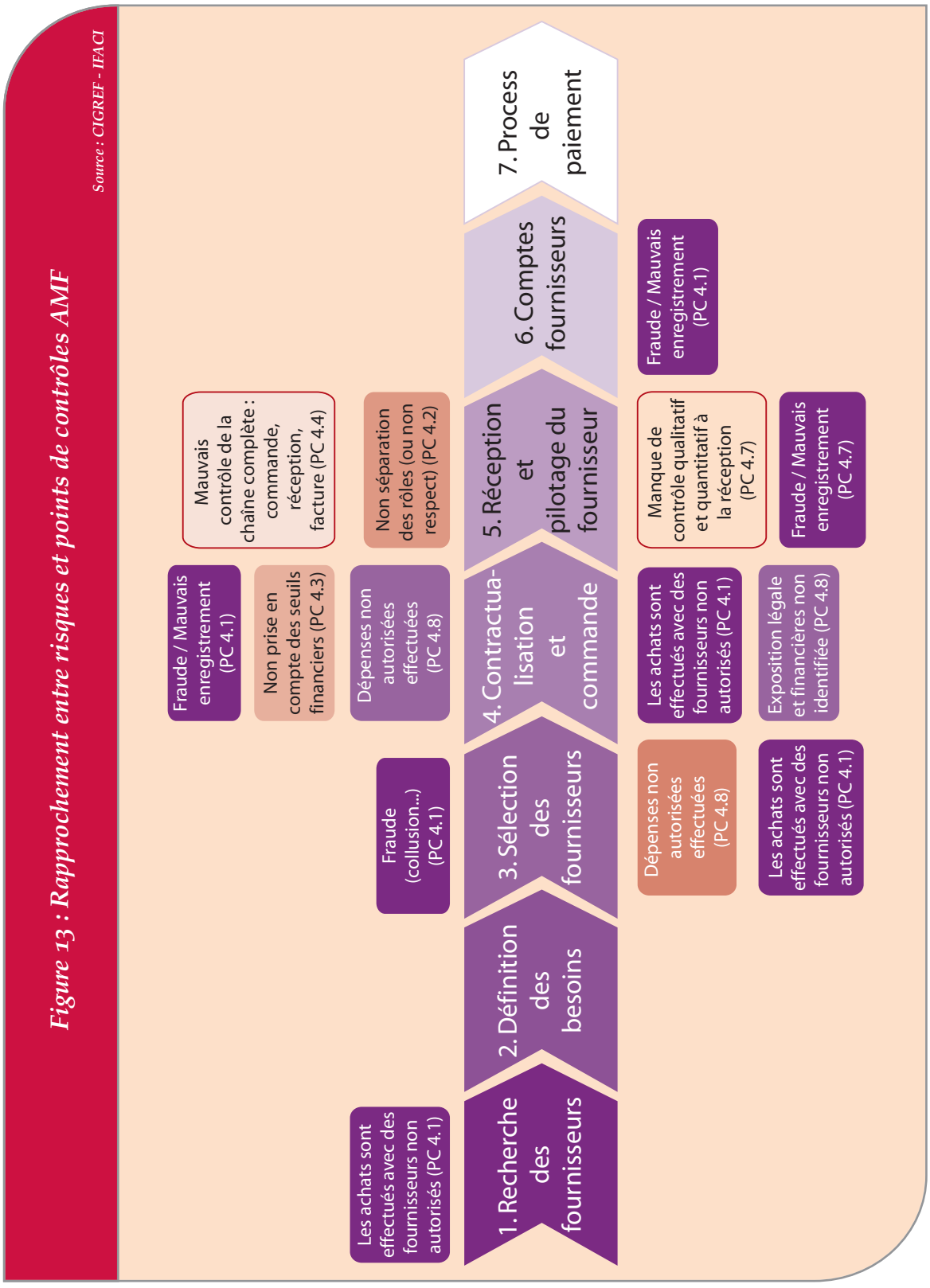


Figure 13 : Rapprochement entre risques et points de contrôles AMF

Source : CIGREF - IFACI

4.4.5. Rappel des principaux points de contrôle du guide d'application AMF

Le tableau ci-dessous reprend les principaux points de contrôle tels que listés dans le guide d'application du cadre de référence AMF.

Figure 14 : Rappel des principaux points de contrôle lié au processus achats

Source : Cadre de référence AMF (chap 2 - p41-42)

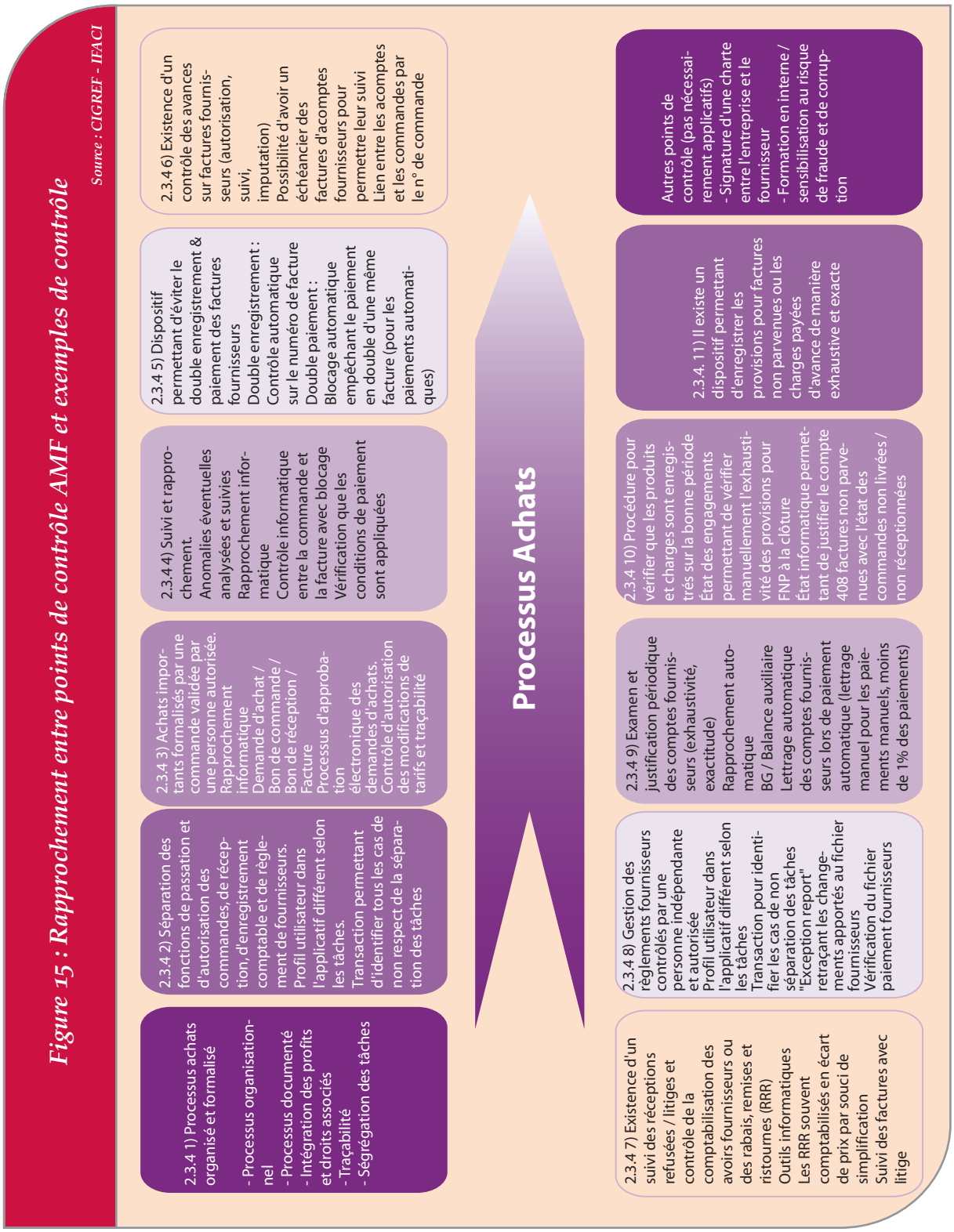
N° de §	Nom de l'opération
2.3.4	**Achats fournisseurs et assimilés**
2.3.4.1	Le processus achats est organisé et formalisé dans le cadre de procédures applicables par tous les acteurs concernés.
2.3.4.2	Il existe une séparation des fonctions de passation et d'autorisation des commandes, de réception, d'enregistrement comptable et de règlement des fournisseurs.
2.3.4.3	Les achats importants font l'objet d'une commande formalisée, validée par une personne autorisée.
2.3.4.4	Il existe un suivi et un rapprochement entre les bons de commande, les bons de réception et les factures (quantité, prix, conditions de paiement). Les anomalies éventuelles font l'objet d'une analyse et d'un suivi.
2.3.4.5	Il existe un dispositif permettant d'éviter le double enregistrement / paiement des factures fournisseurs.
2.3.4.6	Il existe un contrôle des avances sur factures fournisseurs (autorisation, suivi, imputation).
2.3.4.7	Il existe un suivi des réceptions refusées / litiges et un contrôle de la comptabilisation des avoirs fournisseurs correspondants ou des rabais, remises et ristournes (RRR).
2.3.4.8	La gestion des règlements fournisseurs fait l'objet de contrôles par une personne indépendante et autorisée.
2.3.4.9	Les comptes fournisseurs font l'objet d'un examen et d'une justification périodiques (exhaustivité, exactitude).
2.3.4.10	Il existe une procédure permettant de s'assurer que les produits et charges ont été enregistrés sur la bonne période.
2.3.4.11	Il existe un dispositif permettant d'enregistrer les provisions pour factures non parvenues ou les charges payées d'avance de manière exhaustive et exacte.

4.4.6. Rapprochement entre points de contrôle AMF et exemples de contrôle

Le schéma ci-dessous propose un rapprochement entre points de contrôle AMF et exemples de contrôle. Il s'agit d'exemples de contrôle, donnés à titre d'illustration. La liste n'est pas exhaustive. La plupart des contrôles mentionnés ci-après concerne essentiellement des aspects SI.

Figure 15 : Rapprochement entre points de contrôle AMF et exemples de contrôle

Source : CIGREF - IFACI



4.4.7. Vue détaillée du processus achats

Figure 16 : Vue détaillée du processus achats

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Processus Achats / Fournisseurs et assimilés
1) Recherche des fournisseurs	Direction achats	1. Pilotage et évolution des fournisseurs : la fonction achats coopère avec les autres départements pour anticiper les besoins futurs. Pendant ce temps là les connaissances sur les fournisseurs, les techniques, les innovations industrielles et les évolutions du marché sont capitalisées. Les fournisseurs principaux (actuels et potentiels) sont connus. 2. Recherche de solutions alternatives : cela inclut des études sur les technologies et les modes d'achat des biens et services critiques. 3. Liste des prestataires acceptés : la liste des prestataires acceptés mise à jour est définie par segment / famille de produits et selon des critères pertinents. Cette liste doit être utilisée par les acheteurs.	Analyse de marché / recherche insuffisante Les achats sont effectués auprès de fournisseurs non autorisés Les partenariats sont développés avec les meilleurs fournisseurs (Risque de dépendance) Solidité financière du fournisseur insuffisante Risque de défaut de paiement Oubli de (petits) fournisseurs innovants	*2.3.4.1) Le processus achats est organisé et formalisé dans le cadre de procédures applicables par tous les acteurs concernés.* => Processus organisationnel => Le processus doit être documenté Intégration des profils et droits associés Traçabilité Séparation des tâches incompatibles *2.3.4.2) Il existe une séparation des fonctions de passation et d'autorisation des commandes, de réception, d'enregistrement comptable et de règlement des fournisseurs.* - Profil utilisateur dans le progiciel / logiciel différent selon les tâches - Il existe une transaction permettant d'identifier tous les cas de non respect de la séparation des tâches *2.3.4.3) Les achats importants font l'objet d'une commande formalisée, validée par une personne autorisée.* - Rapprochement informatique Demande d'achat / Bon de commande / Bon de réception / facture - Processus d'approbation électronique des demandes d'achats / commande - Contrôle d'autorisation des modifications de tarif et traçabilité
2) Définition des besoins	Prescripteurs, métiers	1. Anticipation des besoins / consolidation des besoins : les besoins sont identifiés en terme d'objectifs, d'attentes et de coût par les utilisateurs et communiqués au département achats. Les achats sont planifiés et regroupés par période et entre unités / sites. 2. Validation : Les demandes d'achat sont émises pour tous les achats et approuvées par le responsable du budget, selon les délégations de pouvoir définies.	Des dépenses non-autorisées sont effectuées, budget insuffisant Les achats ne sont pas optimisés à cause d'un manqué d'anticipation / de consolidation Mauvaise définition des besoins / prévision incorrecte Budget insuffisant, Mauvaise imputation analytique et comptable de la dépense / investissement	

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Processus Achats / Fournisseurs et assimilés
3) Sélection des fournisseurs	Direction achats, métiers, comptabilité	1. Demande de devis / d'information : un nombre de fournisseurs identifiés sont invités à envoyer des offres détaillants leurs solutions, les prix, le calendrier. L'appel d'offre doit aussi spécifier les règles auxquelles chaque fournisseur devra se conformer pendant le processus de sélection ainsi que le calendrier, les dates clés et les livrables. 2. Analyse de l'offre : les différents devis sont analysés par l'équipe en utilisant des critères prédéterminés, applicables à tous les fournisseurs. L'analyse est présentée dans un tableau de synthèse pour faciliter la comparaison des réponses de chaque fournisseur. Une présélection des fournisseurs peut être faite avant d'aller plus loin. Avant d'entrer dans les négociations avec les fournisseurs, les objectifs des discussions doivent être définis et documentés pour rendre les objectifs clairs pour tout le monde. 3.Négociation et sélection : cela recouvre les aspects financiers, juridiques et le calendrier. Les questions concernant les spécifications seront abordées si un expert technique (ou un utilisateur) est impliqué. Plusieurs rounds de négociation peuvent être nécessaires, ce qui peut impliquer de nouveaux devis. Après la négociation avec chaque fournisseur, un fournisseur est sélectionné, en utilisant des critères objectifs et documentés. Les critères peuvent être pondérés. L'utilisateur valide la sélection de l'acheteur d'un point de vue fonctionnel et technique, essentiellement en fonction des spécifications définies préalablement.	Les achats sont effectués auprès de fournisseurs non autorisés Achats de fournitures non autorisés La négociation sur les coûts n'est pas optimisée Fraude (collusion, …) Appel d'offre non enregistré / ou mal enregistré Non conformité avec le cadre réglementaire européen sur les marchés publics La productivité de la fonction achat n'est pas correctement mesurée La sélection des fournisseurs est seulement basée sur le prix	*2.3.4.4) Il existe un suivi et un rapprochement entre les bons de commande, les bons de réception et les factures (quantité, prix, conditions de paiement). Les anomalies éventuelles font l'objet d'une analyse et d'un suivi.* - Rapprochement informatique, demande d'achat / Bon de commande / Bon de réception / facture - Contrôle informatique entre la commande et la facture sur les quantités et les prix avec blocage - Etat informatique permettant de justifier le compte 408 factures non parvenues avec l'état des commandes non livrées/ non réceptionnées - Vérification que les conditions de paiement sont appliquées *2.3.4.5) Il existe un dispositif permettant d'éviter le double enregistrement / paiement des factures fournisseurs.* - Pour éviter le double enregistrement d'une facture, il existe un contrôle automatique sur le numéro de facture - Pour éviter le double paiement, il existe un blocage automatique qui empêche le paiement en double d'une même facture (pour les paiements automatiques) *2.3.4.6) Il existe un contrôle des avances sur factures fournisseurs (autorisation, suivi, imputation).* - Possibilité d'avoir un échéancier des factures d'acomptes fournisseurs pour permettre leur suivi - Lien entre les acomptes et les commandes par le n° de commande

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Processus Achats / Fournisseurs et assimilés
4) Contractualisation et commande	Direction juridique, direction achats	1. Contractualisation et commande : la contractualisation des engagements des fournisseurs peut revêtir plusieurs formes (bon de commande, commande ouverte, accord de site, accord d'entreprise). Les contrats sont soumis aux conditions légales et contractuelles examinées avec le département juridique. Les contrats sont communiqués à tous les départements concernés, dont le département des finances. 2. Autorisation : les engagements d'achat (contrat, commande) sont autorisés en fonction des délégations de pouvoir, des seuils autorisés (par montant et type d'achats) et en fonction de la séparation des tâches.	Les achats sont effectués auprès de fournisseurs non autorisés Des dépenses non-autorisées sont effectuées Les risques légaux et financiers ne sont pas mesurés (délit de marchandage, prêt illicite de main d'œuvre, clauses contractuelles léonines, …) Pas de respect des délégations de signature et des seuils financiers Non respect des conditions générales d'achats et conditions générales de ventes	*2.3.4.7) Il existe un suivi des réceptions refusées / litiges et un contrôle de la comptabilisation des avoirs fournisseurs correspondants ou des rabais, remises et ristournes (à la facture, à la commande).* - Des outils informatiques existent mais pas obligatoires et pas de blocage prévu - Les RRR (rabais, remise, ristourne) sont souvent comptabilisés en écart de prix par souci de simplification - Suivi des factures avec litige (risque de payer l'intégralité du montant alors qu'il y a eu un refus de livraison)
5) Réception et pilotage du fournisseur	Direction métiers, logistique	1. Contrôle de la qualité et quantité : pour les matériaux et biens physiques, une personne différente de l'acheteur, vérifie que les biens reçus correspondent bien à la commande, en termes de type de produit et de quantités. Quand cela s'avère nécessaire, le réceptionnaire peut demander à l'utilisateur final de vérifier la qualité du bien si une expertise technique est requise. Pour les services, l'acheteur vérifie que les services reçus correspondent bien à la commande, en termes de livrables, délais et indicateurs de qualité. La réception est matérialisée par formulaire de livraison signé remis au fournisseur, inscrit dans un progiciel (ERP) et comparé avec le bon de commande initial. 2. Gestion des réclamations et pilotage du fournisseur : tous les départements impliqués dans la réception des biens et services informent le service des achats du moindre problème. Tous les retours et les réclamations sont enregistrés et suivis par le service des achats. Les résultats sont utilisés pour « challenger » les fournisseurs ou renégocier les conditions d'achats.	Manque de contrôle qualitatif et quantitatif à la réception des biens Fraude / Enregistrement incorrect *Cut-off* Non séparation des tâches (ou non respect)	*2.3.4.8) La gestion des règlements fournisseurs fait l'objet de contrôles par une personne indépendante et autorisée.* - Profil utilisateur dans le progiciel différent selon les tâches - Il existe une transaction / test permettant d'identifier tous les cas de non respect de la séparation des tâches - Existence d'un rapport d'exception *(« exception report »)* qui retrace tous les changements (création, suppression, changement) apportés au fichier Fournisseurs (ex : modification des coordonnées bancaires, création d'un fournisseur fictif, changement des conditions de paiement …) - Vérifier qu'il n'y a pas de modification possible du fichier paiement fournisseurs (par le trésorier)

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Processus Achats / Fournisseurs et assimilés
6) Compte fournisseur et gestion fichier fournisseur	Direction juridique, direction comptabilité, direction administrative	1. Contrôle des factures : les factures sont comparées avec les bons de livraison des produits / services, soit physiquement (papier) soit électroniquement (via une application) par le département en charge des comptes fournisseurs (comptabilité fournisseur). Si les documents correspondent (montant total, quantité, prix) la facture est approuvée pour paiement en fonction des principes de délégation de pouvoirs et de séparations de tâches. S'il y a des erreurs ou écarts, le département contacte le fournisseur pour qu'il corrige la facture, ou le réceptionnaire pour qu'il vérifie ce qu'il a vraiment reçu, ou l'acheteur pour qu'il vérifie les termes et prix négociés. Veiller au respect des délais et aux processus de contestation qui doivent être formalisés dans le contrat. 2. Pilotage de la comptabilité fournisseur : des procédures de clôture sont menées régulièrement pour s'assurer de l'exactitude des positions de la comptabilité fournisseurs. Par exemple les comptes sont nettoyés régulièrement et réconciliés avec des parties tierces.	*Cut-off* Fraude / Enregistrement incorrect La productivité du service comptable du fournisseur n'est pas optimisée Mauvais contrôle de la chaine globale : commande, réception, facturation Délais	*2.3.4.9) Les comptes fournisseurs font l'objet d'un examen et d'une justification périodiques (exhaustivité, exactitude).* - Rapprochement automatique Balance Globale / Balance auxiliaire - Lettrage automatique des comptes fournisseurs lors de paiement automatique (lettrage manuel à faire pour les paiements manuels : - de 1% des paiements) - Tous les comptes Fournisseurs ouverts correspondent à des fournisseurs réels ; o Exemples : il n'y a pas de fournisseurs génériques. Il existe des états qui permettent d'obtenir les historiques des changements, modifications … o Surveillance de la part de chaque Fournisseur dans le total des Achats, pour identifier/limiter les risques de dépendance o Bonne pratique – contrôle une fois par mois (ou trimestre selon le type d'activité, les gammes de produits, les clients)
7) Processus de paiement	Direction juridique, trésorerie, métiers	Une fois la facture approuvée, le fournisseur est payé selon les termes négociés dans le contrat. Le paiement est lancé par la Trésorerie et autorisé par la Comptabilité en conformité avec le principe de séparation des tâches.	Fraude / Enregistrement incorrect Erreurs de paiement : fournisseur ou paiement incorrect ou double etc. Pratiques non professionnelles des transactions Charge de travail, délai de traitement entre le département achats et le service comptabilité	*2.3.4.10) Il existe une procédure permettant de s'assurer que les produits et charges ont été enregistrés sur la bonne période.* - Il existe un état des engagements qui permet de vérifier manuellement l'exhaustivité des provisions pour FNP à la clôture - Etat informatique permettant de justifier le compte 408 factures non parvenues avec l'état des commandes non livrées/ non réceptionnées

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Processus Achats / Fournisseurs et assimilés
				2.3.4.11) Il existe un dispositif permettant d'enregistrer les provisions pour factures non parvenues ou les charges payées d'avance de manière exhaustive et exacte. - Idem au point de contrôle précédent (2.3.4.10) Autres points de contrôle (pas nécessairement applicatifs) - Signature d'une charte entre l'entreprise et le fournisseur - Formation en interne / tutoriel de sensibilisation au risque de fraude et de corruption

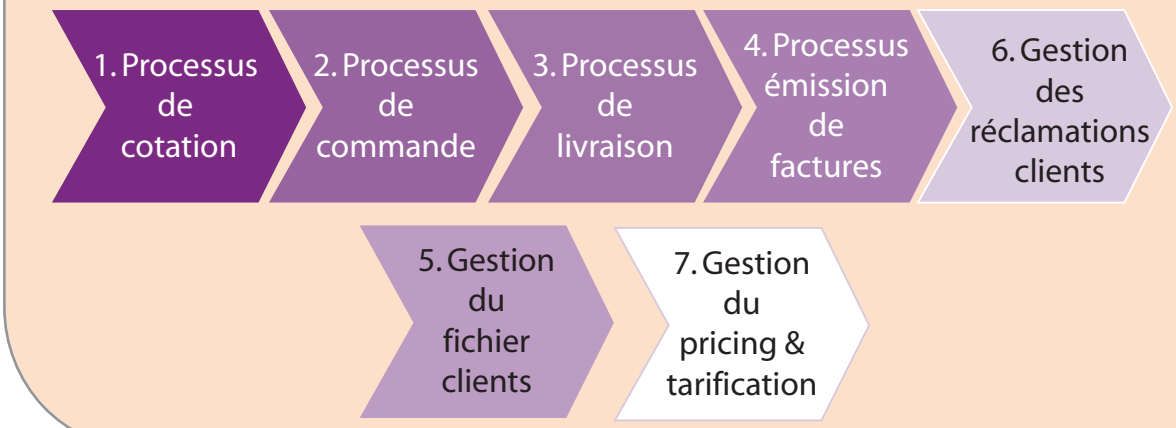
4.5. Description du processus ventes

4.5.1. Processus

Le processus de vente se découpe en sept étapes, résumées dans le graphique ci-dessous.

Figure 17 : Description du processus ventes

Source : CIGREF - IFACI

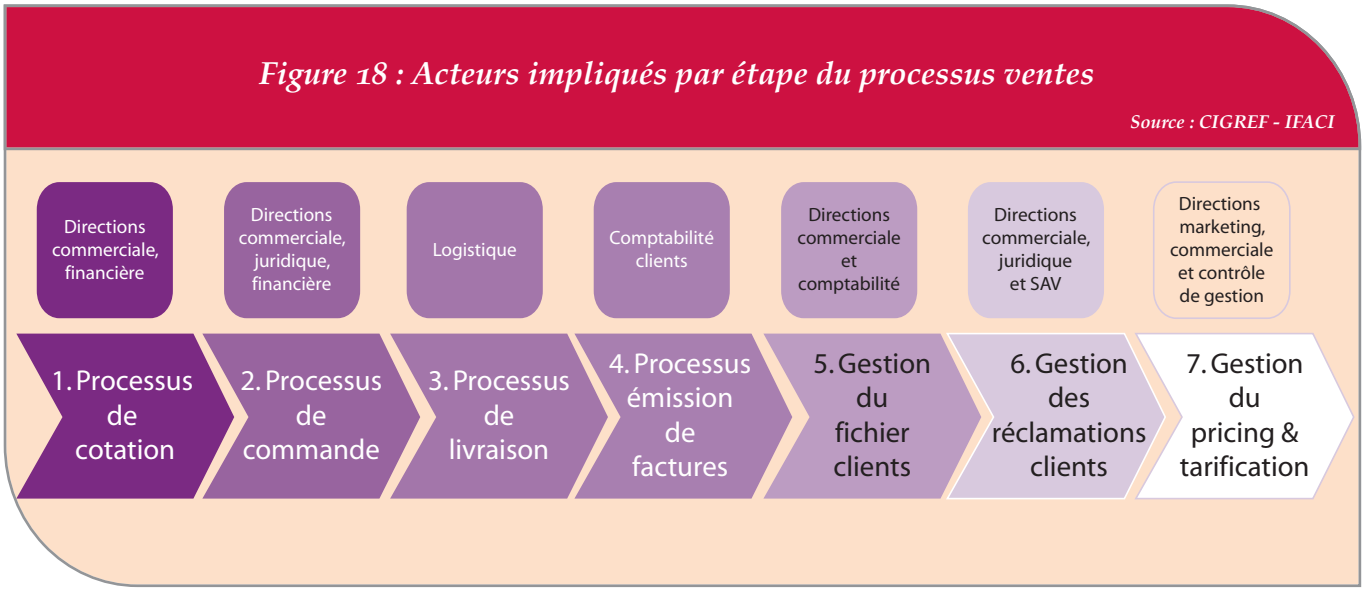


4.5.2. Acteurs

Les acteurs impliqués par étape sont décrits dans le schéma ci-dessous.

Figure 18 : Acteurs impliqués par étape du processus ventes

Source : CIGREF - IFACI



4.5.3. Risques

Les principaux risques sont des risques liés à la fraude, des risques de non conformité aux lois et réglementations commerciales, des risques liés à la fiabilité du reporting financier et des risques liés à la performance et à l'efficacité des opérations.

Figure 19 : Risques par étape du processus ventes

Source : CIGREF - IFACI

4.5.4. Rapprochement entre risques et points de contrôles AMF

Le schéma ci-dessous relie les risques aux points de contrôle décrits dans le cadre de référence AMF. Chaque entreprise peut avoir une démarche spécifique et relier ses propres risques aux points de contrôles.

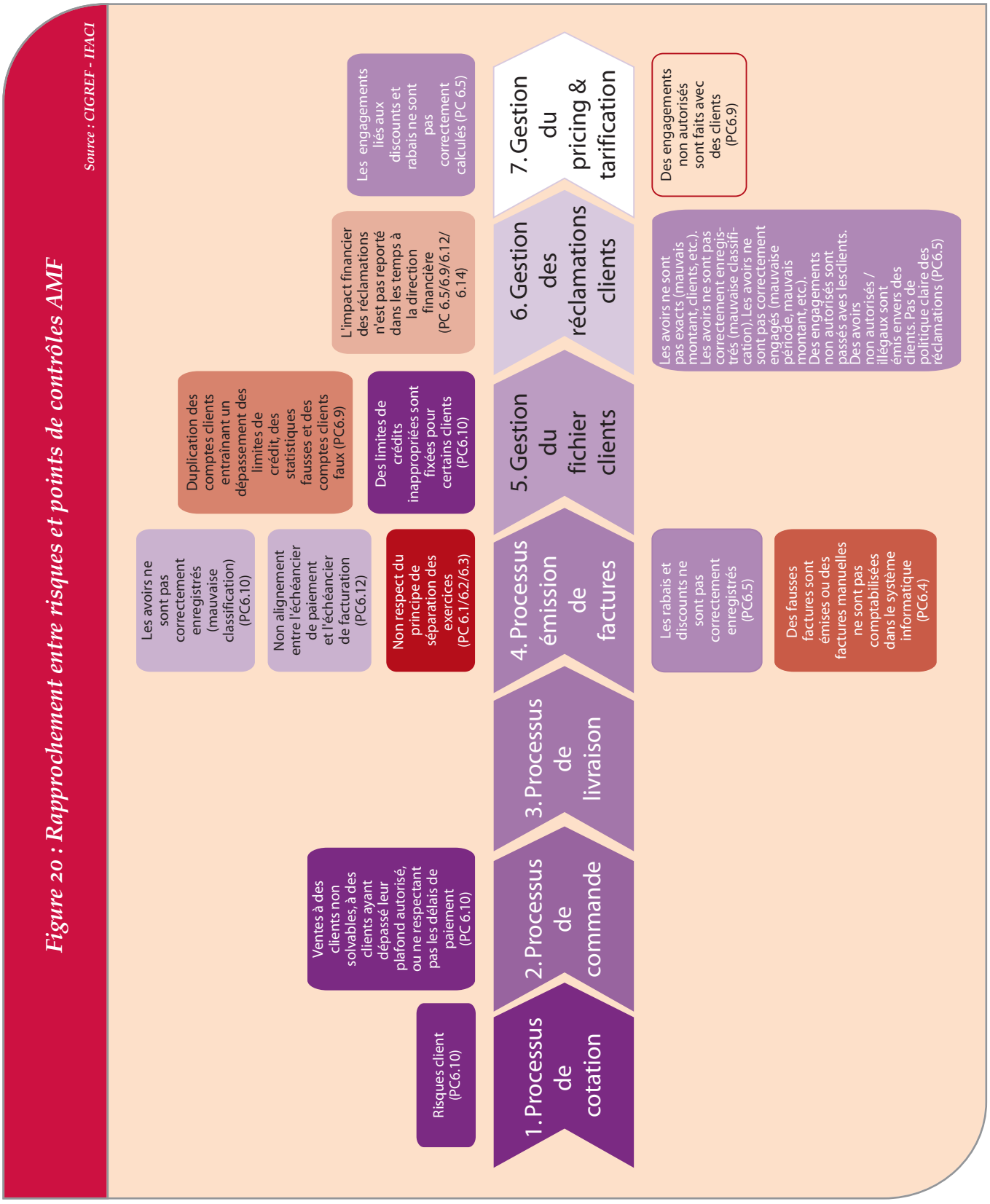


Figure 20 : Rapprochement entre risques et points de contrôles AMF

Source : CIGREF - IFACI

4.5.5. Rappel des principaux points de contrôle du guide d'application AMF

Le tableau ci-dessous reprend les principaux points de contrôle tels que listés dans le guide d'application du cadre de référence AMF.

Figure 21 : Rappel des principaux points de contrôle liés au processus ventes

Source : Cadre de référence AMF (chap 2 - p43-44)

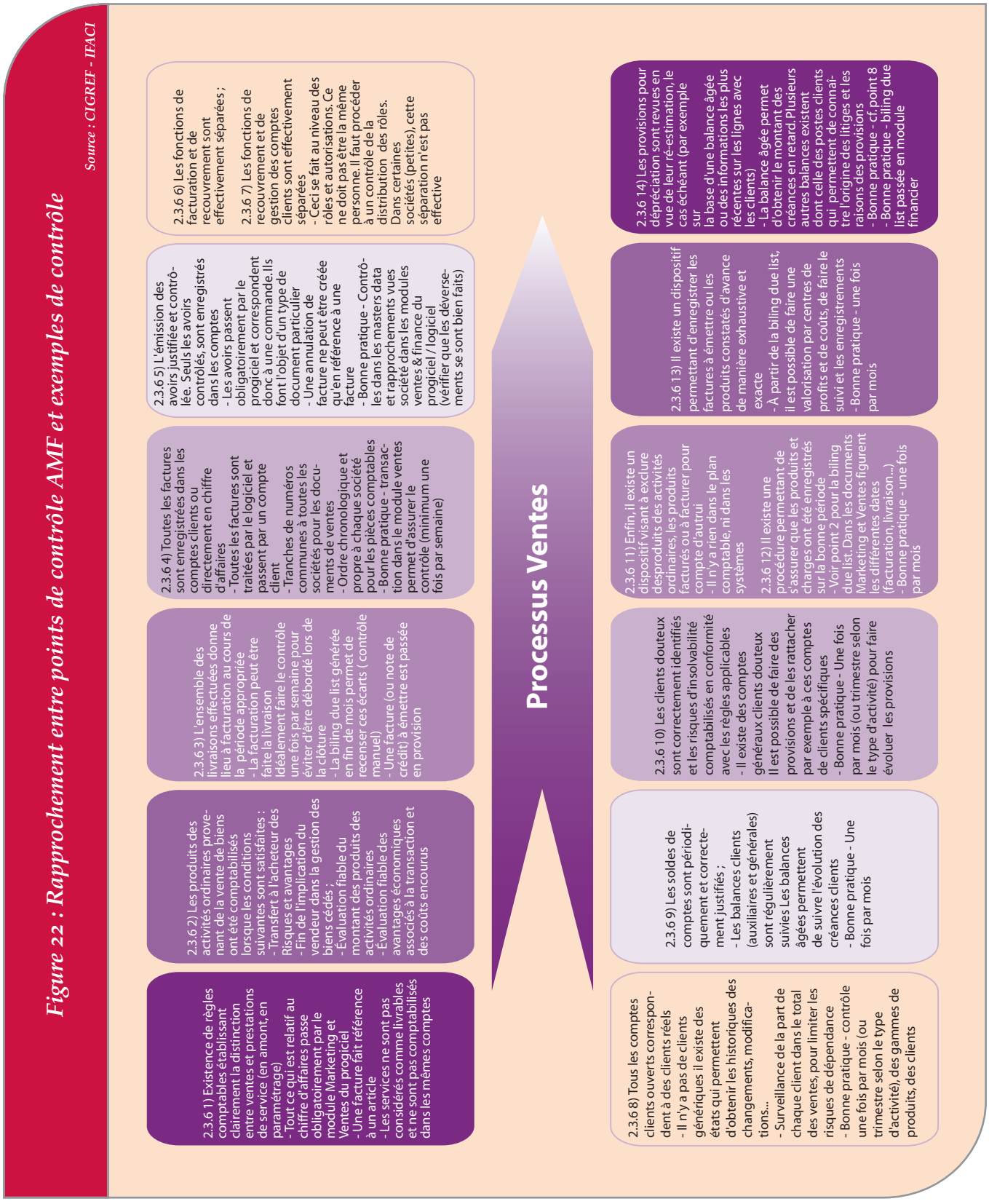
N° de §	Nom de l'opération
2.3.6	**Produits des activités ordinaires / Clients et Assimilés**
2.3.6.1	Les règles comptables adoptées par la société établissent clairement la distinction entre ventes et prestations de service et indiquent si nécessaire les modalités de séparation adoptées pour les contrats à composantes multiples
2.3.6.2	Les produits des activités ordinaires provenant de la vente de biens ont été comptabilisés lorsque l'ensemble des conditions suivantes ont été satisfaites : - la société a transféré à l'acheteur les risques et avantages importants inhérents à la propriété des biens ; - la société a cessé d'être impliquée dans la gestion, telle qu'elle incombe normalement au propriétaire, et dans le contrôle effectif des biens cédés ; - le montant des produits des activités ordinaires peut être évalué de façon fiable ; - il est probable que des avantages économiques associés à la transaction iront à la société, - les coûts encourus ou à encourir concernant la transaction peuvent être évalués de façon fiable.
2.3.6.3	L'ensemble des livraisons effectuées (ou services rendus) donne lieu à facturation au cours de la période appropriée.
2.3.6.4	Toutes les factures (séquentiellement numérotées) sont enregistrées dans les comptes clients ou directement en chiffre d'affaires.
2.3.6.5	L'émission des avoirs est justifiée et contrôlée. Seuls les avoirs contrôlés sont enregistrés dans les comptes.
2.3.6.6	Les fonctions de facturation et de recouvrement sont effectivement séparées.
2.3.6.7	Les fonctions de recouvrement et de gestion des comptes clients sont effectivement séparées.
2.3.6.8	Tous les comptes clients ouverts correspondent à des clients réels.
2.3.6.9	Les soldes de comptes sont périodiquement et correctement justifiés.
2.3.6.10	Les clients douteux sont correctement identifiés et les risques d'insolvabilité comptabilisés en conformité avec les règles applicables.
2.3.6.11	Il existe un dispositif visant à exclure des produits des activités ordinaires, les produits facturés ou à facturer pour compte d'autrui.
2.3.6.12	Il existe une procédure permettant de s'assurer que les produits et charges ont été enregistrés sur la bonne période.
2.3.6.13	Il existe un dispositif permettant d'enregistrer les factures à émettre ou les produits constatés d'avance de manière exhaustive et exacte.
2.3.6.14	Les provisions pour dépréciation sont revues en vue de leur ré-estimation, le cas échéant (par exemple sur la base d'une balance âgée, ou des informations les plus récentes sur les litiges avec les clients).

4.5.6. Rapprochement entre points de contrôle AMF et exemples de contrôle

Le schéma ci-dessous propose un rapprochement entre points de contrôle AMF et exemples de contrôles, à titre d'illustration. La liste n'est pas exhaustive.

Figure 22 : Rapprochement entre points de contrôle AMF et exemples de contrôle

Source : CIGREF - IFACI



4.5.7. Vue détaillée du processus vente

Figure 23 : Vue détaillée du processus ventes

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
1) Processus de cotation	Direction commerciale Direction financière Direction juridique	Ce processus consiste à répondre aux demandes des clients ou des prospects, en rassemblant l'information nécessaire pour établir le compte, négocier et contractualiser si possible. **Point de départ / Point de clôture** Demande de cotation de la part du prospect / client Réponse au prospect / client et signature du contrat si possible	Des engagements non autorisés sont passés avec le client Non conformité aux lois et réglementations commerciales Exposition à des risques de change non identifiés Rupture de la cohérence de la politique de prix par région, par segment, par produit, par moyen de transport Perte d'opportunités de vente liée à l'arrivée tardive des propositions commerciales Risque client (Risque Financier & Marché) (scoring) Client refusant de payer (mauvais contrôle de la dette) Risque pays ou de contrepartie Risque prix (profitabilité, compétiteurs) Mauvais engagement sur des services en dehors du prix (délai de livraison, etc.) Pas de prise en compte du risque de change	*2.3.6.1) Les règles comptables adoptées par la société établissent clairement la distinction entre ventes et prestations de service (en amont, en paramétrage).* Exemples - Tout ce qui est relatif au chiffre d'affaires passe obligatoirement par le module Marketing et Ventes du progiciel (ERP) ou d'un autre logiciel.. - Une facture fait référence à un article et il existe un type d'articles spécifiques pour les prestations de services. Au niveau du groupe d'imputation articles, une distinction est faite sur ce qui est facturé (paramétrage). - Les services ne sont pas considérés comme livrables et ne sont pas comptabilisés dans les mêmes comptes.

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
2) Processus de commande	Direction commerciale Direction juridique Direction financière	Ce processus comprend : - La réception du bon de commande du client - La génération du bon de commande (incluant le prix, le type de produit, les coûts de transport si nécessaire et le code produit) - La confirmation de la commande (engagement sur la quantité) **Point de départ / Point de clôture** Bon de commande du client (oral, papier ou en EDI) Commande ouverte basée sur un contrat cadre (oral, papier ou EDI) Cotation Commande confirmée pour la livraison Commande annulée due à des requêtes non résolues	Des engagements non autorisés sont passés avec le client Ventes à des clients non solvables, à des clients ayant dépassé leur plafond autorisé, ou ne respectant pas les délais de paiement. Réclamations faites par le client (non respect des termes de vente) Mauvaise qualité de services due à des informations incorrectes ou insuffisantes sur le client Délai ou erreur faite dans le processus de commande Défaut dans le conseil au client Clause d'exonération de responsabilité dans le contrat Changement dans l'environnement légal Démarrage du projet avant la signature du contrat	*2.3.6.2) Les produits des activités ordinaires provenant de la vente de biens ont été comptabilisés lorsque l'ensemble des conditions suivantes ont été satisfaites :* - *la société a transféré à l'acheteur les risques et avantages importants inhérents à la propriété des biens ;* - *la société a cessé d'être impliquée dans la gestion, telle qu'elle incombe normalement au propriétaire, et dans le contrôle effectif des biens cédés ;* - *le montant des produits des activités ordinaires peut être évalué de façon fiable ;* - *il est probable que des avantages économiques associés à la transaction iront à la société, et* - *les coûts encourus ou à encourir concernant la transaction peuvent être évalués de façon fiable.*
3) Processus de livraison	Logistique	Ce processus comprend l'arrivée des véhicules de transport, leur pesée, leur chargement, l'impression des documents de livraison **Point de départ / Point de clôture** Confirmation du bon de commande ou ordre de transfert Le produit quitte le site	Des livraisons non autorisées sont faites Les quantités livrées ne correspondent pas à celles enregistrées dans le livre des ventes Les quantités physiques ne sont pas bien pesées Les livraisons ne sont pas correctement enregistrées (fraude, mauvaise facture) Fraude Vol ou fraude de marchandises par un transporteur ou un client non autorisé Les factures ne reflètent pas les ventes ou les livraisons (mauvaise quantité, prix, discounts, taxes, fraude…) Difficultés à tracer les informations, au regard des plaintes, de la commande à la livraison et à la facture Délai de livraison non respecté Conditions de livraison non respectées Qualité de produit ou packaging non satisfaisant Temps d'attente non optimisé	*2.3.6.3) L'ensemble des livraisons effectuées (ou services rendus) donne lieu à facturation au cours de la période appropriée ;* Exemples : - Pour 99% des cas la facturation est faite à la livraison. En fin de mois, il est possible de décaler. Idéalement faire le contrôle une fois par semaine pour éviter d'être débordé lors de la clôture - La *billing due list* (écart entre livraison et facturation) générée en fin de mois permet de recenser ces écarts par centre de profits, articles, clients. (peut se traduire par une émission de provision) (contrôle manuel) - Une facture (ou note de crédit) à émettre est passée en provision. Confirmation de la *picking list* basée sur le prélèvement des quantités. Seules les *picking lists* confirmées peuvent être facturées.

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
4) Processus d'émission de facture	Comptabilité clients	Ce processus concerne la facturation des ventes nettes de produits **Point de départ / Point de clôture** Confirmation de la livraison des produits Facture envoyée au client	Non alignement entre l'échéancier de paiement et l'échéancier de facturation Les factures en devises ne sont pas correctement enregistrées Les rabais et discounts ne sont pas correctement enregistrés Les avoirs ne sont pas correctement enregistrés (mauvaise classification) Les factures ne reflètent pas les ventes ou les livraisons (quantité, prix, discount, taux de fiscalité erroné, fraude…) Des factures manuelles frauduleuses sont préparées ou des factures manuelles sont mal rentrées dans le système Non conformité aux lois et réglementations Application du mauvais taux de TVA Les relations avec les clients peuvent être dégradées, du fait d'une des opérations suivantes : Facture dupliquée Facture non envoyée au client Facture tardive Documentation annexe non jointe à la facture	*2.3.6.4) Toutes les factures (séquentiellement numérotées) sont enregistrées dans les comptes clients ou directement en chiffre d'affaires.* Exemples - Toutes les factures sont traitées par le progiciel (ERP) ou logiciel et passent par un compte client au niveau du module des ventes. Il n'y a pas d'enregistrement de factures au niveau du module finances. - Tranches de numéros : o Communes à toutes les sociétés pour les documents de vente o Ordre chronologique et propre à chaque société pour les pièces comptables - Bonne pratique - Une transaction dans le module ventes du progiciel / logiciel permet de le vérifier (Mini une fois par semaine)

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
5) Processus de gestion du fichier clients	Direction commerciale, Direction comptabilité	Ce processus concerne la création, la maintenance et la désactivation, dans le système, dans le temps, des informations concernant les prospects et les clients (informations techniques, marketing, financières, etc.) **Point de départ / Point de clôture** Création du fichier client / prospect Mise à jour du fichier client / prospect Désactivitation du fichier client / prospect Mise à jour du fichier maitre permettant l'enregistrement des transactions	Plusieurs comptes dupliqués sont créés par client, conduisant à une surestimation du crédit autorisé, des statistiques erronées et des « *accruals* » Les clients payant comptant à la livraison sont mal classifiés Le fichier clients ne contient pas les bonnes informations ou les informations complètes (exemple : hiérarchie client manquante, drapeaux signalant les liens capitalistiques inter-sociétés…) Non conformité aux lois, réglementations et pratiques locales Des engagements non autorisés sont passés avec des clients Des personnes non autorisées ont accès au fichier clients ou peuvent faire des changements dans le fichier clients Des clients avec des crédits non autorisés sont rentrés dans le système des ventes. Risque de dépendance clients Duplication de l'entité légale dans les carnets d'adresse Duplication de fichiers clients dans le fichier maitre Mauvaise qualité des données	*2.3.6.5) L'émission des avoirs est justifiée et contrôlée. Seuls les avoirs contrôlés sont enregistrés dans les comptes.* Exemples - Les avoirs passent obligatoirement par un module du SI (progiciel ou autre) et correspondent donc à une commande. Ils font l'objet d'un type de document particulier. - Une annulation de facture ne peut être créée qu'en référence à une facture. D'autres éléments (comme les ristournes de fin d'année) peuvent faire référence à une commande mais pas à une facture. - Bonne pratique - Contrôles aussi dans le fichier clients et rapprochement vues sociétés dans les modules ventes et finance du progiciel ou logiciel (vérifier que les déversements se sont bien faits, toutes les factures clients vers la comptabilité). *2.3.6.6) Les fonctions de facturation et de recouvrement sont effectivement séparées.* *2.3.6.7) Les fonctions de recouvrement et de gestion des comptes clients sont effectivement séparées.* Exemples - Ceci se fait au niveau des rôles et autorisation. Ce ne doit pas être la même personne. Il faut procéder à un contrôle de la distribution des rôles. Dans certaines sociétés (petites), cette séparation n'est pas effective.

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
6) Processus de traitement des réclamations clients	Direction commerciale Direction juridique Service Après-vente	Ce processus concerne la notification et la résolution des problèmes en interne ou avec le client : Quantité / Produit / Qualité / Prix / problèmes de facturation / Erreurs de livraisons / Conditions de paiement Le système doit être configuré pour permettre de classifier les factures d'avoir et d'analyser les points suivants : erreurs de prix, erreurs de quantité, problèmes de qualité, livraisons tardives ou incomplètes, etc. **Point de départ / Point de clôture** Plainte du client Résolution du problème	Les avoirs ne sont pas exacts (mauvais montant, client, etc) Les avoirs ne sont pas correctement enregistrés (mauvaise classification) Les avoirs ne sont pas correctement engagés (mauvaise période, mauvais montant, etc) L'impact financier des réclamations n'est pas reporté dans les temps à la direction financière Des engagements non autorisés sont passés avec des clients Des avoirs non autorisés / illégaux sont passés avec des clients Perte de clients due à un processus tardif ou inefficace de gestion des réclamations Pas de politique claire de réclamation Entreprise mal organisée pour gérer de manière appropriée les plaintes clients (manque de ressources humaines et de bases de données pour suivre les plaintes) Pas de processus clair et partagé de résolution des incidents Gaspillage de temps et de ressources dans la résolution du problème Mauvaise définition du processus de réclamation / divergence ou mauvaise application du processus Risque de réputation Risque contentieux Gestion des retours	*2.3.6.8) Tous les comptes clients ouverts correspondent à des clients réels.* Exemples - Il n'y a pas de clients génériques. Comme pour les achats, il existe des états qui permettent d'obtenir les historiques des changements, modifications … - Surveillance de la part de chaque client dans le total des ventes, pour identifier/limiter les risques de dépendance - Bonne pratique – contrôle une fois par mois (ou trimestre selon le type d'activité, les gammes de produits, les clients) *2.3.6.9) Les soldes de comptes sont périodiquement et correctement justifiés.* Exemples - Les balances clients (auxiliaires et générales) sont régulièrement suivies. Les balances âgées permettent de suivre l'évolution des créances clients. - Bonne pratique - Une fois par mois *2.3.6.10) Les clients douteux sont correctement identifiés et les risques d'insolvabilité comptabilisés en conformité avec les règles applicables.* Exemples - Il existe des comptes généraux clients douteux. Il est possible de faire des provisions et de les rattacher à ces comptes clients spécifiques. Les pratiques diffèrent. Certaines entreprises font des provisions au niveau d'un compte général, d'autres au niveau des comptes clients. - Bonne pratique – une fois par mois (ou trimestre selon le type d'activité) pour faire évoluer les provisions

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
7) Gestion du pricing / tarification	Direction Marketing Direction Commerciale Contrôle de gestion	Ce processus comprend 1) Définition de la structure de prix et les ajustements Les ajustements peuvent avoir trait à : - Différenciation produit - Différenciation Service - Segmentation marché - Promotions (pour un nouveau produit) - Services logistique - Changement des prix (hausse ou baisse) NB: ces ajustements peuvent résulter de plusieurs types de transaction : Rabais, Discounts, Produits gratuits, Changement de prix 2) Définition des étapes d'approbation pour tout changement de prix. 3) Entrée de la structure de prix et des ajustements dans le système, de façon à ce que le prix soit automatiquement calculé quand les bons de commandes et les factures sont générés. **Point de départ / Point de clôture** Définition de la structure de la base de prix et des ajustements - Feedback clients - Market intelligence (segmentation) - Stratégie Marketing (promotions, nouveaux produits, logisitique, import / export, etc.) Le catalogue de prix est approuvé et entré dans la table de prix Notification au client	Les engagements liés aux discounts et rabais ne sont pas correctement calculés Des engagements non autorisés sont faits avec des clients Pas d'information correcte sur les prix pour chaque client Erreur dans le calcul des discounts et rabais Non conformité aux lois et réglementations commerciales Erreur dans les prix communiqués aux clients Manque d'influence sur la place de marché – manque de crédibilité Perte de clients liée à une mauvaise relation client / communication Pas de prise en compte de l'évolution des prix du marché (matières premières, etc.)	*2.3.6.11) Enfin, il existe un dispositif visant à exclure des produits des activités ordinaires, les produits facturés ou à facturer pour compte d'autrui.* Exemples - Il n'y a rien dans le plan comptable, ni dans les systèmes. *2.3.6.12) Il existe une procédure permettant de s'assurer que les produits et charges ont été enregistrés sur la bonne période.* Exemples - Voir point 2 pour la *billing due list*. Dans les documents Marketing et Ventes figurent les différentes dates (facturation, livraison …) - Bonne pratique – une fois par mois *2.3.6.13) Il existe un dispositif permettant d'enregistrer les factures à émettre ou les produits constatés d'avance de manière exhaustive et exacte.* Exemples - A partir de la *billing due list*, il est possible de faire une valorisation par centres de profits et de coûts, de faire le suivi et les enregistrements. - Bonne pratique – une fois par mois

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Produits des activités ordinaires / Clients et assimilés
				2.3.6.14) Les provisions pour dépréciation sont revues en vue de leur ré-estimation, le cas échéant (par exemple sur la base d'une balance âgée, ou des informations les plus récentes sur les litiges avec les clients). Exemples - La balance âgée permet d'obtenir le montant des créances en retard. Plusieurs autres balances existent dont celles des postes clients qui permettent de connaître l'origine des litiges et les raisons des provisions. Il y a des comptes de provisions liés aux ventes. - Bonne pratique – identique au point 2.3.6.8 (mois ou trimestre) la pratique dépend aussi de la manière dont sont traitées les provisions et s'il y a beaucoup de mauvais payeurs - Bonne pratique – *billing due list* – transaction pour factures passées dans le système comptable (en module finance) Autres contrôles (étape 7 du processus – gestion du pricing et tarification) - Produits financiers de couverture des changes - Approbation du catalogue des prix - Validation et traçabilité des ajustements - Contrôles bloquants pour vérifier la cohérence et l'exhaustivité des données et des contrôles arithmétiques automatiques.

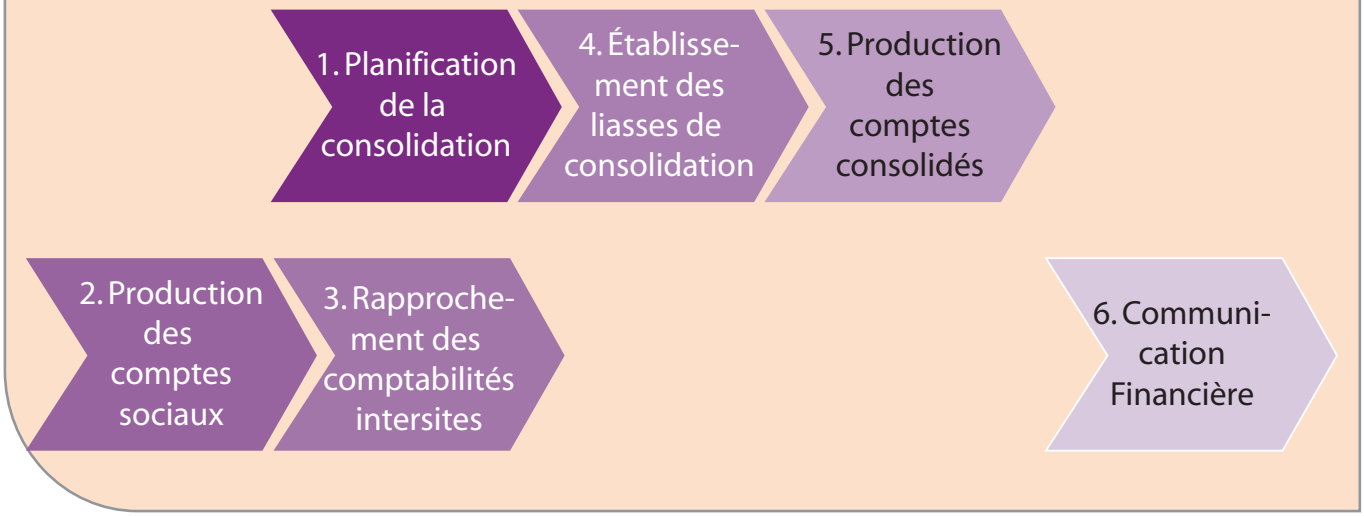
4.6. Description du processus consolidation financière

4.6.1. Processus

Le processus de consolidation financière se découpe en cinq étapes, résumées dans le graphique ci-dessous. Le processus de communication financière (étape 6) est un processus décrit séparément dans le cadre de référence AMF. Nous le faisons figurer ici uniquement à titre indicatif. Il n'est pas détaillé par la suite en termes d'acteurs, de risques, de points de contrôle ni de contrôle.

Figure 24 : Description du processus consolidation financière

Source : CIGREF - IFACI

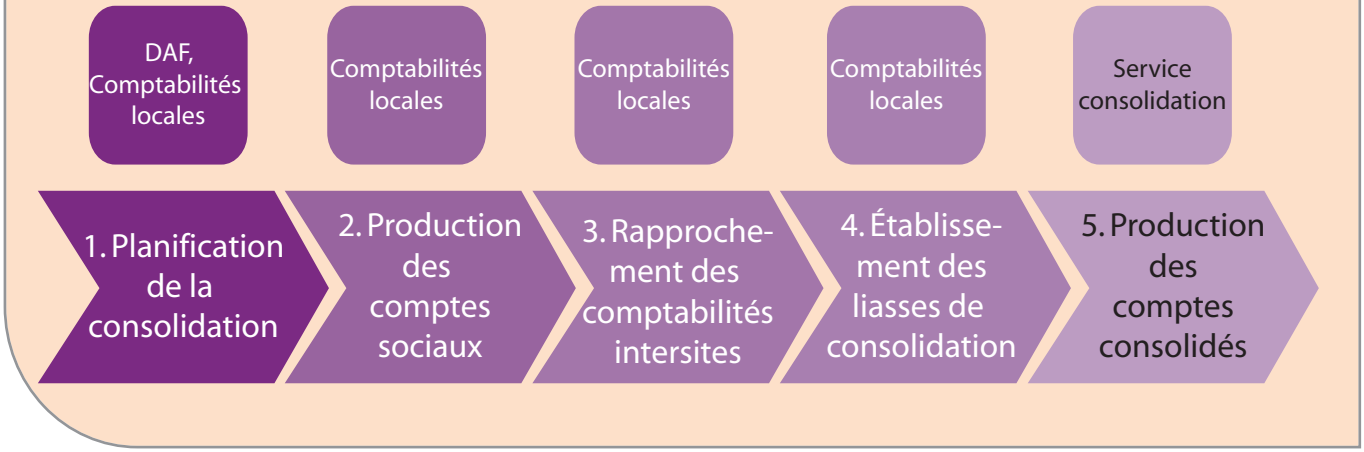


4.6.2. Acteurs

Les acteurs impliqués par étapes sont décrits dans le schéma ci-dessous.

Figure 25 : Acteurs impliqués par étape du processus consolidation financière

Source : CIGREF - IFACI

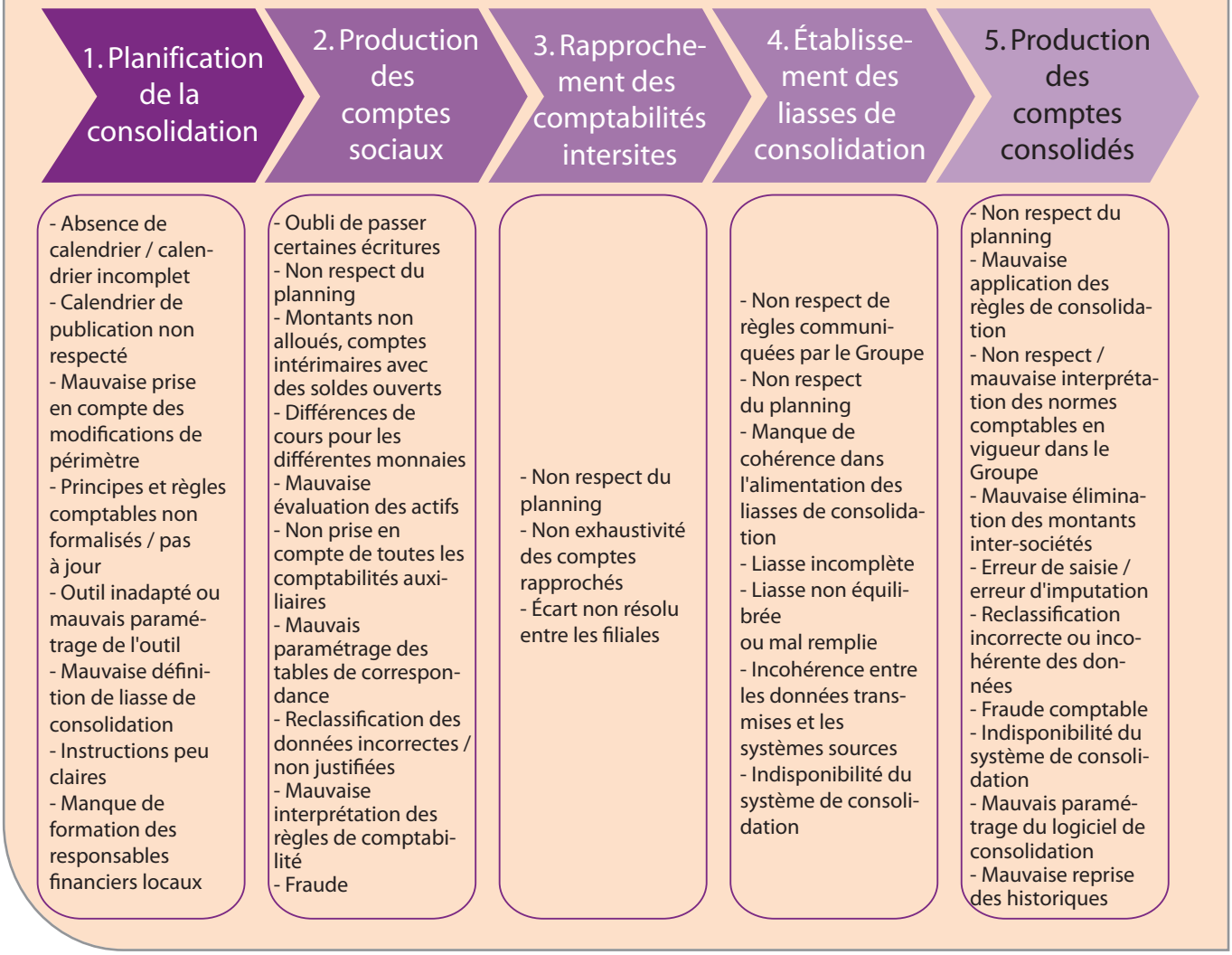


4.6.3. Risques

Les risques portent principalement sur des non-connaissances de règles, le non-respect des calendriers, des erreurs d'évaluation, des erreurs de paramétrage, des risques de fraude.

Figure 26 : Risques par étape du processus consolidation financière

Source : CIGREF - IFACI

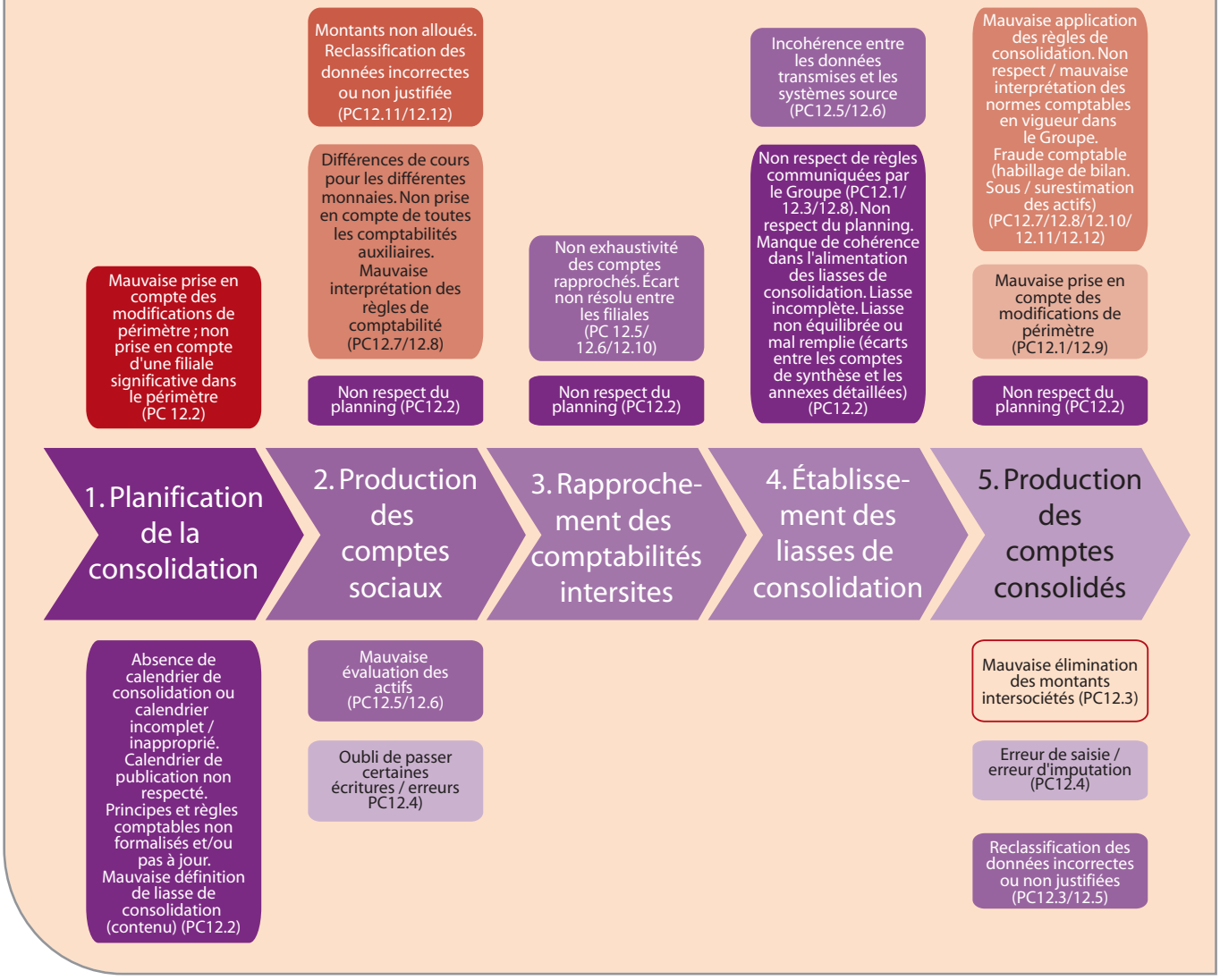


4.6.4. Rapprochement entre risques et points de contrôle AMF

Le schéma ci-dessous relie les risques aux points de contrôle décrits dans le cadre de référence AMF. Chaque entreprise peut avoir une démarche spécifique et relier ses propres risques aux différents points de contrôle.

Figure 27 : Rapprochement entre risques et points de contrôles AMF

Source : CIGREF - IFACI



4.6.5. Rappel des principaux points de contrôle du guide d'application AMF

Le tableau ci-dessous reprend les principaux points de contrôle tels que listés dans le guide d'application du cadre de référence AMF.

Figure 28 : Rappel des principaux points de contrôle liés au processus consolidation financière

Source : Cadre de référence AMF (chap 2 - p48)

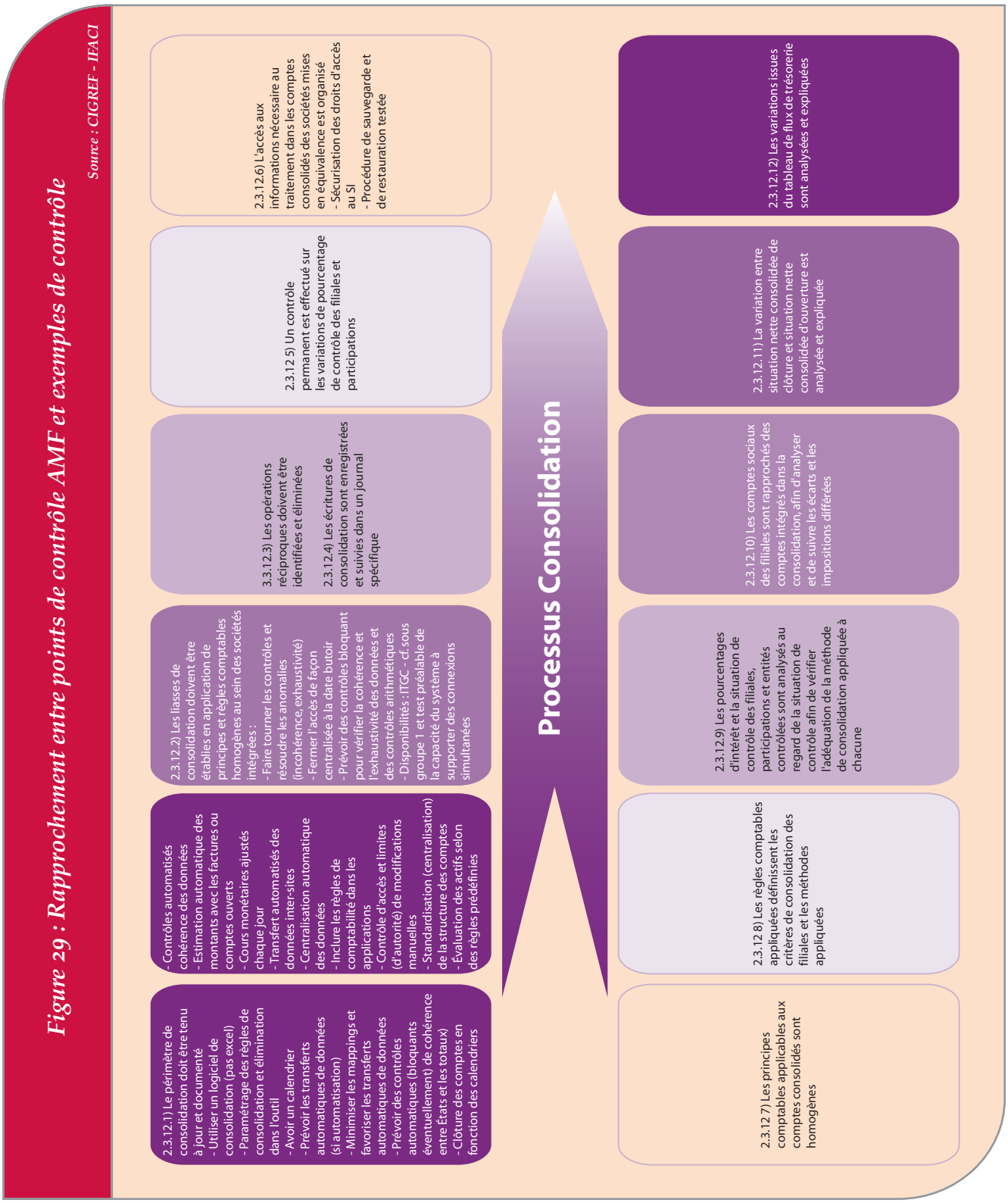
N° de §	Nom de l'opération
2.3.12	**Consolidation**
2.3.12.1	Le périmètre de consolidation est tenu à jour et documenté
2.3.12.2	Les liasses de consolidation sont établies en application de principes et règles comptables homogènes au sein des sociétés intégrées.
2.3.12.3	Les opérations réciproques sont identifiées et éliminées, en particulier les opérations financières et les résultats internes (marges sur stocks, dividendes, résultats sur cessions d'immobilisations…).
2.3.12.4	Les écritures de consolidation sont enregistrées et suivies dans un journal spécifique.
2.3.12.5	Un contrôle permanent est effectué sur les variations de pourcentage de contrôle des filiales et participations afin que les traitements appropriés puissent être mis en œuvre lors des arrêtés de comptes (périmètre de consolidation, modification de la méthode de consolidation…).
2.3.12.6	L'accès aux informations nécessaires au traitement dans les comptes consolidés des sociétés mises en équivalence est organisé.
2.3.12.7	Les principes comptables applicables aux comptes consolidés sont homogènes.
2.3.12.8	Les règles comptables appliquées définissent les critères de consolidation des filiales et les méthodes appliquées.
2.3.12.9	Les pourcentages d'intérêt et la situation de contrôle des filiales, participations et entités contrôlées sont analysés au regard de la situation de contrôle afin de vérifier l'adéquation de la méthode de consolidation appliquée à chacune.
2.3.12.10	Les comptes sociaux des filiales sont rapprochés des comptes intégrés dans la consolidation, afin d'analyser et de suivre les écarts et les impositions différées.
2.3.12.11	La variation entre situation nette consolidée de clôture et situation nette consolidée d'ouverture est analysée et expliquée.
2.3.12.12	Les variations issues du tableau de flux de trésorerie sont analysées et expliquées.

4.6.6. Rapprochement entre points de contrôle AMF et exemples de contrôle

Le schéma ci-dessous propose un rapprochement entre points de contrôle AMF et exemples de contrôles. Il s'agit d'exemples de contrôle, à titre d'illustration. La liste n'est pas exhaustive.

Figure 29 : Rapprochement entre points de contrôle AMF et exemples de contrôle

Source : CIGREF - IFACI



4.6.7. Vue détaillée du processus consolidation financière

Figure 30 : Vue détaillée du processus consolidation financière

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Consolidation financière
1) Planification de la consolidation	Consolidation centrale	1. Préparation du calendrier de consolidation 2. Définition du périmètre consolidable 3. Rédaction des principes et règles comptables à suivre 4. Paramétrage du logiciel de consolidation 5. Définition des tables de correspondance des comptes et des éléments statistiques 6. Envoi des instructions de consolidation à destination de l'ensemble des filiales en précisant les nouveautés en terme comptable et de reporting sur la période et le calendrier des opérations pour la clôture	Absence de calendrier de consolidation ou calendrier incomplet / inapproprié Calendrier de publication non respecté Mauvaise prise en compte des modifications de périmètre Principes et règles comptables non formalisés et/ou pas à jour Outil inadapté ou mauvais paramétrage de l'outil Mauvaise définition de liasse de consolidation (contenu) Instructions peu claires ou peu compréhensibles Manque de formation des responsables financiers locaux	*2.3.12.1) Le périmètre de consolidation doit être tenu à jour et documenté.* - Utiliser un logiciel de consolidation (pas excel) - Paramétrage des règles de consolidation et d'élimination dans l'outil - Avoir un calendrier - Prévoir les transferts automatiques de données (si automatisation) - Minimiser les mappings, et favoriser les transferts automatiques de données - Clôture des comptes en fonction du calendrier incluant les différentes tâches à accomplir - Contrôles automatisés de la cohérence des données en amont (vérification de seuils limites, cohérence, etc.) - Cours monétaires ajustés chaque jour et réconciliation des différences de taux de change. - Centralisation automatique des données. Vérification de la cohérence des données et reclassification si nécessaire - Inclure les règles de comptabilité dans les applications (avec des contrôles et des rapports d'exception de non-respect) - Contrôle d'accès et limites (d'autorité) de modifications manuelles - Standardisation (centralisation) de la structure des comptes et vérification que les entités ne génèrent pas de propres comptes auxiliaires inconnus. - Evaluation des actifs selon des règles prédéfinies ou calculés automatiquement par une source externe - Le rapprochement intercos peut être fait via le logiciel de consolidation ce qui facilite le processus
2) Production des comptes sociaux (en amont)	DAF filiale, Comptabilité locale	1. Ecritures d'arrêté des comptes (Ecritures de régularisation, valorisation des immobilisations, stocks et investissements, évaluation des participations, conversion…) 2. Clôture des comptabilités auxiliaires dans les différentes entités. 3. Centralisation dans le grand livre 4. Vérification des opérations de centralisation (soldes, devises,…) 5. Analyse et production des comptes sociaux.	Oubli de passer certaines écritures / erreurs Non respect du planning Montants non alloués, comptes intérimaires avec des soldes ouverts Mauvaise évaluation des actifs Non prise en compte de toutes les comptabilités auxiliaires Mauvais paramétrage des tables de correspondance (comptes) Reclassification des données incorrecte ou non justifiée Mauvaise interprétation des règles de comptabilité Fraude (manipulation des donnés comptables et financières)	

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Consolidation financière
3) Rapprochement des comptabilités inter filiales (en amont)	DAF filiale, Comptabilité locale	En amont, un rapprochement est effectué entre toutes les entités du groupe de leurs comptes inter compagnies (comptes de bilan et du compte de résultat : produits/charges) pour permettre leur élimination lors du processus de consolidation.	Non respect du planning Non exhaustivité des comptes rapprochés Ecart non résolu entre les filiales	*2.3.12.2) Les liasses de consolidation doivent être établies en application de principes et règles comptables homogènes au sein des sociétés intégrées.* - Paramétrage des règles de consolidation et d'élimination dans l'outil - Cours monétaires ajustés chaque jour et réconciliation des différences de taux de change - Standardisation (centralisation) de la structure des comptes et vérification que les entités ne génèrent pas de propres comptes auxiliaires inconnus - Evaluation des actifs selon des règles prédéfinies ou calculés automatiquement par une source externe - Exécuter les contrôles et résoudre les anomalies (incohérences, exhaustivité) - Fermer l'accès de façon centralisée à la date butoir - Prévoir des contrôles bloquants pour vérifier la cohérence et l'exhaustivité des données et des contrôles arithmétiques automatiques *2.3.12.3)Les opérations réciproques doivent être identifiées et éliminées, en particulier les opérations financières et les résultats internes (marges sur stocks, dividendes, résultats sur cessions d'immobilisations…).* - Le rapprochement intercos peut être fait via le logiciel de consolidation ce qui facilite le processus - Analyse des écarts au-dessus des seuils prédéfinis
4) Etablissement des liasses de consolidation	DAF filiale, Comptabilité locale	1. Alignement du calendrier local en fonction du calendrier Groupe 2. Transfert des données des différents systèmes dans le système de consolidation (par saisie manuelle ou interface automatique) et saisie des autres données 3. Rapprochement des soldes de comptes transférés avec les systèmes source et test de cohérence des données transmises.	Non respect de règles communiquées par le Groupe Non respect du planning Manque de cohérence dans l'alimentation des liasses de consolidation Liasse incomplète Liasse non équilibrée ou mal remplie (écarts entre les comptes de synthèse et les annexes détaillés) Incohérence entre les données transmises et les systèmes source Indisponibilité du système de consolidation	

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Consolidation financière
5) Production de comptes consolidés	Consolidation centrale	1. Opérations d'élimination des opérations inter-sociétés 2. Ajustements et reclassifications nécessaires pour assurer la conformité aux normes Groupe 3. Production d'analyses et de reporting 4. Données réelles sont comparés aux données prévisionnelles 5. Vérification de la cohérence des données entre les différents états de consolidation, etc. 6. Rédaction de l'annexe aux comptes consolidés	Non respect du planning Mauvaise application des règles de consolidation Non respect/mauvaise interprétation des normes comptables en vigueur dans le Groupe Mauvaise élimination des montants inter-sociétés Erreur de saisie /Erreur d'imputation Manque d'analyse et/ou communication d'informations incorrecte ou incohérente. Fraude comptable (habillage de bilan, Sous- / Surestimation des actifs) Indisponibilité du système de consolidation Mauvais paramétrages du logiciel de consolidation Mauvaise reprise des historiques	*2.3.12.4) Les écritures de consolidation sont enregistrées et suivies dans un journal spécifique : distinguer ou avoir plusieurs journaux par type d'écriture.* *2.3.12.5) Un contrôle permanent est effectué sur les variations de pourcentage de contrôle des filiales et participations afin que les traitements appropriés puissent être mis en œuvre lors des arrêtés de comptes (périmètre de consolidation, modification de la méthode de consolidation…).* - analyse de la variation de la situation nette comptable consolidée (si possible automatisé) *2.3.12.6) L'accès aux informations nécessaires au traitement dans les comptes consolidés des sociétés mises en équivalence est organisé.* *2.3.12.7) Les principes comptables applicables aux comptes consolidés sont homogènes.* - Inclure les règles de comptabilité dans les applications (avec des contrôles et des rapports d'exception de non-respect) *2.3.12.8) Les règles comptables appliquées définissent les critères de consolidation des filiales et les méthodes appliquées.*

Etape	Acteurs	Description	Risques	Exemple de contrôles applicatifs Contrôles transversaux au processus Cadre de référence AMF : Consolidation financière
				2.3.12.9) Les pourcentages d'intérêt et la situation de contrôle des filiales, participations et entités contrôlées sont analysés au regard de la situation de contrôle afin de vérifier l'adéquation de la méthode de consolidation appliquée à chacune. *2.3.12.10) Les comptes sociaux des filiales sont rapprochés des comptes intégrés dans la consolidation, afin d'analyser et de suivre les écarts et les impositions différées.* - Prévoir des contrôles automatiques (bloquants éventuellement) de cohérence (entre les états et les totaux) - Contrôles automatisés de la cohérence des données en amont (vérification de seuils limites, cohérence, etc.) - Tableau de passage situation nette - conso *2.3.12.11) La variation entre situation nette consolidée de clôture et situation nette consolidée d'ouverture est analysée et expliquée.* *2.3.12.12) Les variations issues du tableau de flux de trésorerie sont analysées et expliquées.*

5. Le contrôle interne de la DSI

A l'instar des autres métiers, la DSI doit mettre en œuvre un dispositif de contrôle interne lui permettant de maîtriser ses risques pour atteindre ses objectifs opérationnels. Les objectifs du contrôle interne, pour la DSI comme pour toute autre fonction, sont :

- la conformité aux instructions de la direction générale, aux lois et règlements ;
- l'efficacité des opérations, en particulier à travers l'utilisation optimale des ressources affectées et la maîtrise des processus ;
- l'identification, l'analyse et l'évaluation des risques ;
- la sécurité des personnes, la sauvegarde des actifs et la protection des données ;
- la qualité de l'information financière, opérationnelle et de gestion.

Les spécificités de l'informatique, liées à sa technicité et à sa transversalité, donnent une dimension particulière au contrôle interne de la DSI.
Selon le cadre de référence de contrôle interne de l'AMF, le dispositif de contrôle interne doit prévoir :

1. une organisation comportant une définition claire des responsabilités et s'appuyant sur des systèmes d'informations, des procédures et des pratiques appropriées ;
2. la diffusion en interne d'informations pertinentes et fiables ;
3. un système de recensement et d'analyse des principaux risques et des procédures de gestion de ces risques ;
4. des activités de contrôle proportionnées aux enjeux ;
5. une surveillance du dispositif de contrôle interne.

Ces principes doivent être appliqués dans les DSI. Leur mise en œuvre est évaluée pour donner une assurance sur l'efficacité du contrôle interne et identifier des pistes de progrès.

5.1. Objectifs

Ce chapitre fournit :

- une illustration de l'application des objectifs et des composantes du cadre de référence de l'AMF au contrôle interne de la DSI ;
- une synthèse des préalables nécessaires à la mise en place d'un dispositif de contrôle interne efficace au sein d'une DSI ;
- une description de six processus représentatifs des activités d'une DSI, ainsi qu'une définition du rôle des principaux acteurs concernés par ces processus ;
- des guides d'évaluation à destination des DSI, des contrôleurs internes et des auditeurs internes. Ils facilitent la coopération entre les fonctions et permettent de vérifier le degré de maîtrise des processus.

5.2. Périmètre retenu

Six processus ont été sélectionnés, car ils contribuent puissamment à l'atteinte des objectifs de contrôle interne rappelés précédemment :

- gestion des compétences ;
- projet et développement ;
- maintenance et gestion des changements ;
- sécurité logique et gestion des accès physiques ;
- gestion des incidents ;
- contrats d'infogérance et pilotage de la sous-traitance.

Le tableau de concordance figurant en annexe 3 permet d'établir une relation entre ces processus et les objectifs de contrôle issus du cadre de référence de l'AMF.

Cependant, cette analyse n'est pas exhaustive. Ainsi, la continuité d'exploitation n'est pas traitée, et la gouvernance des systèmes d'information est partiellement abordée dans le processus de gestion de projets. Bien que ces domaines jouent un rôle important dans le contrôle interne de la DSI, le groupe de travail a préféré appliquer le principe de réalité en privilégiant la richesse du retour d'expérience sur un nombre limité de processus.

Le tableau ci-après précise le périmètre d'analyse de chaque processus. Enfin, les interfaces éventuelles avec d'autres processus sont identifiées.

Processus	Périmètre	Projet et développement	Maintenance et gestion des changements	Gestion des incidents	Gestion de la sécurité logique et des accès physiques	Gestion de la sous-traitance
Gestion des compétences	Gestion spécifique des compétences critiques (garantissant la réussite du SI) et des compétences clés (critiques et rares sur le marché)			✓		
Projet et développement	Maîtrise des projets de développement informatique y compris la conduite du changement		✓		✓	✓
Maintenance et gestion des changements	Maintenance et gestion des changements (applicatifs et techniques)	✓		✓		✓
Gestion des incidents	Gestion et résolution des incidents touchant les applicatifs, les systèmes, la sécurité …		✓		✓	✓
Gestion de la sécurité logique et des accès physiques	Environnement de contrôle interne et mise en œuvre de la politique de sécurité des SI	✓		✓		
Gestion de la sous-traitance	Maîtrise des services fournis par des prestataires externes dans les SI tant en projets, en maintenance qu'en exploitation	✓	✓	✓		

5.3. Démarche suivie et principaux livrables

Les travaux se fondent sur une approche par les risques. Pour chaque processus, le groupe de travail a procédé à l'identification des :

- sous-processus et étapes clés ;
- acteurs et de leur responsabilité respective ;
- risques associés à chaque étape-clé ;
- activités de contrôle permettant la maîtrise du risque identifié ;
- bonnes pratiques à partir des référentiels existants et du retour d'expérience des contributeurs, ce qui donne un caractère opérationnel aux documents produits.

Les six processus étudiés correspondent bien à la nomenclature CobiT et ces travaux sont compatibles avec les grands référentiels comme Val IT, ITIL, CMMI, ISO, eSCM…

Thème	Référentiels utilisés	Processus CobiT
Projet et développement	**VAL IT** **ITIL**	PO5 : Gérer les investissements informatiques PO9 : Evaluer et gérer les risques PO10 : Gérer les projets AI1 : Trouver des solutions informatiques AI2 : Acquérir des applications et en assurer la maintenance AI4 : Faciliter le fonctionnement et l'utilisation AI5 : Gérer les changements AI7 : Installer et valider les solutions et les modifications DS1 : Définir et gérer les niveaux de services DS6 : Identifier et imputer les coûts DS11 : Gérer les données DS12 : Gérer l'environnement physique
Maintenance et gestion des changements	**IIA/GTAG 2 : Change and patch management controls**	PO4 : Définir les processus, l'organisation et les relations de travail AI2 : Acquérir des applications et en assurer la maintenance AI6 : Gérer les changements AI7 : Installer et valider les solutions et les modifications
Sécurité logique et gestion des accès physiques	**ISO 27001**	DS5 : Assurer la sécurité des systèmes DS12 : Gérer l'environnement physique
Contrats d'infogérance et pilotage de la sous-traitance	**eSCM**	DS2 : Gérer les services tiers
Gestion des incidents	**ITIL** **Soutien des services/ Gestion des incidents**	DS8 : Gérer le service d'assistance client et les incidents
Gestion des compétences		PO7 : Gérer les ressources humaines de l'informatique

Les résultats des travaux sont structurés dans trois catégories de livrables qui sont cohérents entre eux tout en donnant un éclairage particulier sur le processus concerné.

- Le **flowchart** constitue l'une des valeurs ajoutées de ces travaux. Il schématise les flux d'informations ainsi que les activités qui relient les étapes clés et les acteurs. Ce document donne une bonne compréhension des activités ;
- le **RACI**[1] clarifie les responsabilités respectives des acteurs concernés et illustre l'évolution de ces responsabilités à chaque étape ; ce tableau est illustré par les principaux livrables qui constituent des preuves tangibles de la maîtrise des risques ;
- la **matrice risques/contrôles** avec le format suivant :
  - sous-processus (le cas échéant) ;
  - étapes-clés ;
  - référence à un référentiel existant (CobiT, ITIL, ISO...) ;
  - objectifs de contrôle ;
  - risque ;
  - activité de contrôle ;
  - bonnes pratiques.

Cette matrice est suffisamment opérationnelle pour mettre en œuvre le dispositif de contrôle ou pour procéder à son évaluation. Elle devrait contribuer à l'amélioration de l'efficacité des activités de la DSI et faciliter la comparaison des pratiques.

5.4. Les préalables au contrôle interne de la DSI

Le dispositif de contrôle interne de la DSI nécessite la préexistence d'un contexte favorable au bon déploiement du dispositif et à son amélioration continue.

Un de ces préalables consiste à avoir un niveau adéquat de sponsorisation du dispositif. A ce propos, le cadre de référence de l'AMF préconise que la direction générale se tient régulièrement informée des dysfonctionnements, des insuffisances et des difficultés d'application, voire des excès, et veille à l'engagement des actions correctives nécessaires. Ce principe général doit être adapté en fonction des enjeux du contrôle interne dans la DSI.

L'efficacité du dispositif requiert l'application de règles du jeu telles que :

- l'adoption et la communication d'une politique SI ;
- une déclinaison de cette politique en objectifs de contrôle permettant d'évaluer la réalité de son déploiement et son efficacité ;
- une méthodologie orientée sur les risques qui facilite la définition et la priorisation des activités de contrôle ;
- une définition des responsabilités et des pouvoirs assurant une séparation adéquate des tâches ; elle est retranscrite dans les droits des utilisateurs et permet la gestion des flux d'information en fonction des responsabilités ;
- la surveillance de l'application des politiques et des standards.

[1] *Le modèle RACI est un modèle qui permet de décrire les rôles et responsabilités des acteurs au sein d'une organisation, sur un processus donné. RACI définit 4 rôles - R: Responsible ou Réalisateur, A: Accountable ou Approbateur C: Consulted ou Consulté, I: Informed ou Informé.*

Ces préalables sont retranscrits au niveau de chaque processus analysé.

La question du contrôle interne de la DSI renvoie spontanément aux politiques liées aux infrastructures et aux applications. Pourtant, dans un contexte de raréfaction des ressources et de tension sur le marché des professionnels du SI, il convient de porter une attention particulière à la **gestion des compétences** et au contrôle de la **sous-traitance**. La continuité des compétences doit être assurée par un pilotage des rôles critiques et des rôles clés de la DSI. Il est guidé par la politique RH de l'entreprise et le schéma directeur des SI. La stratégie de *sourcing* concerne les processus centraux de la DSI (réalisation, maintenance, exploitation, sécurité). De ce fait, l'exécution et le pilotage des contrats tiers nécessitent des politiques (RH SI, Achats, Schéma directeur SI…) et des règles clairement définies.

De même, pour mener à bien un **projet informatique**, il est indispensable d'adopter et d'appliquer des principes de bonne gouvernance comme la surveillance permanente de l'alignement des projets SI avec la stratégie et les priorités de l'entreprise. En pratique, les projets sont priorisés par un comité d'investissements qui fonde sa décision sur une analyse des enjeux, des investissements et des risques. La validation des jalons essentiels du projet (expression des besoins, lancement, tests, recettes) est systématisée. La conduite du changement (analyse d'impacts, communication, formation, soutien et reprise des données) doit être engagée le plus en amont possible.

La maîtrise de la **maintenance** des applications exige une adéquation continue des fonctionnalités avec les besoins des métiers. Cette bonne gestion répond également à des impératifs de coût, de qualité et de sécurité. L'efficacité de ce dispositif repose sur la documentation et l'application d'un plan stratégique de maintenance, et des règles de gestion des changements qui prévoient les situations d'urgence ainsi que la séparation effective des tâches notamment entre le développement et l'exploitation.

La **gestion des incidents** doit être effectuée dans un contexte caractérisé par la multiplication des technologies et l'hétérogénéité de plateformes toujours plus interconnectées. Ce processus nécessite l'utilisation d'une méthodologie préalablement définie pour l'identification des causes de l'incident et la maîtrise de la cascade d'événements qui pourrait être générée par cet incident. Il convient notamment de mettre en place des dispositifs automatiques de surveillance des matériels, réseaux, systèmes d'exploitation, bases de données et applicatifs critiques.

Le processus lié à la **sécurité logique** et à **la gestion des accès physiques** garantit des données intègres, en empêche une divulgation inappropriée et supporte la continuité de l'activité de l'entreprise. La politique de sécurité précise les vulnérabilités identifiées et les objectifs de protection. Pour avoir des niveaux de protection proportionnés aux enjeux, il faut s'appuyer sur les résultats de la qualification des informations.

Les actions engagées au sein de la DSI doivent être cohérentes avec les autres démarches de contrôle interne engagées dans l'organisation.

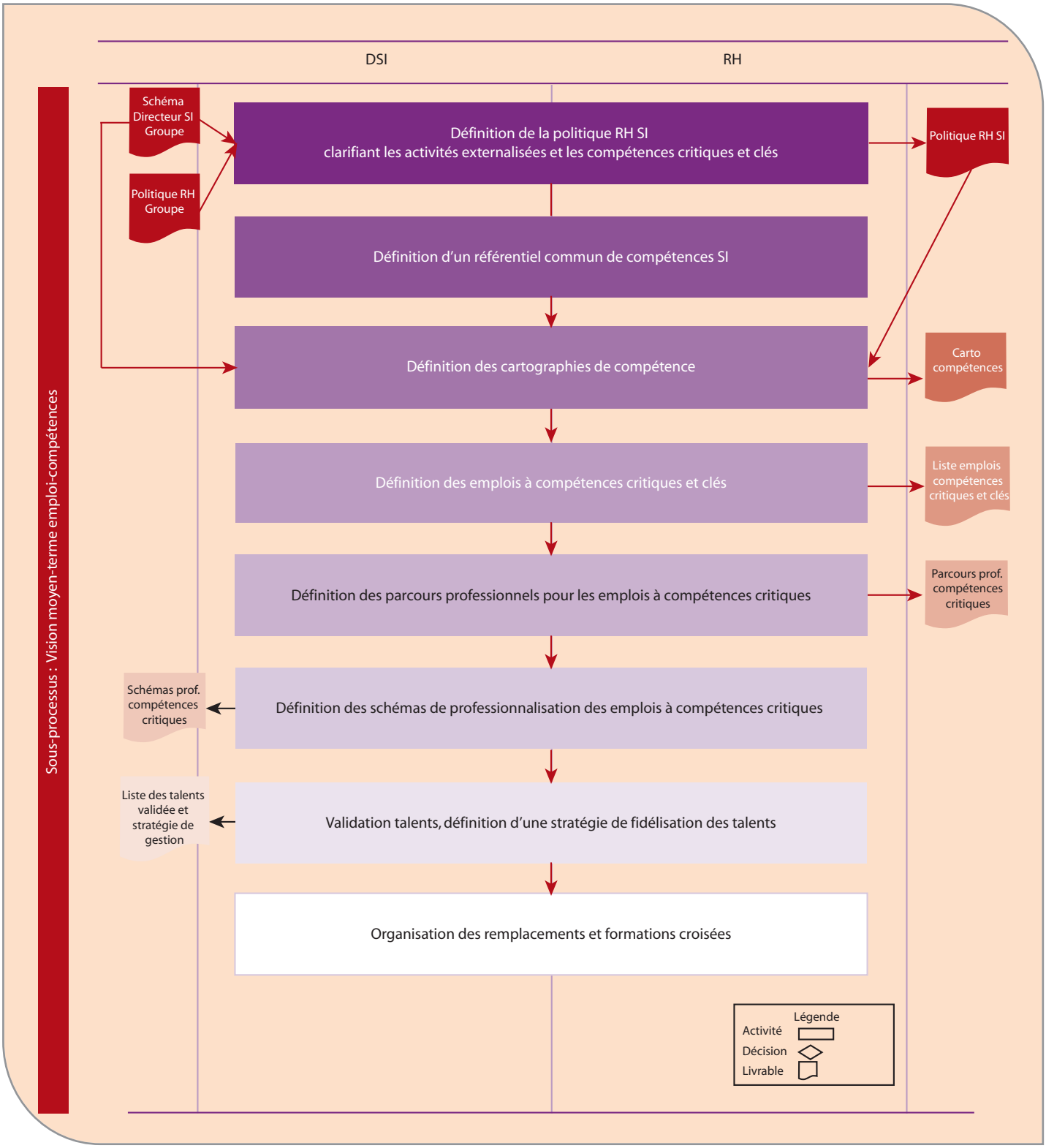
5.5. Gestion des compétences

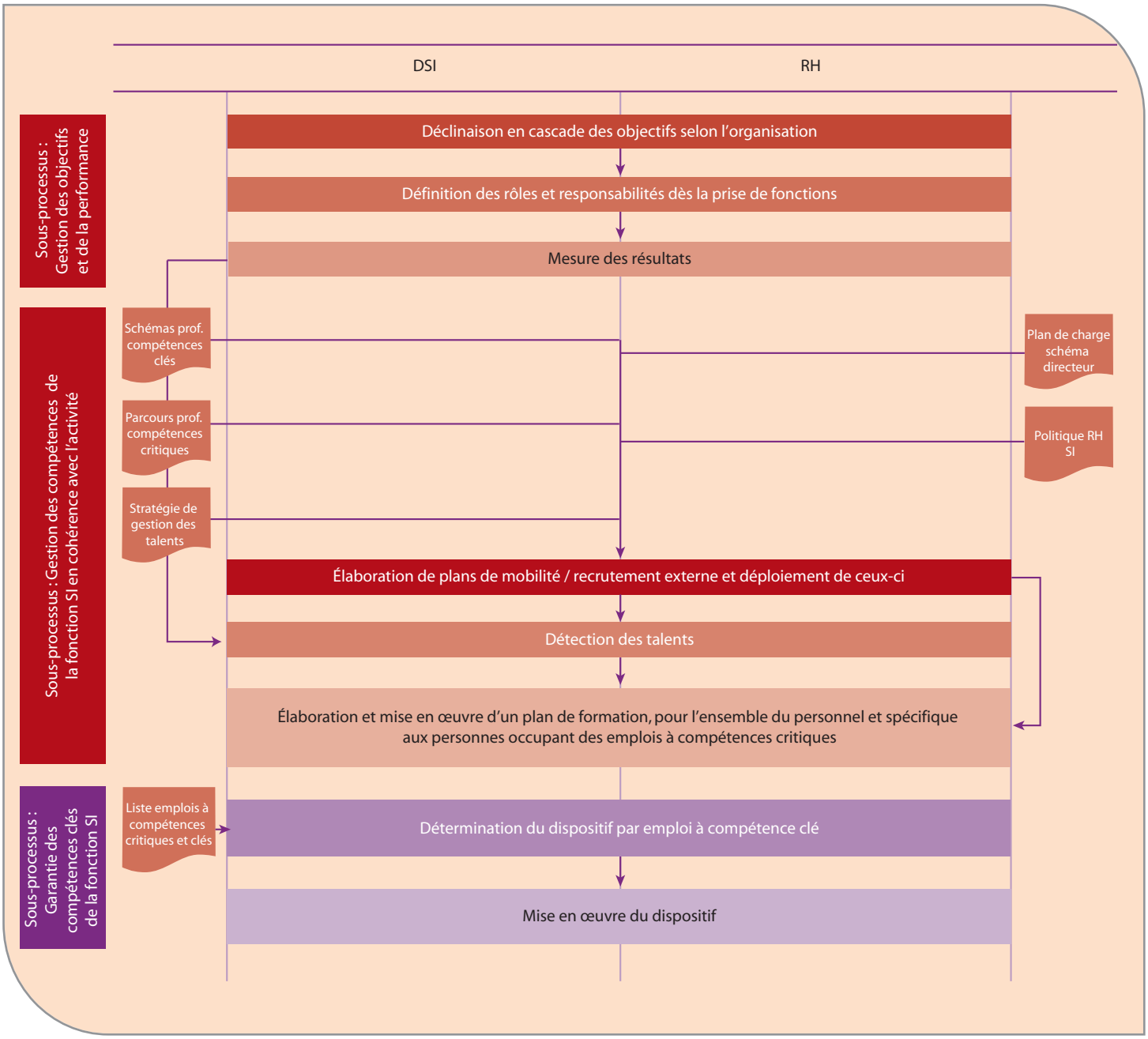
La gestion des compétences dans le domaine informatique est une constante depuis la montée en puissance des systèmes d'information dans tous les métiers de l'entreprise et de l'administration, et en parallèle depuis la tension sur la disponibilité des ingénieurs et techniciens informatiques. En réalité, derrière « gestion des compétences » se profile un pilotage des rôles, et en particulier des rôles critiques (essentiels pour le bon fonctionnement de la DSI, et a priori non externalisables) et des rôles clés (rôles critiques particulièrement rares sur le marché).

La gestion des rôles est donc la traduction concrète, au sein d'une DSI, de la gestion globale des talents dans l'organisation. Mais pourquoi une gestion des compétences spécifique à l'informatique par rapport aux autres services ? Parce que la diffusion du système d'information dans tous les processus métiers de l'entreprise ou de l'administration s'est doublée de la rareté des ressources disponibles, le rendant critique et rendant toute l'organisation vulnérable à sa criticité. De même que l'on travaille sur la continuité des infrastructures à travers des plans de secours et de reprise d'activité, de même il convient de travailler sur la continuité des compétences.

La gestion des compétences informatiques se fonde sur deux préalables : une politique RH globale dans l'entreprise, et un schéma directeur des SI. Leur combinaison débouche sur une politique RH SI dont la définition et la mise en œuvre sont décrites dans le processus ci-après.

5.5.1. Flowchart du processus de gestion des compétences de la DSI





5.5.2. RACI du processus de gestion des compétences de la DSI

Etape clé	DSI	DRH	Livrables majeurs de sortie	Commentaires
Sous-processus : Vision moyen-terme emploi-compétences				
Définition d'une politique RH SI, clarifiant les activités externalisées et les compétences critiques clés	A	R	Politique RH SI	
Définition d'un référentiel commun de compétences SI	A	R	Référentiel Groupe mis à jour et plan de communication associé	
Définition des cartographies de compétences	A	R	Cartographie des compétences	
Définition des emplois à compétences critiques et clés	A	R	Liste des compétences critiques et clés	
Définition des parcours professionnels pour les emplois à compétences critiques	A	R	Définition des parcours professionnels des compétences critiques	
Définition des schémas de professionnalisation des emplois à compétences critiques	A	R	Schémas de professionalisation des emplois à compétences critiques	
Validation talents, définition d'une stratégie de fidélisation des talents	A	R	Liste des talents validée et stratégie de gestion	
Organisation des remplacements et formations croisées	A	R	Schémas de backup et formations associées	
Sous-processus : Gestion des objectifs et de la performance				
Déclinaison en cascade des objectifs selon l'organisation	AR	C	Objectifs déclinés dans l'organisation	Action réalisée par les managers des différentes entités, sous la responsabilité du DSI et validée par le DSI.
Définition des rôles et responsabilités dès la prise de fonctions	AR	C	Lettre de mission	Action réalisée par les managers des différentes entités, sous la responsabilité du DSI et validée par le DSI.
Mesure des résultats	AR	C	Entretiens annuels Reporting sur le respect des objectifs entités	Action réalisée par les managers des différentes entités, sous la responsabilité du DSI et validée par le DSI.

Etape clé	DSI	DRH	Livrables majeurs de sortie	Commentaires
Sous-processus : Gestion des compétences de la fonction SI en cohérence avec l'activité				
Élaboration des plans de mobilité / recrutement externe et déploiement de ceux-ci	A	R	Plan de mobilité et de recrutement externe et déploiement de ces plans	Les managers des différentes entités, sous la responsabilité du DSI, sont contributeurs de cette activité.
Détection des talents	AR	C	Liste des talents détectés	La détection des talents est réalisée par les managers des différentes entités, sous la responsabilité du DSI et validée par le DSI.
Élaboration et mise en œuvre d'un plan de formation, pour l'ensemble du personnel et spécifique aux compétences critiques	AR	C	Plans de formation pour l'ensemble du personnel Plans de formation spécifiques aux compétences critiques Plans de déploiement associés	Action réalisée par les managers des différentes entités, sous la responsabilité du DSI et validée par le DSI.
Sous-processus : Garantir les compétences clés de la fonction SI				
Détermination du dispositif par compétence clé	A	R	Dispositif de gestion des compétences clés	
Mise en œuvre du dispositif	AR	C	Reporting de déclinaison du dispositif	Action réalisée par les managers des différentes entités, sous la responsabilité du DSI et validée par le DSI.

5.5.3. Matrice risques / contrôles du processus de gestion des compétences de la DSI

Processus	Etapes-clés	N° de réf COBIT, ITIL, ISO…	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Vision moyen-terme emploi-compétences	Politique RH SI	PO7.1	S'assurer de l'existence, mise à jour et partagée, d'une politique RH SI adéquate avec la vision moyen-terme	Politique RH SI inexistante, inadaptée ou ignorée.	Revue de la politique RH SI et mesure de son adéquation aux points majeurs suivants : 1) déclinaison politique RH de l'entreprise ou l'administration ; 2) clarification des activités à externaliser ; 3) mise à jour autant que nécessaire pour répondre aux enjeux du SI. Mesure de l'appropriation de la politique RH SI par les acteurs majeurs concernés.	Existence d'une politique RH SI répondant aux conditions définies dans l'activité de contrôle. Appropriation de la politique RH SI par l'ensemble des managers.
	Référentiel commun de compétences SI	PO7.2	S'assurer de l'existence, de la mise à jour et du partage d'un référentiel commun des compétences SI en intégrant la vision moyen-terme	Hétérogénéité des référentiels de compétences SI.	Revue du référentiel commun de compétences SI et mesurer de son adéquation aux besoins identifiés en compétences SI dans le schéma directeur SI. Mesure de son appropriation par les managers SI.	Mise à jour annuelle du référentiel de compétences SI et déclinaison de celle-ci par entité. Intégration d'une thématique RH dans les conventions annuelles présentant les changements apportés par rapport à la version précédente du référentiel de compétences. Appropriation de ce référentiel par l'ensemble des managers SI.

Processus	Etapes-clés	N° de réf CobiT, ITIL, ISO…	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Vision moyen-terme emploi-compétences	Cartographies de compétences	PO7.3	S'assurer de la définition, de la mise à jour et du partage des cartographies de compétences.	Inadéquation des compétences avec les activités prévues au schéma directeur SI Groupe.	Revue de l'existence d'un processus d'établissement et de mise à jour des cartographies. Revue des cartographies des compétences pour vérifier leurs mises à jour sur la base du réel (situation actuelle, situation cible) et des besoins du schéma directeur SI Groupe. Mesure de la connaissance des cartographies de compétences par les managers.	Les cartographies des compétences sont construites à partir du référentiel de compétences, et remises à jour sur la base du réel et des besoins du schéma directeur SI Groupe. Les cartographies de compétences sont connues de l'ensemble des managers.
	Emplois à compétences critiques et clés	PO7.4	S'assurer de la définition, de la mise à jour et du partage des compétences critiques et clés	Non recencement des compétences critiques et clés.	Revue de l'existence d'un processus de définition, de mise à jour et de partage des compétences critiques et clés. Revue de l'existence d'une liste précisant les emplois à compétences critiques et clés mise à jour périodiquement. Mesure de la connaissance de cette liste par les managers.	Le processus de définition, mise à jour et partage des compétences critiques et clés fait l'objet d'une boucle d'amélioration continue et permet de définir une liste d'emplois à compétences critiques et clés mise à jour périodiquement. Cette liste est connue par l'ensemble des managers.
	Parcours professionnels des emplois à compétences critiques	PO7.1	S'assurer de l'existence de parcours professionnels pour les emplois à compétences critiques, mis à jour et partagés.	Mauvaise gestion des compétences critiques.	Revue de l'existence de documents clarifiant les parcours professionnels des emplois à compétences critiques . Mesure de l'appropriation de ces documents par les managers	Existence de documents clarifiant les parcours professionnels des emplois à compétences critiques mis à jour autant que de besoin. Ces documents sont connus par l'ensemble des managers

Processus	Etapes-clés	N° de réf CobiT, ITIL, ISO…	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Vision moyen-terme emploi-compétences	Schémas de professionnalisation des emplois à compétences critiques	PO7.4	S'assurer de l'élaboration, du partage et de la mise à jour des schémas de professionnalisation des emplois à compétences critiques	Pas de professionnalisation ou professionnalisation insuffisante des emplois à compétences critiques.	Revue de l'existence de schémas de professionnalisation associés à chaque compétence critique recensée. Mesure de l'appropriation de ces schémas par les managers.	Existence de schémas de professionnalisation appropriés pour chaque compétence critique. Mise à jour des schémas de professionnalisation sur la base des bilans sur les pratiques et de leurs impacts sur la performance du SI. Les schémas de professionnalisation sont connus de l'ensemble des managers
	Validation des talents et stratégie de fidélisation des talents	PO7.1	S'assurer de la validation des talents, de la définition du déploiement d'une stratégie visant à fidéliser les talents	Fuite des talents.	Mesure de l'appropriation par les managers de la stratégie de fidélisation des talents. Mesure de la mise en œuvre du dispositif de validation des talents	Il existe un processus de validation des talents détectés ; celui-ci est mis en œuvre à 100%. Des listes à potentiels SI (talents) sont établies et mises à jour. Gestion dynamique des parcours professionnels et donc de la rémunération. La stratégie de fidélisation des talents est connue de l'ensemble des managers.
	Remplacements et formations croisées	PO7.8 PO7.5	S'assurer de l'adéquation du dispositif d'organisation des remplacements et des formations croisées	Non existence de schémas de backup pour les positions critiques.	Revue de l'existence : - d'un dispositif de clarification des postes à position critique ; - de schémas de back-up pour les postes à position critique par ailleurs testés. Mesure de la prise en compte, lors d'une mutation sur un poste à compétence critique, d'une période de recouvrement.	Mise à jour des postes à position critique. Mise en place de tables de succession. Couverture de chaque poste à position critique par un schéma de backup. Le schéma de backup peut être déployé sans difficulté, en cas de besoin.

Processus	Etapes-clés	N° de réf CobiT, ITIL, ISO…	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion des objectifs et de la performance	Déclinaison des objectifs	PO7.7	S'assurer de la bonne déclinaison des objectifs au sein de l'organisation	Des objectifs personnels non adéquats avec l'organisation.	Revue de la définition en cascade de lettres de mission suivant l'organisation et en adéquation avec les objectifs de l'entité SI.	Existence de lettres de missions par entité et définition d'objectifs individuels cohérents avec ceux de l'entité d'appartenance. La responsabilité des objectifs clés tient compte du potentiel et de l'expérience des hommes en place.
	Rôles et responsabilités	PO7.3	S'assurer de la définition des rôles et responsabilités dès la prise de fonction (recrutement, mobilité ou réorganisation)	Manque de clarification des objectifs.	Revue de l'existence d'une lettre de mission fournie à chaque acteur, prenant une nouvelle fonction.	Lettres de missions réalisées dès la prise de la nouvelle fonction pour chaque acteur; chacune d'entre elles clarifient les rôles et responsabilités assignés.
	Mesure des résultats	PO7.7	S'assurer de la mise en place d'un dispositif adéquat de mesure des résultats	Pas d'évaluation des performances individuelles Respect des objectifs non mesuré.	Revue de l'existence d'entretiens pour apprécier les performances individuelles et déceler les souhaits de mobilité. Revue du respect des objectifs ainsi que de l'existence d'un plan d'action associés visant à accroître la performance. Revue de l'existence d'un plan de déploiement visant à ancrer le dispositif de contrôle interne, d'éthique et de sécurité de l'information	Définition d'un canevas d'entretien annuel diffusé et utilisé par l'ensemble des managers qui intègre les spécificités SI. Entretien annuel réalisé pour l'ensemble du personnel suivant le canevas défini. Plans d'action visant à accroître la performance, établis périodiquement sur la base de contrôle des objectifs par entités et de façon individuelle. Mise en place d'un dispositif de sensibilisation au contrôle interne, à l'éthique et à la sécurité, ciblé par type d'acteur en fonction de sa place dans l'organisation et basé sur une mesure de l'appropriation par type de population.

Processus	Etapes-clés	N° de réf CobiT, ITIL, ISO…	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion des objectifs et de la performance	Plans de mobilité / recrutement externe	PO7.1	S'assurer de l'élaboration périodique d'un plan de mobilité interne/recrutement externe adéquat	Retard / anticipation excessive des mobilités et des recrutements. Des postes critiques non couverts. Surcoût.	Revue de l'existence d'un plan de mobilité interne/recrutement externe défini annuellement. Mesure de la mise en œuvre de ce plan de mobilité.	Un plan de recrutement externe / mobilité est défini annuellement et déployé conformément à la trajectoire définie. Le plan de recrutement externe/mobilité est anticipé et tient compte de l'ensemble des éléments suivants : - le plan de charge ; - la politique RH SI ; - les parcours professionnels définis pour les emplois à compétences critiques ; - la stratégie de gestion des talents.
	Détection des talents	PO7.2	S'assurer de l'existence d'un processus de détection des talents adéquat	Démotivation des employés.	Revue de l'existence d'un processus de détection des talents défini. Mesure de la mise en œuvre de ce processus.	Processus de détection des talents connu des managers. Détection des talents en émergence et appréciation périodique de ceux-ci.
	Plan de formation	PO7.4	S'assurer de l'élaboration du plan de formation adéquat	Pas de plan de formation permettant des montées en compétences du personnel.	Revue de l'existence d'un plan de formation établi sur la base de schémas de professionalisation des emplois à compétences critiques. Mesure de la mise en œuvre de ce plan de formation et notamment d'une sensibilisation à la sécurité.	Existence de plans de formation adéquats et mis en œuvre pour l'ensemble du personnel. Déclinaison des schémas de professionnalisation en plans de formation pour les compétences critiques.
Garantir les compétences clés de la fonction SI	Dispositif par compétence clé	PO7.2 PO7.5	S'assurer de l'adéquation du dispositif de gestion de chaque compétence clé	Non gestion des compétences clés.	Revue de l'association d'un dispositif de gestion spécifique à chaque compétence clé identifiée. Mesure de la mise en œuvre des dispositifs de gestion des compétences clés.	Des dispositifs personnalisés de gestion de chaque compétence clé définis, mis en œuvre et partagés par l'ensemble des managers.

5.6. Projet et développement

Les projets informatiques sont souvent la vitrine d'une DSI, puisqu'ils jouent le premier rôle dans les grands projets de transformation, tant dans l'entreprise que dans le secteur public. Cette forte visibilité s'accompagne souvent d'une mauvaise réputation, car nombre de projets dérapent en coûts ou en délais, voire avortent tout simplement.

En effet, les risques subis par les projets sont multiples et souvent concomitants :

- risques liés à l'organisation et au contexte de l'entreprise ;
- risques liés aux processus et aux moyens de développement ;
- risques liés aux caractéristiques du produit.

C'est pourquoi, certains pré-requis en matière d'environnement de contrôle sont nécessaires pour créer les conditions de réussite des projets informatiques :

1. Afin d'abord de garantir l'alignement stratégique des projets sur les métiers, la politique informatique et sa déclinaison en plan stratégique doivent être décrites et communiquées, et les projets priorisés selon leurs enjeux, investissements et risques par un comité de gouvernance avant d'être lancés. La stratégie et les priorités de l'organisation doivent se refléter en permanence dans le portefeuille de projets.
2. Les organes de gouvernance de l'activité projets et développement (office des projets) et du projet proprement dit (comité de pilotage) regroupent des représentants des directions métiers (maîtrise d'ouvrage) et des représentants de la DSI, incluant des structures de support : contrôle de gestion, assurance qualité. Ces organes valident la justification des projets et suivent son bon déroulement :
   - la performance opérationnelle et économique du projet est mesurée, discutée puis incluse dans un tableau de bord de toute l'activité de projets et développements ;
   - le dispositif de management de la qualité et contrôle interne est décrit et opérationnel.
3. La politique de sécurité du système d'information, définie par la DSI, permet d'intégrer les exigences de sécurité appropriées dès le début du projet, et de les actualiser au fur et à mesure de l'avancement.
4. Enjeu capital dans la réussite ou l'échec d'un projet, la conduite du changement (analyse d'impact, communication, formation, reprise des données, support) doit être appréhendée le plus en amont possible et mise en place dans le cadre du déploiement de la solution.
5. Les référentiels méthodologiques de la DSI en matière de gestion de projet comme de standards de développement doivent être définis et communiqués, car ils sont les éléments opérationnels fondamentaux pour maîtriser l'environnement informatique :
   - La méthode de conduite de projet intègre les étapes clés et les grands jalons de validation : expression des besoins, recettes, mise en production, déploiement de la solution (y compris la documentation associée) ; de même, elle explicite formellement les rôles et responsabilités : maître d'ouvrage, chef de projet, architecture, exploitation, formation, support.
   - Les normes et procédures définies par la DSI (CobiT, Val IT, ITIL, CMMI, ISO, eSCM, …) permettent de garantir la standardisation, le contrôle qualité, et les principes de séparation de fonctions et d'environnement (études et production).

5.6.1. Flowchart du processus de projet et développement

Cf. flowchart « Maintenance et gestion du changement » p.90

5.6.2. RACI du processus de projet et développement

Etape clé du process projet et développement	Office des projets	Maîtrise d'Ouvrage	Etudes / Développements	Production / Exploitation	Architecture	Fonctions Support (Contrôle Interne, Sécurité, réglementaire, juridique)	Livrables attendus	Processus CobiT
Lancement / cadrage / validation du projet		AR	C	C	C	C	Expression de besoins	**AI1 PO5**
		AR	C	C	C	C	Etude préalable et/ou d'opportunité	
	A	AR	C	I	I	I	Compte-rendu d'arbitrage du comité en charge des projets SI (enjeux/gains/risques)	
Conduite du changement (activités transverses)		AR	C	C	C	C	Dossier d'analyse d'impact	**AI2 AI4 AI7**
		AR	C	I		I	Plan de formation Plan de communication Documentations utilisateur	
		A	C	AR			Description du soutien	
		I	C	AR	C		Dossier d'exploitabilité	
Gestion du projet (activités transverses)	A	AR	C	C	I	I	Schéma d'organisation	**PO4 PO8 PO10**
	A	R	AR	R	I	I	Plan projet / Planning du projet	
	I	I	AR	C	I	I	Tableau de Bord d'avancement	
Conception		AR	R	R	C	C	Cahier des charges, spécifications générales Spécifications détaillées fonctionnelles et techniques intégrant les contrôles applicatifs, l'auditabilité et les contrôles de sécurité et de disponibilité	**AI2**
Réalisation / Développement		I	AR	C	I	I	Développement, paramétrage, tests (MOE) unitaires et d'intégration Migration/Conversion Feu vert pour mise en recette Plan Assurance Qualité	**AI2**
Qualification de l'application : test/recette		I	AR	I	I		Plans de tests unitaires et d'intégration par MOE et bilan	**AI7**
	I	AR	C	C	C	C	Plans de tests utilisateurs (jeux et scénarios de tests par MOA) et bilan des tests (PV de recette)	
	I	AR	R	C	I	C	Mise en place d'un pilote et autorisation pour le déploiement	
Accompagnement utilisateurs / Formation		AR	C	I	I	C	Plan et supports de formation	**AI4 AI7**

Etape clé du process projet et développement	Office des projets	Maîtrise d'Ouvrage	Etudes / Développements	Production / Exploitation	Architecture	Fonctions Support (Contrôle Interne, Sécurité, réglementaire, juridique)	Livrables attendus	Processus CobiT
Packaging, mise en production et déploiement		C	AR	R		I	Impacts sur la production identifiés et exploitabilité validée Packages prêts pour diffusion en production (Bons de livraison) Documents à jour (Dossiers d'exploitation et de configuration) Planification et feu vert pour mise en production	**AI7** **DS1** **DS12**
		C	R	AR			Applicatif disponible pour les utilisateurs	
Bilan	A	AR	C	C	C	C	Bilan Post installation Inventaire des anomalies résiduelles (levées des réserves) Plan d'actions pour les résoudre Clôture du projet	**AI7**

5.6.3. Matrice risques/contrôles du processus de projet et développement

Processus	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Environnement de contrôle	PO1.1 PO1.2 PO1.4 PO6.1 PO6.5	**Stratégie et politique** La politique SI est décrite. Un plan stratégique SI moyen et long terme est décrit. Il est en ligne avec la stratégie Business de l'entreprise.	Déclinaison SI incorrecte des éléments du plan stratégique Business.	La politique des systèmes d'information est communiquée. L'alignement des projets avec les objectifs stratégiques SI est suivi régulièrement. Des plans d'investissement SI sont réalisés et révisés régulièrement.	La politique du système d'information doit traiter au moins des domaines suivants (gouvernance, maîtrise des technologies utilisées, sécurité logique et physique du SI, exploitation informatique et continuité de service, gestion des risques, RH …). Elle peut renvoyer vers des politiques sectorielles (comme la politique de la sécurité des systèmes d'information).
	PO6.2 PO9.1 PO9.4	**Management des risques** Une cartographie des risques SI est disponible, et est maintenue.	Non maîtrise des activités SI. Non utilisation de la connaissance des risques SI pour définir la stratégie.	L'évaluation et l'acceptation des risques SI sont menées périodiquement, et s'appuient sur la cartographie des risques. Les impacts sur les activités sont évalués.	Le cadre d'évaluation des risques (matrice, outil de gestion des risques …) permet d'associer à chacun des risques des plans d'action adéquats et raisonnables pour couvrir le risque, le minimiser ou le tolérer. Des contrôles permettent de couvrir les risques identifiés dans la cartographie établie.
	PO4.1 PO4.2 PO4.3	**Organes de gouvernance** L'organisation autour des projets SI garantit la bonne gouvernance et la maîtrise des investissements, conformément à la stratégie Business de l'entreprise.	Non alignement des investissements SI avec les objectifs Business.	Des comités d'investissements constitués de toutes les parties prenantes sont mis en place pour la gestion des investissements et du pilotage des projets.	Les projets SI sont placés sous la responsabilité des directions métiers. Elles disposent des budgets SI pour les projets et les pilotent.

Processus	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Environnement de contrôle	PO8.2 PO8.3	**Standards, procédures** Les référentiels de bonnes pratiques du domaine sont connus. Une méthodologie de gestion de projet et de développement informatique a été retenue. Les processus sont décrits et placés sous assurance qualité.	Non respect des règles de bonnes pratiques du domaine SI.	Le management a défini et communiqué les règles permettant de maîtriser l'environnement SI (organisation et activités).	Des comparaisons avec les pratiques communément utilisées ou déployées dans d'autres entreprises sont réalisées. Des normes/standards/référentiels internationaux sont utilisés (CobiT/Val IT, ITIL, CMMI, ISO, eSCM …).
	PO7.2 PO8.1 DS6.2	**Maîtrise de l'activité** Le contrôle de gestion des projets est opérationnel. La séparation de fonctions est documentée. La gestion des compétences est en place. Le contrôle interne est documenté. Un système de management de la qualité est en place.	Dérives non contrôlées, sécurité de l'information et fraude, gestion des ressources non efficiente.	Les investissements et charges SI sont suivis. Les rôles et responsabilités du personnel SI sont formellement définis. L'organisation des RH SI et le management des connaissances sont correctement pilotés. Le dispositif de contrôle interne (contrôles généraux informatiques) est décrit et opérationnel (activités de contrôle identifiées et évaluées régulièrement pour vérifier l'efficience). Un processus d'assurance qualité est clairement défini, maintenu et administré pour toutes les activités SI.	Des indicateurs financiers pertinents sont mis en place et permettent de comparer la performance du SI avec d'autres entreprises comparables (benchmark) : investissement SI/chiffres d'affaires par exemple. La performance des projets est mesurée suivant les 3 axes (coût, délai, qualité). La gestion prévisionnelle des ressources humaines est assurée. Elle permet d'anticiper les plans de formation, les recrutements de profils clés ...

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Cadrage des projets	Structure et processus de décision	PO5.2 PO5.3 PO5.4 PO5.5	Les décisions d'investissement suivent un processus décrit et sous contrôle. Elles impliquent le bon niveau managérial en fonction des investissements consentis.	Manque d'implication des commanditaires, de la direction générale jusqu'à la fin du projet (Sponsor)	La gouvernance de projet est en place (comité d'investissement, comité de pilotage qui se réunit régulièrement avec MOA, MOE). Les comptes-rendus et plan d'actions sont rédigés et suivis.	Des comités d'investissement SI sont créés, impliquant toutes les parties prenantes (direction générale, métier-BU, SI, responsable sécurité, juriste, réglementeur, responsable fraude ...). Le niveau hiérarchique pour l'acceptation des projets est fonction de seuils d'investissement prédéfinis, fonction de la taille de l'entreprise.
	Portefeuille des applications et des projets	PO1.6 PO10.1	Le patrimoine informationnel est connu et maîtrisé.	Méconnaissance en interne de l'entreprise Dépenses SI non sous contrôle Mauvaise gestion des investissements	Il existe une liste (portefeuille) des applications en service et des projets en cours avec une identification des propriétaires.	La gestion de portefeuille d'applications et des projets est centralisée. Un outil partagé (sur Intranet) aide à maintenir à jour le portefeuille. Des regroupements d'applications/projets en programmes sont opérés suivant des critères prédéfinis (par processus métiers, par niveau de sensibilité des applications). Une cartographie de l'ensemble des applications est disponible et tenue à jour.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Cadrage des projets	Alignement du SI sur la stratégie de l'entreprise	PO1.2	Les décisions d'investissement respectent et soutiennent la stratégie métier et SI. Un consensus sur les objectifs et enjeux/risques des projets est obtenu par les parties prenantes.	Déclinaison incorrecte du plan stratégique	Les projets font l'objet de priorisation en comité de direction sur critères Les projets sont portés par le métier qui les finance (identification d'un sponsor).	Les applications les plus critiques (pour le Business, le respect de la réglementation, la sécurité ...) sont repérées. Les applications sont classées suivant le niveau de sensibilité des données manipulées (disponibilité, intégrité, confidentialité) . Le budget pour les applications et projets SI est alloué au Business (unités d'affaires, branche métier). La responsabilité des applications et des projets est assumée par le Business (choix d'investissement, coût, délai, qualité).
	Etude d'opportunité et de faisabilité	AI11 AI1.2 AI1.3 AI1.4 PO10.9	Tous les projets font l'objet d'une étude d'opportunité avant leur lancement.	Lancement de projets sans valeur ajoutée pour l'entreprise	Les projets font l'objet d'étude de faisabilité, d'analyse de risque (y compris sécurité), d'analyse d'impact métier et organisationnel et d'un Business Plan.	Les projets font l'objet d'un scoring : enjeux, gains et risques Dans le cas de l'acquisition d'un progiciel, la sélection est encadrée par une procédure et contrôlée (cahier des charges, sélection, validation...) La phase d'étude de faisabilité/opportunité ne doit pas durer trop longtemps (6 mois pour les projets importants). Elle doit servir à cerner les vrais besoins métiers et leurs priorités et, à justifier le projet par un calcul rigoureux du ROI (retour sur investissement). Le ROI est systématiquement calculé et présenté en comité d'investissement. La décision de lancement de projet doit se faire sur la base d'un cahier des charges précis, d'engagement de réalisation précis et d'identification des dépenses engagées. La qualité de l'instruction de cette étape est fondamentale car elle est la base de la mise en œuvre du projet. Des erreurs, oublis ou négligences commis durant cette phase seront difficilement rattrapables, ou alors avec un fort impact de coût et de délai. L'étude de faisabilité conduit à envisager plusieurs scénarii avec pour chacun les risques pesant sur le projet.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Conduite du changement	Analyse des impacts organisationnels et processus		L'organisation à mettre en place et les modes de fonctionnement futurs sont anticipés et opérationnels à la mise en production de l'application.	Sous-estimation de l'ampleur des changements et de leurs impacts. Manque d'homogénéité entre le projet SI et les choix organisationnels. Mauvaise intégration du volet social.	Les impacts organisationnels et processus métier, notamment dans le cas d'ERP, sont identifiés et anticipés. La population cible est recensée et les messages clés identifiés. Les aspects RH sont pris en compte (éventuellement communication au comité d'entreprise).	Tous les impacts de la nouvelle application sont identifiés et mesurés. Les risques sont également évalués. Les domaines d'impact possible à analyser sont notamment : organisation, processus, sécurité, fraude, réglementation. Ces analyses sont réalisées et documentées avec les parties prenantes.
	Formation et documentation	AI7.1 AI4.2 AI4.3	La nouvelle solution ou les évolutions sont appropriées par les futurs utilisateurs.	Insatisfaction utilisateur	Les plans de formation des utilisateurs sont anticipés. Des sessions de formations sont organisées conformément aux besoins de mise à niveau des utilisateurs. La documentation (utilisateurs, exploitants, contrôle interne …) est disponible au démarrage de l'application.	Des plans de communication sont élaborés pour prévenir les utilisateurs de l'arrivée d'une nouvelle application. Ils présentent les messages clés, les impacts identifiés, les plans de formations adaptés aux populations recensées. Des supports de communication sont produits. Les formations sont adaptées aux populations concernées. Des outils de type e-learning sont utilisés. Dans le cadre de l'acquisition d'un progiciel, seule une bonne maîtrise du progiciel en interne (centre de compétences, expert métier/processus...) pourra garantir une meilleure appropriation et une prise en compte à moindre coût des besoins métier (par le paramétrage).

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Conduite du changement	Soutien applicatif et métier	AI4.4	L'organisation du soutien permettant d'assister les utilisateurs est opérationnelle dès la mise en production.	Soutien non opérationnel au lancement (dispositif d'assistance inexistant ou insuffisant). Soutien débordé	Le soutien au démarrage de l'application est suffisamment dimensionné pour assurer le pic d'appels. La chaîne de soutien est décrite, organisée en plusieurs niveaux, impliquant tous les acteurs concernés (soutien métier, soutien applicatif, soutien technique, experts)	Des scénarii d'appels au soutien sont élaborés. Ces scripts de question/réponse sont utilisés par la Hot Line pour identifier précisément l'objet de l'appel et pour y répondre le plus rapidement possible en l'aiguillant vers le bon niveau de soutien. Des fiches consignes sont écrites pour les différents intervenants de la chaîne de soutien. Un soutien renforcé (task force) est mis en place en phase post-installation (sur une durée limitée) pour gérer les pics d'appels à la Hot-Line.
	Exploitabilité de l'application	AI2.10 AI4.4	La capacité à exploiter la solution est étudiée et mesurée avec les exploitants avant la mise en production.	Application non exploitable dans de bonnes conditions de performance et de satisfaction utilisateurs.	Les critères d'exploitabilité sont prédéfinis, notamment les exigences de sécurité, les plans de sauvegarde/restauration et niveau de secours de l'application. L'exploitabilité de l'application par critère est mesurée avant sa mise en production. Les points bloquants sont identifiés et traités rapidement.	L'exploitabilité est gérée comme un processus, initialisée dès l'étude d'opportunité de l'application. La progression, tout au long du projet, du niveau d'exploitabilité fait l'objet d'un suivi régulier au passage de jalons du projet jusqu'à sa mise en production. Le niveau d'exploitabilité est un des critères de mise en production. La disponibilité est prise en compte le plus tôt possible dans le processus de conception.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Conduite du changement	**Initialisation / Migration des données**	AI7.5	La phase de préparation / conversion / migration des données est anticipée, préparée et planifiée.	Application non opérationnelle ou présentant des dysfonctionnements importants liés à la qualité des données.	La phase de conversion/migration de données est anticipée et préparée. Elle est gérée comme un projet. Les principes de migration sont définis (scénario, tables de trans-codification) et la recette de la migration / conversion est réalisée (exhaustivité et exactitude des données migrées : qualité des données). Un plan de retour arrière après bascule est prévu en cas de problèmes (restauration des données).	Chaque nouvelle application vers laquelle des données doivent être migrées possède sa propre stratégie de migration de données et son propre plan. La migration des données est gérée comme un sous-projet. Il démarre dès l'étude d'opportunité du projet et identifie les différents scénarii possibles (en fonction des risques). Des tests préalables sont réalisés avant la bascule réelle.
Gestion de projet	**Organisation**	PO4.6 PO4.7 PO4.8 PO4.9 PO10.3	L'organisation de chaque projet est décrite en impliquant tous les acteurs. La séparation effective des fonctions est assurée (Matrice de séparation de fonction).	Responsabilités non clairement définies. Pilotage défectueux. Prise de décision non contrôlée. Manque d'implication de la direction générale et des commanditaires (sponsor).	Des structures de pilotage sont en place. Ces instances de pilotage se réunissent à chaque jalon majeur du développement des projets. Elles peuvent décider de l'arrêt d'un projet si nécessaire (le plus en amont possible pour limiter les pertes). Les rôles et les responsabilités « Etudes / Métiers / Développement / Exploitation » sont clairement définis.	La structure du projet doit être pérenne tout au long du projet. Une note d'organisation est réalisée et, si besoin, des fiches de fonction sont établies. Pour les projets importants (en investissement, à risques, Business), le chef de projet (ou directeur de programme) doit être rattaché au comité de direction. Une définition claire du périmètre d'action des différentes parties prenantes est élaborée (notamment MOA vs MOE). Exemple d'organisation de projet piloté par la Maîtrise d'Ouvrage (MOA) : - MOA (direction de projet), MOA déléguée (chef de projet), assistance à MOA (support technique et méthodologique, suivi projet, assurance qualité, sécurité, contrôle interne, audit, communication) et utilisateurs experts fonctionnels ; - MOE (chef de projet), Equipe conception/réalisation, sous-traitants, équipe support (responsable qualité, support méthodologique, sécurité, exploitation, déploiement ...).

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion de projet	Planification	PO10.12	Les projets font l'objet d'une planification initiale adaptée à leur dimension.	Non maîtrise des plannings. Planning irréaliste ou non représentatif. Fonctionnement en boîte noire (aucune visibilité sur l'avancement, difficultés de réaction en cas de dérives).	Un planning initial est réalisé, revu si nécessaire, en cours de projet. Le projet est découpé en lots mesurables pour éviter l'effet tunnel ou le phénomène de boîte noire.	Les éventuels liens avec les projets connexes sont pris en compte. La montée en charge du projet (en effectif) est maîtrisée. La planification est réalisée à l'aide de diagramme de Gantt et de la Méthode PERT (identification du chemin critique).
	Suivi / pilotage	PO10.3 PO10.7 PO10.4 PO10.6 PO10.9 PO10.10 PO10.13 PO10.14 DS6.2	L'avancement du projet est suivi régulièrement (risques, charges initiales, charges consommées, reste à faire, délais, qualité).	Non maîtrise du projet. Dérive non contrôlée.	Des indicateurs de suivi de projet pertinents sont définis Des points réguliers sont réalisés avec les parties prenantes. Tout dépassement de budget fait l'objet d'une alerte au management (avec justification de l'écart).	Le comité de pilotage s'assure du respect des budgets et de l'alignement avec la stratégie. Il se réunit régulièrement, les décisions y sont entérinées et des comptes-rendus sont rédigés. Les risques du projet sont suivis. Un reporting des projets est assuré via des tableaux de bord intégrant des indicateurs de performance des projets (KPI). Il remonte jusqu'à la direction générale. Les coûts complets (y compris coût de personnel interne et externe) font l'objet d'un suivi régulier. Un bilan de projet est systématiquement réalisé après déploiement. Une communication régulière sur l'avancement du projet, ses enjeux, est primordiale pour conserver la mobilisation de tous les acteurs.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion de projet	Méthode et outils	PO8.3 PO8.2	Tous les projets suivent le même cadre méthodologique de conduite de projet.	Méthode de travail ne permettant pas de garder la maîtrise du déroulement du projet. Absence de cadre méthodologique de conduite de projet. Coûts sous-estimés ou incomplets.	Une méthodologie de développement de projet est définie et suivie. Cycle de vie des projets. Des étapes de validation jalonnent le projet = points de contrôle (jalons de validation : lancement, tests, recette).	Des outils de planification et de suivi sont utilisés pour faciliter les contrôles, et ils sont partagés. Des comités de validation sont mis en place (investissement, architecture technique, architecture fonctionnelle, déploiement …). Le jalon marque un événement sensible de la réalisation du projet nécessitant un contrôle. Chaque jalon permet de vérifier que les conditions nécessaires à la poursuite du projet sont réunies. Les jalons sur le projet sont prédéfinis et planifiés (échéancier) *cf planification du projet*. Des revues de codes peuvent être planifiées.
	Appel à la sous-traitance	AI5.2 AI5.3 AI5.4	Les besoins en sous-traitance sont identifiés, justifiés et validés.	Coûts non justifiés et non maîtrisés. Dépassement budgétaire. Contractualisation avec les prestataires externes présentant des points faibles ou des lacunes. Non respect de la loi relative à la sous-traitance (n°75-1334 du 31/12/1975). Absence d'engagement liant les parties, dépendance vis-à-vis des prestataires. Confidentialité et propriété intellectuelle non prises en compte.	L'appel à la sous-traitance fait l'objet d'une demande justifiée par le chef de projet (ressources insuffisantes, coûts inférieurs, compétences particulières...). Il est encadré par un appel d'offres (sélection) sur la base d'un cahier des charges validé. A l'issue de la sélection, un contrat avec engagement de services (moyens/résultats) et clause de confidentialité/auditabilité/droits de propriétés est signé. Les fournisseurs font l'objet de contrôles en cours de missions et d'évaluation à l'issue de la prestation.	Les tâches confiées à la sous-traitance sont clairement définies et le champ d'action finement délimité. L'activité confiée à la sous-traitance ne devra pas entraîner une dépendance forte en termes de compétences et de technologie. Se conformer aux exigences réglementaires, notamment la loi n°75-1334 du 31 décembre 1975 relative à la sous-traitance (version consolidée au 1er janvier 2006). Un transfert de compétences et de technologie doit être prévu dès le départ du contrat (surtout dans le cas d'acquisition de progiciel).

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion de projet	**Audit et contrôle**	SE1.4 SE2.5 PO8.6	Des audits internes sont prévus sur les projets majeurs/critiques (évaluation de la performance). Le contrôle qualité est en place et assuré tout au long du projet.	Non atteinte des objectifs initiaux des projets. Non-conformité aux règles et standards du domaine, de l'entreprise.	Des audits de projets sont systématiquement planifiés pour les projets majeurs (investissement > à xk€, durée > à 1 an …) ou à hauts risques (sécurité par exemple). Des revues qualité sont menées aux jalons des projets.	Une évaluation de la sensibilité est menée durant les premières phases du développement. Les aspects sécurité des données et contrôle interne de la future application sont évalués lors de la conception, de manière à y intégrer les concepts de sécurité le plus tôt possible (Idem pour la sécurité logique, gestion des habilitations dans l'application conformément à la matrice de séparation des tâches). Des audits peuvent être menés avant le passage de jalons ou en cas de crise.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion de projet	**Bilan**	AI7.9	Un bilan de mise en œuvre est réalisé tel que défini dans le plan de mise en œuvre.	Le retour sur investissements ne répond pas aux attentes du management. Incapacité d'identifier que les systèmes ne répondent pas aux besoins des utilisateurs finaux.	Mettre en place une procédure de bilan de projet. Utiliser des indicateurs d'évaluation de projet. Faire participer les responsables des processus métiers, informatiques techniques et de contrôle interne ou de gestion des risques. Etablir un plan d'action pour traiter les problèmes identifiés.	Mettre en place une procédure de bilan de projet, pour identifier, évaluer et rapporter dans quelles mesures : • les besoins ont été couverts ; • les avantages attendus ont été obtenus ; • le système est considéré utilisable ; • les attentes des intervenants internes et externes sont satisfaites ; • des impacts inattendus sur l'organisation ont eu lieu ; • les principaux risques ont été jugulés ; • la gestion du changement, d'installation et de processus d'accréditation a été effectué de manière efficace et efficiente. Consulter les responsables métier et informatiques pour définir des indicateurs de succès, réalisation des exigences et bénéfices obtenus. Le formulaire de bilan fait partie du processus de gestion du changement. Faire participer les propriétaires des processus métiers ou parties tiers, le cas échéant. Examiner également les exigences hors métier ou DSI (par exemple, l'audit interne, la gestion des risques de l'entreprise, la conformité réglementaire). Etablir un plan d'action pour traiter les problèmes restants, identifiés durant le projet. Faire participer les responsables métier et informatiques dans son élaboration.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Conception et Développement (Fabrication)	**Spécifications fonctionnelles et détaillées**	AI2.1 AI2.2 AI2.3 AI2.4 AI2.5 AI2.9	Les besoins sont exprimés et validés par le métier (Business Unit, sponsor, utilisateurs…). La mise en place des contrôles applicatifs automatisés (embarqués dans l'application) et des contrôles opérationnels manuels sur les processus métier est anticipée (en lien avec les risques).	Etude des besoins incomplète et non validée. Non-conformité des spécifications aux besoins des utilisateurs. Manque d'homogénéité entre le projet SI et les choix organisationnels. Erreurs de traitements non détectées.	Les besoins sont exprimés par le métier et les autres parties prenantes (par ex. : sécurité, juridique). Un cahier des charges (ou spécifications générales) est rédigé et validé. La sécurité est prise en compte dans les développements (sensibilité de l'application, gestion des habilitations, niveau de protection des données manipulées). Les spécifications détaillées sont rédigées et validées (modèle de données, de traitements…). Elles respectent les spécifications générales. Les différences sont tracées et validées par le Business. Les besoins identifiés a posteriori sont validés et planifiés avant prise en compte. Les demandes de changement en cours de projet font l'objet d'estimation (coûts, risques, impacts) et sont validées par la MOA. Les contrôles associés à l'application (sur les données d'entrée/sortie, traitements) sont décrits et maintenus sous la responsabilité de la Maîtrise d'Ouvrage (MOA). Ces contrôles font l'objet de tests/recettes spécifiques.	Des utilisateurs clés sont identifiés et désignés. Ils peuvent constituer un groupe utilisateur qui sera consulté lors de la conception et de la validation fonctionnelle. L'engagement ferme des directions métiers (Business) directement impliquées est indispensable pour arbitrer les choix fonctionnels et pour obtenir l'adaptation des processus et de l'organisation (surtout dans le cadre de l'acquisition d'un progiciel). Dans le cadre de l'acquisition d'un progiciel, les développements spécifiques doivent être limités. Il faut utiliser au maximum le paramétrage proposé par défaut. Au besoin adapter les processus métiers (analyse d'impact préalable). Un représentant sécurité est impliqué dans la conception. Un gestionnaire (administrateur) de données est nommé. Il administre les données au niveau de l'entreprise pour éviter les redondances d'information et le niveau de sécurité exigé sur les données (contrôle d'accès). Les auditeurs et les contrôleurs internes sont impliqués dans la mise en place des contrôles applicatifs. Les exigences de contrôle interne et de sécurité incluent des contrôles applicatifs qui garantissent l'exactitude, la complétude, l'opportunité et l'autorisation des entrées et sorties. Dans le cadre d'ERP, le paramétrage des contrôles prédéfinis dans le progiciel fait l'objet de validation par les responsables de processus.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Conception et Développement (Fabrication)	Réalisation / Développement	AI2.7 AI2.8	La solution développée respecte les spécifications fonctionnelles. Sa maintenance et son évolution doivent être possibles.	Non maintien de la solution	Les développements respectent les règles, normes et standards retenus par l'entreprise. Tous les objets développés sont gérés en configuration (typologie, règle de dénomination, versionnage …). Chaque élément développé (programme/module logiciel) est identifié de manière unique. Toute modification est enregistrée et tracée.	Des outils de modélisation (données, traitements, objets) sont décrits. Les normes d'écriture des programmes sources sont décrites et respectent les bonnes pratiques en ce domaine (indentation permettant une mise en forme et une amélioration de la lisibilité des programmes, commentaires …). Des revues de codes sources sont planifiées. Les contrôles applicatifs importants embarqués dans l'application sont repérés de façon claire dans le code source.
	Maquettage / Prototype		L'intérêt de la solution/application et sa faisabilité sont vérifiés avant de lancer la réalisation.	Développement engagé sans vérification du concept initial	Une maquette (ou prototype) est réalisée pour valider les points fonctionnels en suspens, l'ergonomie / simplicité, et pour confirmer l'intérêt de la solution (valeur ajoutée).	Les critères initiaux sont vérifiés avec les utilisateurs très en amont pour valider le concept avant de commencer la phase de conception/réalisation. Une grande réactivité est demandée par tous les intervenants sur la phase de maquettage. Le maquettage/prototype permet en particulier de lever les incertitudes liées à la conception des SI, en facilitant la démarche de planification qui précède la conception et la réalisation. Cette maquette doit pouvoir refléter les besoins des clients et donc doit être testée et avalisée par ces derniers.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Conception et Développement (Fabrication)	**Architecture technique et logicielle**	AI2.4	Les développements s'intègrent dans l'architecture technique et logicielle prédéfinie par l'entreprise.	Non-conformité aux préconisations. Choix technologiques non validés voire erronés et/ou non cohérents avec le patrimoine existant. Mauvais dimensionnement des architectures. Mauvaise intégration dans le SI existant (interface).	L'architecture technique retenue pour la solution est validée. Les choix techniques sont validés. Ils respectent des technologies validées par la DSI (notamment en termes de sécurité).	Des comités de validation des architectures techniques sont organisés. Tous les projets passent en comités de validation pour valider les options techniques prises. Des comptes rendus sont rédigés. Les choix techniques et fonctionnels reposent sur des solutions éprouvées et reconnues par l'entreprise. Il existe un catalogue des solutions techniques proposées par la DSI. Les environnements de tests et de production sont préparés.
Qualification de l'application : tests/recettes	**Tests d'intégration**	AI7.4	Les tests techniques (unitaires/intégration) sont réalisés avant la validation fonctionnelle. Les tests de non régression avec l'environnement SI (applications dépendantes) sont effectués.	Tests techniques insuffisants.	Un bilan de qualification est réalisé à l'issue des développements sur la base de fiches de tests. Des comptes-rendus sont rédigés. Les tests techniques sont réalisés par la MOE.	Les environnements de test doivent être séparés des environnements de production pour des raisons de sécurité. Si possible, les bases de tests ne doivent pas comporter de données réelles en production surtout si les données, manipulées par l'application, sont sensibles (données personnelles, données financières et commerciales...). En cas de nécessité liée aux tests, l'utilisation de données réelles devra être justifiée et validée par la MOA. Des contrôles complémentaires (organisationnels, procédures, techniques...) devront être mis en place pour garantir la sécurité de l'information.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Qualification de l'application : tests/recettes	Recette fonctionnelle par les utilisateurs	AI7.2	La solution est acceptée par les métiers et un feu vert pour la mise en production est donné.	Recette fonctionnelle non réalisée par les utilisateurs (MOA, Business).	Des cahiers de tests fonctionnels, validés par la MOA, sont établis et servent de support à la recette. Une recette finale est réalisée avec les utilisateurs et autres parties prenantes (sécurité, juriste...) sur la base de scénarii de tests et de fiches de tests.	La recette fait l'objet d'une description détaillée. Ce dossier de contrôle est réalisé au plus tard à l'issue de la phase de conception. La recette est ensuite réalisée conformément au dossier de contrôle fourni par la MOA. A l'issue de la recette, un Procès Verbal de Recette est signé par la MOA et la MOE. Les réserves sont identifiées et classifiées (bloquantes, non bloquantes). Les plans d'action sont formalisés et suivis pour lever les réserves au plus tôt.
	Mise en place pilote	AI7.7	Une mise en place pilote peut être nécessaire avant généralisation de la solution pour valider les points fonctionnels et techniques en suspens.	Non validation en grandeur nature sur une échelle réduite avant mise en production.	Une phase pilote est organisée pour la vérification en situation réelle. Les attentes et objectifs de la phase pilote sont exprimés par les parties prenantes. Les points en suspens sont vérifiés. Toutes les réserves sont levées. Le niveau de satisfaction des utilisateurs est mesuré à l'issue de la phase pilote. L'appropriation de la solution par les utilisateurs est mesurée. Une réunion de validation finale est organisée par le sponsor avec toutes les parties prenantes. Un « Go / No Go » est prononcé par le sponsor au vu des résultats des tests et des risques résiduels. La décision est tracée dans un compte-rendu. Un feu vert pour le déploiement est donné par la MOA après accord de toutes les parties prenantes (sécurité, juriste, conformité).	Un bilan de Mise en Place Pilote (MPP) est réalisé avec les utilisateurs. Ils mentionnent des réserves identifiées. La MPP permet de tester la solution dans sa dimension technique. Elle permet également de préparer le déploiement, de mieux en apprécier la charge et d'en identifier les difficultés a priori. La MPP fait l'objet d'un plan de communication et de formation à destination des premiers utilisateurs de la nouvelle solution. Les objectifs de la MPP sont identifiés et présentés aux utilisateurs et un bilan est réalisé à la fin.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Mise en production / exploitation	Gestion des livraisons	AI7.4 AI7.8	Les livraisons pour mise en production sont identifiées. Un retour arrière à la situation précédente est toujours possible.	Non maîtrise des versions installées.	Les livraisons font l'objet de PV de livraison à destination des exploitants.	Le détail des livraisons (composants logiciels) est indiqué dans un bon de livraison à destination des exploitants qui devront installer la nouvelle version. L'identification des composants logiciels est importante car elle doit garantir qu'aucune modification du logiciel n'est intervenue depuis la recette. L'installation respecte les procédures de mise en exploitation.
	Procédures d'exploitation	AI7.4 AI7.8 DS11.5	Les procédures d'exploitation, notamment sauvegardes/restauration, sont opérationnelles. Elles sont décrites dans des procédures et maintenues.	Continuité de service non assurée.	Toutes les procédures d'exploitation font l'objet de fiches accessibles et lisibles.	Ces procédures sont intégrées au manuel d'exploitation, livré avec l'application par le prestataire qui a réalisé l'application, adaptées éventuellement par l'équipe d'exploitation. Elles couvrent notamment la gestion de la sécurité (sauvegarde, restauration, plan de secours...), archivage, administration et surveillance de l'exploitation, la qualité de service et l'assistance en cas de panne (Cf. processus d'infogérance page 130).

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Mise en production / exploitation	Engagement sur le niveau de service attendu	DS1.1 DS1.3 DS1.4	Le niveau de service attendu est exprimé par le sponsor et fait l'objet de contrat engageant les parties (contrat de service ou *SLA : Service Level Agreement*).	Service rendu aux utilisateurs non conforme aux exigences des utilisateurs (performances par exemple).	Chaque application dispose d'un contrat de service (interne ou externe) qui définit les exigences de fonctionnement du SI (disponibilité, performance, KPI...).	Le contrat passé entre un fournisseur et une entreprise permet de sécuriser et fiabiliser les niveaux de service, que l'entreprise considère comme cruciaux de maintenir ou d'acquérir, pour répondre à ses objectifs métier (non seulement des engagements de disponibilité du service mais également l'assurance de l'adéquation du niveau de service fourni aux enjeux stratégiques de l'entreprise et de ses métiers). Les objectifs (en termes de performance, de disponibilité par exemple) sont explicités et des indicateurs permettent de suivre l'atteinte des objectifs. Des pénalités doivent être définies en cas de non respect des engagements. Des tableaux de bord sont réalisés mensuellement.
	Levée des réserves		Les réserves identifiées à l'issue de la recette font l'objet d'un suivi après déploiement en vue de leur levée.	Dysfonctionnements non réglés.	Un suivi rapproché en phase de post-déploiement est en place pour lever les points restant en suspens.	Une revue post-installation est réalisée pour s'assurer que les points en suspens et les réserves sont levés. La revue peut également servir à capitaliser sur l'expérience acquise pour en faire profiter les projets à venir.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Mise en production / exploitation	**Achats des ressources informatiques**	DS12.1	Les achats de ressources informatiques sont anticipés. L'arrivée des ressources informatiques dans les salles serveurs est préparée (notamment en termes d'environnement technique, m² disponibles, plan de secours...).	Non anticipation des besoins en matériel. Mauvaise gestion des actifs.	L'arrivée des ressources informatiques dans les salles serveurs est préparée (notamment en termes d'environnement technique).	Les achats en matériel informatique sont anticipés et intégrés aux investissements de départ. Les nouveaux biens sont répertoriés (actifs). Les achats suivent le processus "achat" de l'entreprise. Il existe une base de données répertoriant tous les serveurs et autres matériels informatiques, ainsi que leur localisation (salles serveurs). Des comités d'implantation de serveurs peuvent être mis en place pour décider du lieu d'installation en fonction de critères prédéfinis.

5.7. Maintenance et gestion des changements

Le patrimoine applicatif d'une entreprise ou d'une administration représente un capital considérable d'intelligence et de connaissance qui a coûté des milliers d'hommes.an, et il joue un rôle unique dans le fonctionnement opérationnel. Pour maintenir ces milliers d'applications et ces millions de données, il manque souvent la discipline en matière de documentation et de normes.

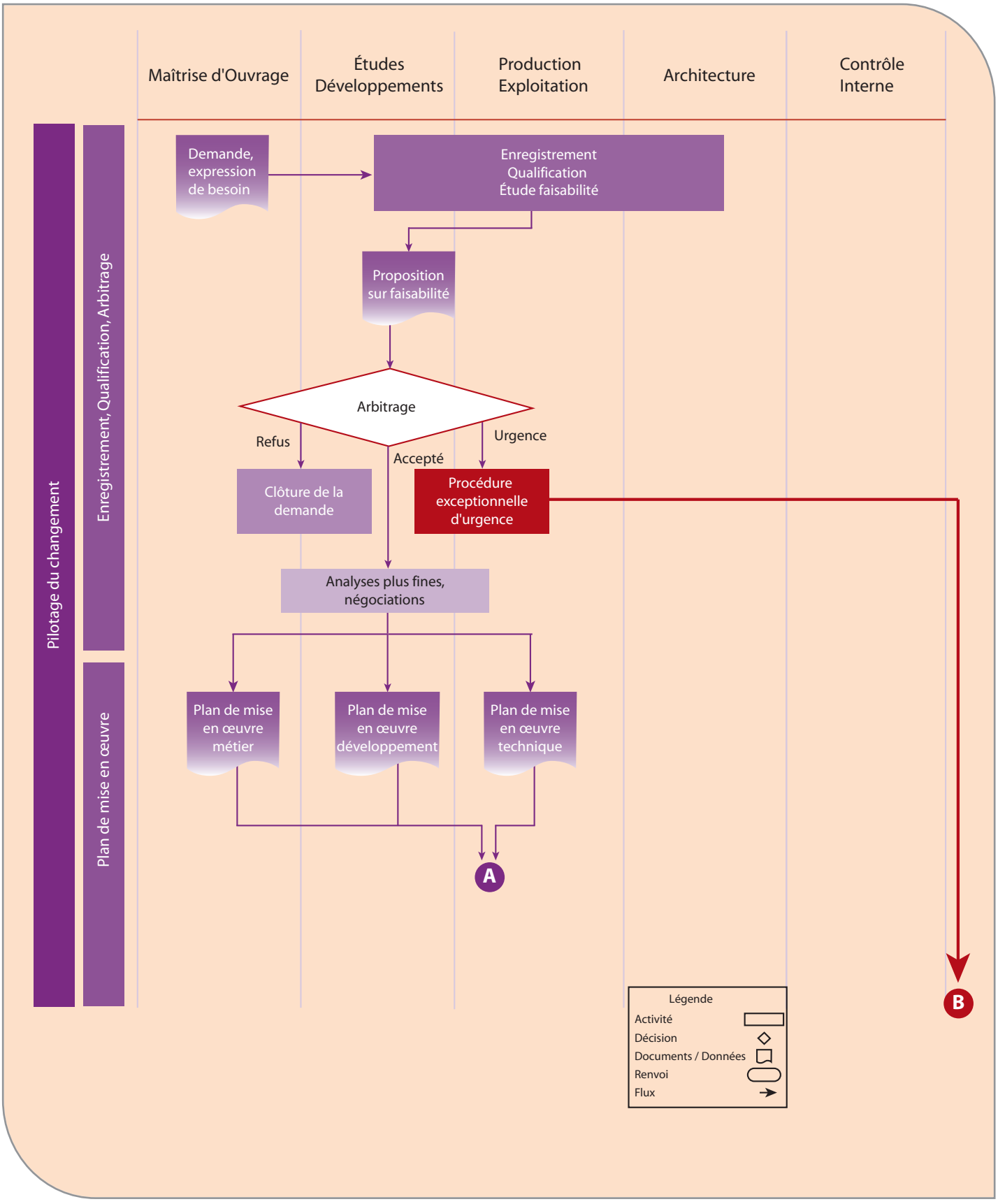
Or, les principaux risques du processus de maintenance applicative sont :

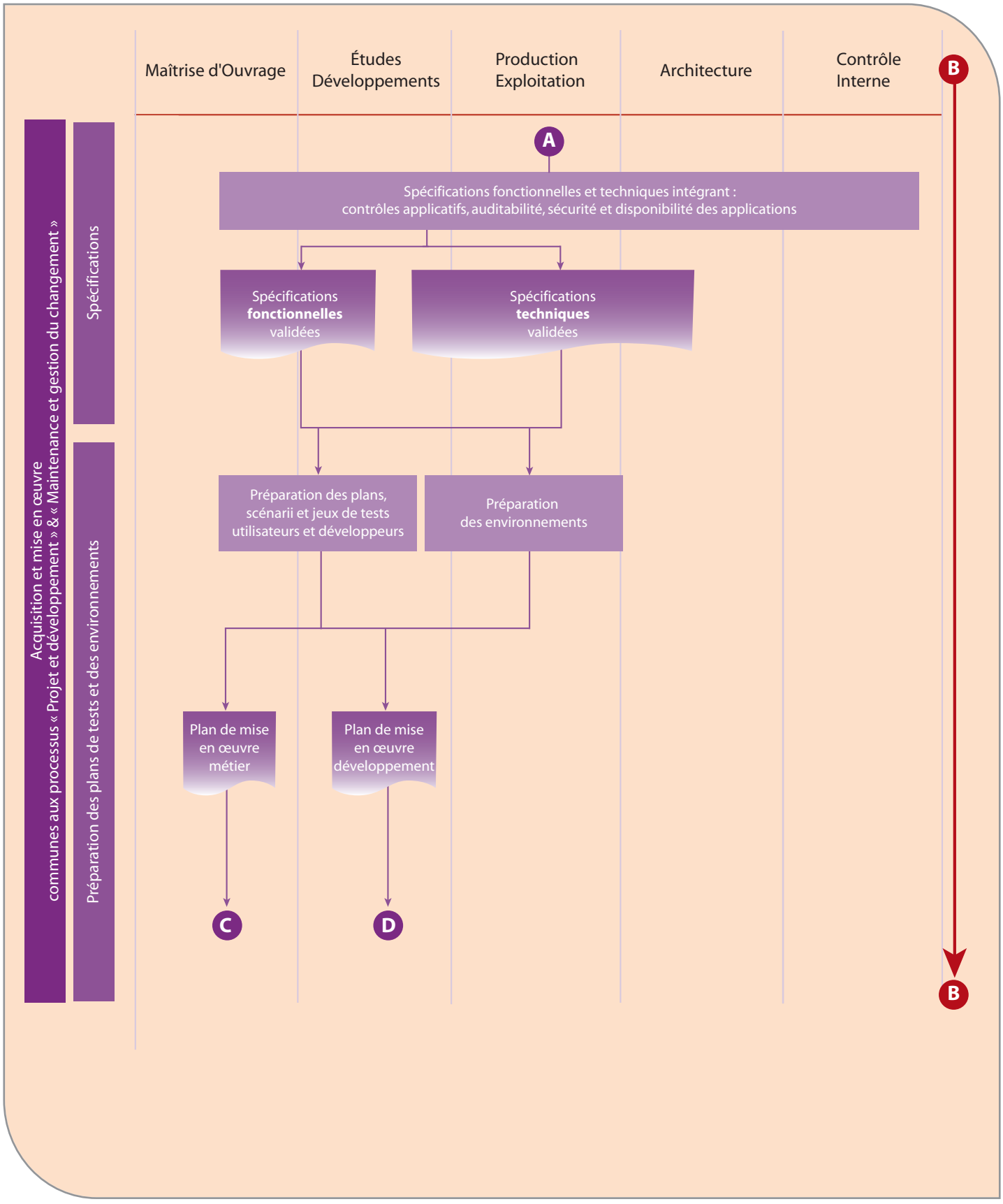
- les surcoûts liés à une insuffisance de planification ;
- la régression fonctionnelle ou dégradation de la disponibilité des systèmes, à la suite de changements incontrôlés ou non autorisés ;
- les décalages entre les besoins et les fonctionnalités mises en œuvre.

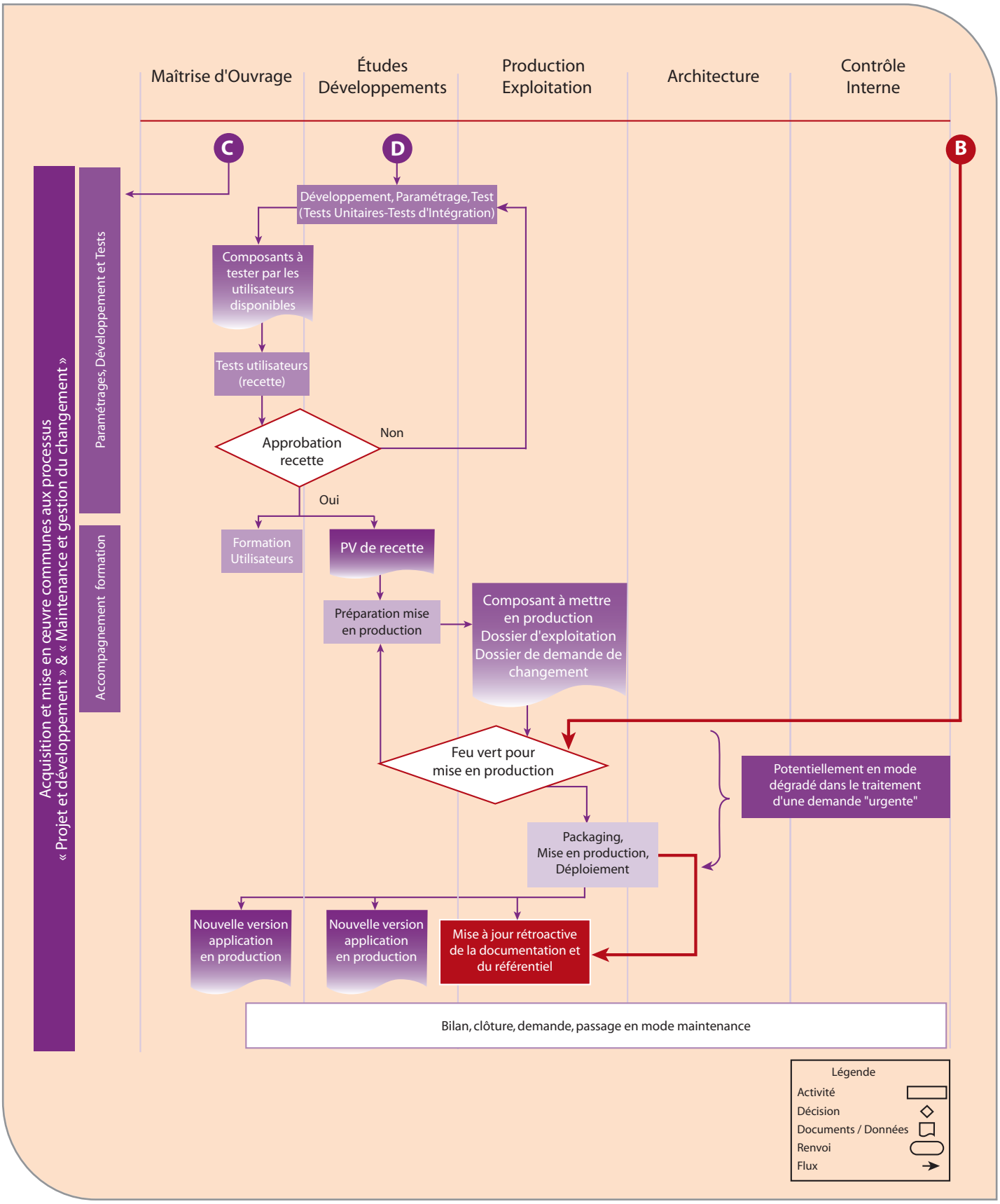
La maîtrise de ces risques repose sur les points suivants, qui constituent des meilleures pratiques :

1. Développer une stratégie de maintenance des applications : train de modifications, comité d'entrée de charge, comité de priorisation.
2. Formaliser et mettre en place une méthodologie et des procédures standardisées de gestion des changements, applicatifs et techniques, incluant également les conditions des changements urgents :
   - les rôles et responsabilités sont clairement répartis entre maîtrise d'ouvrage, études, architecture, sécurité, et exploitation ;
   - ces profils différents sont marqués dans les outils d'administration des habilitations, dont le processus est global, indépendant, transparent et auditable ;
   - les critères de priorisation des changements, s'appuyant sur une approche par les risques ;
   - les étapes successives et les livrables associés (analyse d'impact, dossier d'exploitation, dossier d'exploitabilité),
   - la procédure spécifique de gestion des changements urgents.
3. Mettre en place une séparation effective des tâches entre les « études » qui développent et testent, et la « production » qui exploite, ainsi que les moyens nécessaires :
   - les environnements de développement, de tests, et de production sont distincts ;
   - les contrôles d'accès à ces environnements sont conformes aux exigences de séparation des tâches.

5.7.1. Flowchart du processus de maintenance et gestion du changement







5.7.2. RACI du processus de maintenance et gestion du changement

Etapes clés	Maîtrise d'ouvrage	Etudes / Développements	Production Exploitation	Architecture	Contrôle interne	Livrables attendus	Processus CobiT
Enregistrement, qualification et arbitrage des demandes	I	R	C	C	C	Procédures et standards de gestion des changements	**AI2.9**
	R					Expression de besoin	**AI2.9**
	I	R	I	I	I	Reporting de suivi des changements	**AI6.4**
	AR	AR	C	C	C	Etude préalable et/ou d'opportunité	**AI2.6 AI6.2 AI6.3**
	AR	AR	I	I	I	Compte-rendu d'arbitrage du comité en charge de la maintenance de l'application ou du système Planification souhaitée	**AI6.2**
Plan de mise en œuvre	C	AR	C	I	I	Plan de mise en œuvre avec planification négociée entre MOA et MOE	**AI7.3**
Spécifications	AR	AR	A	C	C	Cahier des charges, spécifications générales Spécifications fonctionnelles et techniques intégrant les contrôles applicatifs, l'auditabilité et les contrôles de sécurité et de disponibilité	**AI2.1 AI2.2**
Préparation des plans de tests et des environnements	I	AR	I	C	C	Plans de tests unitaires par MOE	**AI7.2**
	AR	AR	C	I	I	Plans de tests utilisateurs (jeux et scénarii de tests par MOA)	**AI7.2**
	C	AR	AR	I	I	Environnements de développement, test et recette, disponibles	**AI7.4**
Réalisation	I	AR	R	I	I	Développement, paramétrage, tests (MOE) unitaires et d'intégration Feu vert pour mise en recette Plan assurance qualité	**AI2.5 AI2.7 AI2.8**
Recette	A	R	R	I	I	Validation de l'environnement de recette par les utilisateurs	**AI7.4**
	AR	R	I	I	I	Conservation des résultats des tests PV de recette	**AI7.6 AI7.7**
Accompagnement utilisateurs / Formation	R	C				Plan et supports de formation	**AI7.1**

Etapes clés	Maîtrise d'ouvrage	Etudes / Développements	Production Exploitation	Architecture	Contrôle interne	Livrables attendus	Processus CobiT
Lotissement, mise en production et déploiement	C	AR	AR	I	I	Impacts sur la production identifiés et exploitabilité validée Packages prêts pour diffusion en production Documents à jour (Dossiers d'exploitation et de configuration) Planification et feu vert pour mise en production	**AI7.8**
	I	R	AR	I	I	Applicatif disponible pour les utilisateurs	**AI7.8**
Bilan	AR	AR	C	C	C	Inventaire des anomalies résiduelles Plan d'action pour les résoudre Demande de changement clôturée	**AI7.9**

5.7.3. Matrice risques/contrôles du processus de maintenance et gestion des changements (applicatifs et techniques)

Processus	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Environnement de contrôle	AI2.10	**Maintenance des applications** Développer un plan stratégique de maintenance des applications.	Surcoût lié à un manque de planification. Ecart entre la mise en œuvre et la demande d'évolution.	Définir un processus efficace et efficient des activités de maintenance des applications. Surveiller régulièrement l'activité de maintenance et notamment les changements urgents. Maîtriser le volume d'activités de la maintenance.	Le processus de maintenance doit intégrer : • une gestion des priorités ; • les besoins métier en tenant compte des ressources disponibles ; • un logigramme formalisé ; • une analyse des risques pour évaluer les impacts de maintenance sur les systèmes et infrastructures existants, les interdépendances entre les systèmes et les exigences de sécurité. Pour faciliter la surveillance et la gestion de la maintenance : • regrouper les changements par lots ; • considérer toute maintenance conséquente comme un projet de développement. Faire une revue de tous les changements urgents qui n'adhèrent pas au processus formalisé de gestion des changements. Analyser régulièrement le modèle de maintenance retenu et le volume d'activités associé pour y déceler des tendances anormales qui indiqueraient des problèmes sous-jacents de qualité et de performance. Suivre les activités de maintenance, contrôler qu'elles ont bien été réalisées avec succès et vérifier, si nécessaire, que la documentation fonctionnelle ou technique a bien été mise à jour.

Processus	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Environnement de contrôle	AI6.1	**Standards et procédures de gestion des changements techniques et applicatifs** Formaliser et mettre en place des procédures de gestion des changements permettant une gestion standardisée des demandes de changements pour les applications, les systèmes sous-jacents, les infrastructures, les procédures et les processus. Prendre en compte les changements urgents.	Changements incontrôlés ou non autorisés. Fonctionnalités et disponibilité des systèmes dégradées. Ecarts entre les besoins et les fonctionnalités mises en œuvre.	Disposer d'une méthodologie de gestion projet de développement et de maintenance (SDLC), incluant les changements urgents. Diffuser les procédures et promouvoir leur utilisation. Se donner les moyens de contrôler leur mise en application.	Cette méthodologie doit inclure : • les rôles et responsabilités ; • les critères de classification (techniques, applicatifs) et de priorisation des changements en s'appuyant sur une approche des risques ; • les étapes successives et les livrables associés (analyse d'impact, dossier d'exploitation, dossier d'exploitabilité...) ; • la gestion des changements urgents ; • les moyens de lier les changements aux objets modifiés, recettés et mis en production (techniques et applicatifs). Intégrer l'impact lié à la sous-traitance dans le processus de gestion des changements, notamment les aspects contractuels et le respect des contraintes de conformité légales ou juridiques (CNIL, CFCI).
	PO4.11	**Séparation des tâches entre études et production** Mettre en place une séparation des tâches effective entre ceux qui développent, testent et exploitent pour assurer une distribution correcte des changements.	Changements incontrôlés ou non autorisés. Disponibilité dégradée des systèmes. Augmentation du nombre de changements en production.	Disposer d'une organisation assurant clairement la répartition des rôles et responsabilités entre études, architecture, sécurité, production et MOA pour l'ensemble du périmètre (technique et applicatif).	Disposer d'un environnement de développement de tests et de production distincts, et mettre en place des contrôles d'accès à ces environnements conformes aux exigences de séparation des tâches. Mettre en place un processus qui permette le contrôle des validations des demandes d'accès par les responsables.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage du changement	Enregistrement, qualification, arbitrage	AI2.9	**Gestion des demandes pour les évolutions applicatives** Assurer le suivi des demandes d'évolutions applicatives depuis la conception, la réalisation et la mise en œuvre en s'appuyant sur un processus d'approbation bien établi.	Ecart entre les attentes et la mise en œuvre. Mauvaise prise en compte des demandes. Demandes appliquées à un mauvais système.	Disposer d'un cadre de procédures et de standards pour encadrer la gestion des demandes de changements (réception, enregistrement et approbation). Les diffuser et promouvoir leur utilisation. Faire un suivi des demandes et donner une visibilité claire de leur état à toutes les parties prenantes.	Les procédures doivent définir les rôles et les attentes des différents acteurs. Les règles de priorisation des demandes doivent être définies afin de partager un socle d'analyse avec les clients de la DSI. Un outil de gestion des demandes permet de tracer toutes les demandes (rejetées, en cours, acceptées, terminées). Il permet également de contrôler la mise en place des demandes selon la planification prévue.
		AI6.4	**Gestion et suivi des changements techniques et applicatifs** Mettre en place un système de suivi et de reporting pour assurer le pilotage de la gestion des changements (applicatifs et techniques).	Changements non traçables. Ressources allouées insuffisantes.	Disposer d'un outil de suivi de l'ensemble des changements permettant de soutenir le processus de gestion des changements. Se donner les moyens de contrôler son utilisation.	Cet outil doit permettre : • de renseigner des informations de la demande telles que la criticité, la charge et le planning ; • de suivre le statut des changements (rejetés, acceptés, en cours, validés et déployés) ; • d'avoir une traçabilité des étapes de validation des changements par les différents intervenants ; • de prendre en compte les changements urgents.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage du changement	**Enregistrement, qualification, arbitrage**	AI6.2	**Evaluation des impacts, priorisation, autorisation** Déclarer toutes les demandes de changement via un processus structuré permettant de déterminer l'impact sur les systèmes opérationnels et sur leurs fonctionnalités. S'assurer que les changements sont systématiquement catégorisés, priorisés, et acceptés.	Effets de bord non désirés. Impacts négatifs sur la capacité et la performance des infrastructures techniques. Absence de gestion des priorités entre les changements.	Développer un processus permettant à la MOA et la DSI d'émettre des demandes de changement sur les infrastructures, systèmes et applications. Tous les changements passent par ce processus. Evaluer toutes les demandes de façon structurée : • associer les changements à des catégories et donner des priorités ; • effectuer une analyse d'impact systématique. Impliquer la MOA et la DSI dans cette évaluation. Chaque demande de changement est formellement approuvée par la MOA et la DSI.	Le processus de gestion des changements doit intégrer aussi bien les besoins fonctionnels que techniques. Les catégories de changements peuvent être de type infrastructure, système d'exploitation, réseau, applications, progiciels. L'analyse d'impact de ces changements doit porter sur : • l'infrastructure, les systèmes et les applications ; • les contraintes contractuelles, légales ou vis à vis des autorités de tutelle ; • les interdépendances avec d'autres demandes de changements.
		AI6.3	**Changements urgents** Mettre en place un processus pour définir, développer, tester, documenter, déclarer, autoriser, les changements urgents, pour lesquels on ne peut pas appliquer les processus de changements normaux.	Incapacité à répondre efficacement aux besoins de changements urgents. Autorisations d'accès exceptionnel non supprimées après le changement. Génération de changements non autorisés, suite à l'altération de la sécurité et aux accès non autorisés aux données d'entreprise.	La gestion des changements urgents est documentée et intégrée au processus global de gestion des changements. Tout changement urgent est déclaré, évalué et enregistré dans la base de gestion des changements. Toutes les ouvertures nécessaires au changement urgent sont autorisées, documentées, puis supprimées après la réalisation du changement. Faire un bilan des changements urgents en impliquant toutes les parties concernées.	Le bilan des changements urgents, doit permettre d'apporter une évaluation sur l'efficacité : • de la gestion de la maintenance des systèmes et des applications par la DSI ; • du développement et des environnements de tests ; • de la qualité des développements ; • de la documentation et les manuels ; • de l'intégrité des données.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage du changement	Enregistrement, qualification, arbitrage	AI2.6	**Mises à jour majeures des systèmes existants ou simple évolution ?** Si l'évolution demandée représente un changement significatif par rapport aux fonctionnalités du système existant, il faut alors utiliser le même processus que celui utilisé pour le développement d'un nouveau système.	Absence de maîtrise des coûts pour les grosses évolutions. Altération de la confidentialité, de l'intégrité et de la fiabilité des données traitées. Altération de la fiabilité du système.	Evaluer l'impact de toute mise à jour majeure, la classifier sur la base de critères de création de valeur métier, d'analyse de risques (impact sur les systèmes existants ...) et de coût/bénéfice. Tout changement majeur doit s'appuyer sur le même processus que celui utilisé pour le développement d'un nouveau système. Obtenir l'accord et l'approbation du responsable métier et autres parties prenantes pour considérer l'évolution comme un projet de développement.	Le propriétaire du processus métier et les autres parties prenantes doivent bien comprendre les différences d'organisation, de moyens et de délai entre une maintenance standard et une mise à jour majeure.
	Plan de mise en œuvre	AI7.3	**Plan de mise en œuvre** Définir un plan de mise en œuvre et obtenir sa validation par les parties concernées.	Allocation de ressources insuffisantes pour garantir l'implémentation effective des changements. Failles de sécurité.	Une politique de numérotation et de fréquence des versions est établie en amont. Etablir un plan de mise en œuvre qui prenne en compte une analyse des risques fonctionnels, techniques et métier. Faire valider le plan par toutes les parties prenantes (métier, études, sécurité et technique) et obtenir leur engagement et implication dans toutes les étapes de sa mise en œuvre. Identifier et documenter les scenarii de retour arrière et solutions de secours.	Le plan de mise en œuvre doit inclure : • la stratégie générale de mise en œuvre ; • les différentes étapes de mise en œuvre et leur séquencement ; • les moyens requis ; • les interdépendances ; • les critères d'acceptation par les responsables de mise en œuvre en production ; • les exigences de vérification des installations ; • la stratégie de transition pour le support aux utilisateurs et l'exploitation.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage du changement	**Plan de mise en œuvre**	AI7.5	**Conversion des systèmes et données** S'assurer que tous les éléments nécessaires au bon fonctionnement du nouveau système (matériels, logiciels, données, sauvegardes, archives, procédures, documentation…) et garantissant la compatibilité des interfaces avec les autres systèmes sont convertis de l'ancien système. Une piste d'audit des résultats avant et après conversion doit être développée et maintenue.	Les anciens systèmes ne sont plus disponibles quand on en a besoin. Perte de confiance dans le système et les résultats de la migration. Problèmes d'intégrité de données.	Définir un plan de conversion de données et de migration des infrastructures. Lors de sa mise en œuvre : • le calendrier de la bascule de la conversion est contrôlé ; • il n'y a pas eu de changement de valeur des données converties. S'il y a une nécessité absolue exprimée par le métier, documenter ces changements et avoir une approbation formelle du propriétaire des données ; • le plan de secours, le plan de continuité et le retour arrière sont pris en compte ; • les sauvegardes et archives sont effectuées et conformes aux exigences légales.	Le plan de conversion de données doit intégrer des méthodes de collecte, de conversion et de vérification des données, identifiant et résolvant toute erreur trouvée pendant la conversion. Ceci doit inclure des méthodes de rapprochement entre les données sources et les données converties afin d'assurer l'exactitude et l'intégrité des données. Pendant le développement de ce plan, passer en revue le hardware, le réseau, les systèmes d'exploitation, les logiciels, les transactions de données, les fichiers maîtres, les sauvegardes, les archives, les interfaces avec les autres systèmes (internes et externes), les procédures et la documentation systèmes. Dans la planification des conversions de données et de l'infrastructure de migration, on doit prendre en compte l'intégralité des opérations dans la définition des méthodes de développement, y compris les aspects "piste d' audit", "scenarii de sauvegardes et de retour arrière". On doit privilégier une transition douce sans perte de continuité d'activité et de données. Si nécessaire et dans l'absence d'une alternative, arrêter l'application en production le temps de la bascule.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage du changement	**Plan de mise en œuvre**	AI7.5	**Conversion des systèmes**		Les propriétaires des systèmes doivent effectuer une vérification détaillée du fonctionnement initial du nouveau système juste après son démarrage pour s'assurer que la bascule est réussie.	Sauvegardes et archives : • S'assurer qu'une sauvegarde de tous les systèmes et données a été effectuée avant la bascule de la conversion en production. Des pistes d'audit doivent être maintenues pour permettre de retracer les étapes de la conversion. Un plan de retour arrière doit être établi en cas de défaillance de la conversion. • S'assurer également que les instructions des sauvegardes et la conservation des archives sont conformes aux besoins métier et aux exigences légales ou, aux autorités de tutelles. • Considérer en même temps le plan de secours et de continuité d'activité, ainsi qu'un retour en arrière si ces considérations sont exigées par la direction des risques, le métier ou des autorités de tutelle.
Acquisition et mise en œuvre	**Spécifications**	AI2.1	**Conception générale** Traduire les exigences métiers et les impératifs techniques de développement et faire approuver les spécifications de la conception pour s'assurer que la conception répond bien aux exigences. Réévaluer les spécifications lorsque des écarts techniques ou fonctionnels significatifs apparaissent durant le développement ou la maintenance.	Spécifications non formalisées et dépendantes d'hommes clés. Périmètre du développement mal défini. Solution non conforme aux besoins métiers exprimés.	Rédiger les cahiers des charges et spécifications générales dans le respect des normes et méthodes de conception en vigueur. Les faire approuver de façon formelle par la MOA ou assimilé.	Pendant la phase de conception, impliquer : • les utilisateurs ayant une compétence métier reconnue dans le processus à faire évoluer ; • les parties prenantes de la DSI pour valider les aspects d'architecture, sécurité et contrôle interne. Ne lancer aucun développement sans approbation préalable des spécifications par la MOA.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Spécifications**	AI2.2	**Conception détaillée** Présenter en détail les spécifications générales et les impératifs techniques, en phase avec la conception générale. Réévaluer les spécifications lorsque des écarts techniques ou fonctionnels significatifs apparaissent durant le développement ou la maintenance.	Traitement incorrect des transactions ou des données. Coût supplémentaire de reconception.	Rédiger les spécifications fonctionnelles et techniques dans le respect des normes et méthodes de conception en vigueur. Les faire approuver de façon formelle par les parties prenantes (MOA, architecte).	Classifier les données d'entrée et de sortie en s'appuyant sur le référentiel de données de l'entreprise. Evaluer l'impact avec les systèmes existants et définir les principes d'intégration avec les applications internes ou tierces. Spécifier les données sources devant être collectées. Déterminer les exigences de disponibilité et définir les besoins de redondance, de sauvegarde et de secours. Définir les exigences relatives aux fichiers et bases de données par rapport au stockage, leur localisation et extraction. Définir les étapes des traitements, les types de transaction et règles de traitement (transformation, calculs...). Définir les caractéristiques des données de sortie (destinataires, usage, niveau de détail, fréquence et méthode de génération). Concevoir l'interface utilisateur et/ou interfaces entre les systèmes. Avoir une approche itérative avec la MOA, pouvant inclure un prototype, pour faciliter la compréhension de la conception finale.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Spécifications**	AI2.3	**Contrôles applicatifs et auditabilité** S'assurer que les contrôles métier sont correctement traduits dans les contrôles applicatifs de façon à ce que le traitement soit réalisé avec exactitude, complétude et dans les délais, et qu'il soit autorisé et auditable.	Contrôles compensatoires coûteux. Problème d'intégrité des données. Ecarts entre les contrôles applicatifs et risques réels. Résultats des traitements et référentiels des données non-conformes avec les besoins exprimés. Violations de la sécurité non détectées.	Intégrer la définition des contrôles applicatifs dès la phase de conception. Les faire approuver de façon formelle par les parties prenantes (MOA , contrôle interne).	Définir les contrôles embarqués dans l'application en s'appuyant sur les exigences de contrôle relatives aux processus métier définis dans le cahier des charges. Dans le cas d'un progiciel, étudier comment adapter les contrôles du processus métier à ceux intégrés dans l'application. Valider la conception des contrôles avec les parties prenantes (MOA, architecte, sécurité, contrôle interne). Les contrôles embarqués supportent les objectifs de contrôles généraux (sécurité, intégrité des données, pistes d'audit) et incluent les contrôles d'accès, les contrôles d'intégrité des bases de données. Ces contrôles reçoivent l'approbation des responsables des parties prenantes.
		AI2.4	**Sécurité et disponibilité des applications** Adresser les exigences de sécurité et de disponibilité des applications en se fondant sur une approche des risques, en s'appuyant sur la classification des données et les standards de sécurité de l'entreprise.	Violations de la sécurité non détectées. Contrôles compensatoires coûteux. Ecarts entre les contrôles de sécurité et les risques réels.	Intégrer la sécurité dès la phase de conception. Approuver les spécifications de façon formelle par les parties prenantes (MOA , sécurité).	Définir des solutions de sécurité de disponibilité dans le respect : • de la politique et des standards de sécurité de l'entreprise ; • des bonnes pratiques (ISO 17799), des obligations légales et de conformité avec les autorités de tutelle (incluant le respect de la vie privée). Prendre en compte l'infrastructure de sécurité et de disponibilité déjà en place. Traiter la gestion des droits et des privilèges, la protection des données sensibles, l'authentification, l'intégrité des transactions, les restaurations automatiques (rollback).

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Préparation des plans de tests et des environnements**	AI7.2	**Plan de tests** Définir un plan de tests et obtenir sa validation par les parties concernées afin de contribuer à un alignement entre l'expression des besoins et la solution mise en œuvre.	Tests insuffisamment automatisés. Problèmes de performance non détectés. Rôles et responsabilités des tests indéfinis.	Rédiger un plan de tests conformément au plan qualité. Communiquer et présenter le plan à la MOA ou assimilé et aux parties prenantes de la DSI.	Le plan doit prendre en compte : • les rôles et responsabilités ; • la préparation des tests (jeux et scénarii de tests) ; • l'installation ou la mise à jour de l'environnement de test ; • les tests techniques (capacité, performance, sécurité, maintenabilité) et fonctionnels ; • la documentation de validation ; • la gestion et la correction des erreurs ; • l'approbation formelle de la solution testée ; • les besoins de formation.
		AI7.4	**Environnements de tests** Disposer d'un environnement de test dédié, représentatif de l'environnement de production pour permettre une meilleure efficacité et fiabilité des tests. S'assurer que les données sensibles ne sont pas diffusées et que les résultats des tests sont conservés.	Tests insuffisamment automatisés. Problèmes de performance non détectés. Compromission de la sécurité du système.	Disposer d'un environnement de test représentatif de l'environnement de production.	L'environnement de test doit : • être représentatif de la production en matière de capacité, configuration et sécurité ; • être séparé de toute interaction avec l'environnement de production ; • contenir des données assainies si elles proviennent de l'environnement de production et qu'elles revêtent un caractère privé ou confidentiel ; • disposer de moyens de conservation des résultats des tests et de la documentation, afin de pouvoir réaliser leur revue et l'analyse telle que définies dans le plan ; • être protégé contre la divulgation.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Réalisation**	AI2.5	**Configuration et déploiement d'un progiciel** Configuration et déploiement d'un progiciel pour répondre à un objectif métier.	Augmentation de la dépendance à l'égard des personnes clés. Documentation de la configuration ne reflétant pas la configuration du système. Manque de documentation des processus métier. Echec des mises à jour matériel et des logiciels.	Examiner de façon détaillée les impacts des changements sur les applications et systèmes existants, les aspects contractuels et la personnalisation et le paramétrage. Faire approuver des spécifications relatives à la customisation et au paramétrage. Suivre une approche par étape pour valider la solution avec la MOA et les parties prenantes de la DSI avant de commencer la customisation et le paramétrage. Les procédures de tests intègrent bien les objectifs de contrôle de logiciels, à savoir : fonctionnalité, interopérabilité avec les applications et l'infrastructure existantes, les performances systèmes, les tests de charge et l'intégrité des données.	Evaluer l'impact d'une mise à jour progiciel sur des critères tels que le risque de mise en œuvre (impact sur les systèmes existants, processus ou sécurité) et le rapport coût / bénéfice. Examiner : • les problèmes d'interopérabilité avec les systèmes, technologies et infrastructures existants de l'entreprise dès la phase de conception ; • l'impact de la personnalisation du paramétrage et de la configuration sur les performances, l'efficacité et la maintenance du progiciel et des autres applications et infrastructures existantes ; • les aspects contractuels avec l'éditeur de logiciel par rapport à la personnalisation, le paramétrage et la configuration ; • la disponibilité du code source du progiciel dans le processus de personnalisation et de paramétrage. Vérifier les accords de séquestre du code source avec l'éditeur lorsque celui-ci n'est pas disponible. Evaluer les risques de non maintenance du logiciel en fin de contrat ; • le niveau de la customisation et du paramétrage nécessaire pour répondre au besoin du métier et réévaluer l'adéquation du progiciel, celui-ci pouvant avoir un impact sur la stratégie de mise à jour du progiciel.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Réalisation**	AI2.7	**Développement d'applications (Développement interne)** S'assurer que le développement des fonctions demandées est conforme aux spécifications, respecte les standards de développement et est documenté. Veiller à ce que tous les aspects juridiques et contractuels soient identifiés et traités lors de développements réalisés par des tiers.	Mauvaise utilisation des ressources. Effort non focalisé sur les besoins métier. Nombre élevé de pannes et défauts. Incapacité de maintenir efficacement les applications.	1. Mettre en place des procédures de développement conformes aux méthodologies de développement *(SDLC : Systems Development Life Cycle)*. 2. Le développement s'appuie sur les spécifications et prend en compte les exigences métier, fonctionnelles et techniques. 3. Etablir des points de contrôle et étapes de validation dans le processus de développement (points d'avancement formels avec la MOA). 4. Evaluer l'aptitude du logiciel développé à être compatible ou s'intégrer facilement aux applications et infrastructures existantes.	A la fin du développement, obtenir la validation formelle de la MOA et des parties prenantes de la DSI de toutes les fonctionnalités, de la sécurité, des performances et de la qualité. En fin d'étape, se faire confirmer auprès des responsables techniques et d'exploitation que les applications sont prêtes et aptes à être basculées dans l'environnement de production.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Réalisation**	AI2.8	**Assurance Qualité logiciel** S'assurer que les fonctionnalités mises en œuvre répondent bien aux spécifications et exigences de qualité, que ce soit en termes de développement, documentation, ou de validation. S'assurer également que les aspect légaux et contractuels sont identifiés et gérés pour les applications développées par des tiers.	Mauvaise qualité des logiciels. Répétition des tests. Tests inadaptés ou insuffisants. Détournement de données de test et compromettant la sécurité de l'entreprise. Non respect des exigences de conformité.	Définir un plan d'assurance qualité des logiciels. Concevoir un processus d'assurance qualité logiciels. Effectuer des inspections de code, des tests de cheminement des programmes et des tests applicatifs. Rapporter les résultats de ces contrôles et tests. Surveiller les exceptions de qualité. Réaliser des mesures correctives et contrôler leur mise en œuvre.	Dans le plan, sont spécifiés ou définis : • les critères de qualité ; • le processus d'assurance qualité ; • la méthode d'assurance qualité ; • les qualifications nécessaires pour assurer les fonctions de contrôleur qualité ; • les rôles et responsabilités pour la mise en œuvre de la qualité. Sont pris en compte : • l'intégration de la qualité dans le processus de développement ; • la présence ou l'absence de revues par des équipes d'assurance qualité ; • l'indépendance des contrôles vis-à-vis de l'équipe de développement. Le processus de contrôle qualité des logiciels est basé sur : • les besoins projet ; • la politique de l'entreprise ; • la méthodologie de gestion de projets.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Recette**	AI7.6	**Tests des changements** S'assurer que les changements demandés et arbitrés ont été testés dans l'environnement de test par une équipe indépendante de l'équipe de développement, conformément au protocole de recette en vigueur et avant mise en production.	Mauvaise utilisation des ressources. Dégradation générale de la sécurité. Changements influant sur les performances et la disponibilité du système.	Les tests sont conçus et réalisés par une équipe de test indépendante de celle du développement. Impliquer les propriétaires des processus métier et utilisateurs finaux. Les tests sont effectués uniquement dans l'environnement de test. Les tests et les résultats attendus doivent répondre aux critères de qualité définis dans le plan de test. Les scenarii de test (scripts) mis en œuvre doivent être clairs et doivent inclure des tests de sécurité et de performance. Les tests sont effectués, évalués et approuvés. Combiner intelligemment les tests automatisés et les tests interactifs utilisateurs. Le résultat des tests est conservé et communiqué aux parties prenantes.	Conformément au plan de test, effectuer des tests de : • sécurité, pour identifier et évaluer les faiblesses et vulnérabilités. Ces tests incluent les contrôles d'accès ; • performance de l'application, en réalisant des séries de mesures de temps de réponse (par exemple, vue par l'utilisateur final, la base de données, le système) et des tests de charge ; • sur les échecs de traitement ou de transaction (fallback et rollback). Identifier, conserver et classifier (mineur, important, critique) les bugs rencontrés lors des tests. Rendre disponible une piste d'audit des résultats des tests effectués. Les résultats des tests de non régression et des évolutions sont communiqués à toutes les parties prenantes pour faciliter la correction des bugs et l'amélioration de la qualité.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Recette**	AI7.7	**Tests finaux / Recette** Les tests s'achèvent par une recette, qui permet une évaluation et une approbation formelle des résultats des tests.	Problèmes de performance détectés. Refus des fonctions livrées par la MOA *(Business rejection of delivered capabilities).*	Les tests finaux doivent couvrir l'ensemble des composants du SI impactés par les changements. Tous les problèmes rencontrés pendant les tests ont été consignés, catégorisés et corrigés par l'équipe de développement. Les résultats des tests sont revus et documentés, puis présentés de manière compréhensible au responsable du processus métier et aux parties prenantes de la DSI, afin d'en faciliter l'évaluation. Signature d'un PV de recette par le propriétaire du processus métier et des parties prenantes de la DSI, tel que défini dans le plan de test.	Le périmètre de la recette comprend bien sûr, les composants logiciel, mais aussi les configurations, les procédures utilisateur, et les procédures d'exploitation, de suivi et de support. L'approbation formelle est obligatoire avant toute mise en production.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Accompagnement utilisateurs / Formation**	AI7.1	**Formation** Informer systématiquement : • les utilisateurs des changements fonctionnels et les former en cas d'évolution importante afin de contribuer à la bonne utilisation du système ; • l'équipe d'exploitation des changements techniques, et les former en cas d'évolution importante afin de contribuer à la bonne exploitation du système.	Incapacité de détecter rapidement les problèmes venant des systèmes ou de leur utilisation. Manque des connaissances requises dans l'exécution des tâches confiées aux utilisateurs. Erreurs résultant des nouveaux projets.	Etablir un plan de formation qui s'appuie sur un processus. Il doit : • faire partie intégrante des projets de développement ou de maintenance ; • identifier et impliquer tous les groupes concernés, aussi bien les utilisateurs finaux que les exploitants, le support technique, équipes de développement et prestataires de services. Adapter la stratégie de formation en fonction du besoin (formation des formateurs, certifications, eTraining...). Etablir des supports de formation. Evaluer la formation afin d'obtenir des commentaires pouvant conduire à des améliorations potentielles.	Le plan de formation doit : • identifier les objectifs d'apprentissage, les ressources, les principaux jalons, les dépendances et chemins critiques pouvant influencer la réalisation du plan, • identifier les membres du personnel qui doivent être formés et ceux pour qui la formation est souhaitable, • étudier des stratégies de formation en fonction du métier de l'entreprise, des risques associés (par exemple, pour des systèmes critiques, un mode formel d'accréditation de l'utilisateur susceptible d'être mis en place), et de la réglementation (par exemple, respect des lois sur la vie privée nécessitant une adaptation de la formation au niveau national). Surveiller tous les changements prévus pour s'assurer que les besoins de formation ont été examinés et que le plan de formation est adapté. Ne pas exclure de reporter les changements si la formation n'a pas été effectuée et que cela risque de mettre en péril la mise en œuvre de ces changements.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Lotissement, mise en production et déploiement**	AI7.8	**Mise en production** Après les tests, contrôler le transfert des changements du système vers l'environnement de production, conformément au plan de mise en œuvre. Obtenir l'approbation des principales parties prenantes telles que les utilisateurs, le propriétaire du système et le responsable d'exploitation. Si approprié, procéder à une marche en double (nouveau et ancien système en parallèle pendant un certain temps) et comparer le comportement et les résultats.	Pas de retour en arrière possible à la version du système d'application initiale. Systèmes exposés à la fraude ou autres actes de malveillance. Violations de séparation des droits.	Utiliser un processus formalisé pour la mise en production des changements de l'environnement de test vers l'environnement de production et mettre en place un dispositif d'approbation formel *(signoff)*. Dans ce processus de mise en production : • mettre à jour la documentation (exploitation, configuration), faire des copies des configurations avant activation du nouveau système ou des modifications en production et mettre à jour le plan de secours si nécessaire ; • archiver la version existante et la documentation, gérer la configuration des systèmes, logiciels d'application et d'infrastructure ; • conserver le code source des programmes de la version à mettre en production ; • copier tous les programmes à utiliser dans l'environnement de production. Signer un accord avec l'éditeur pour récupérer les codes source en cas de litige ou de faillite de l'éditeur.	Avoir l'approbation formelle *(signoff)* des responsables du processus métier et des parties prenantes de la DSI (développement, sécurité, architectes, assistance aux utilisateurs et exploitation) et les dates de bascule de mise en production des changements et le cas échéant, d'arrêt des anciens systèmes ou applications. Si la distribution de systèmes ou logiciels d'application est automatique, contrôler que les utilisateurs sont informés et que la distribution est déployée : • aux seules personnes autorisées et identifiées ; • dans l'environnement de destination défini ; • avec la version correcte ; • à la date d'activation approuvée. Inclure dans le processus de livraison, une procédure de retour en arrière en cas de mauvais fonctionnement ou d'erreur d'installation. Si la distribution est manuelle, maintenir un journal d'opération avec les informations suivantes : • logiciels et éléments de configuration, qui ont été distribués ; • destinataires des logiciels et éléments de configuration et localisation de leur mise en œuvre ; • les dates de mise à jour. Conserver un journal exhaustif traçant ces opérations et effectuer des contrôles sur pièce, de la distribution de l'application à la date officielle de déploiement.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Acquisition et mise en œuvre	**Bilan**	AI7.9	**Bilan de mise en œuvre** Réaliser un bilan tel que défini dans le plan de mise en œuvre, en s'appuyant sur des procédures en ligne avec les standards de gestion des changements.	Le retour sur investissement ne répond pas aux attentes du management. Incapacité d'identifier que les systèmes ne répondent pas aux besoins des utilisateurs finaux.	Mettre en place une procédure de bilan de projet. Utiliser des indicateurs d'évaluation de projet. Faire participer les responsables des processus métiers, informatiques, techniques et de contrôle interne ou de gestion des risques. Etablir un plan d'action pour traiter les problèmes identifiés.	Mettre en place une procédure de bilan de projet, pour identifier, évaluer et rapporter si : • les besoins ont été couverts ; • les avantages attendus ont été obtenus ; • le système est considéré comme utilisable ; • les attentes des intervenants internes et externes sont satisfaites ; • des impacts inattendus sur l'organisation se sont produits ; • les principaux risques ont été jugulés ; • les gestions du changement, d'installation et du processus d'accréditation ont été effectuées de manière efficace et efficiente. Consulter les responsables métier et informatiques pour définir des indicateurs de succès, la réalisation des exigences et les bénéfices obtenus. Le formulaire de bilan fait partie du processus de gestion du changement. Faire participer les propriétaires des processus métiers ou parties tiers, le cas échéant. Examiner également les exigences hors métiers ou DSI (par exemple, l'audit interne, gestion des risques de l'entreprise, la conformité réglementaire). Etablir un plan d'action pour traiter les problèmes restants, identifiés durant le projet. Faire participer les responsables métier et informatiques dans son élaboration.

5.8. Gestion des incidents

Processus-clé du support informatique, la gestion des incidents a pour objectif le rétablissement d'un service, interrompu ou altéré par un événement qui ne fait pas partie des opérations standards. La multiplication des technologies et l'interconnexion des systèmes et plateformes complexifie l'identification et le traitement des incidents : en effet, les symptômes visibles peuvent être très éloignés des causes ayant engendré un incident. De même, un incident peut entraîner une multitude d'autres incidents, qui à leur tour vont être traités par ce processus.

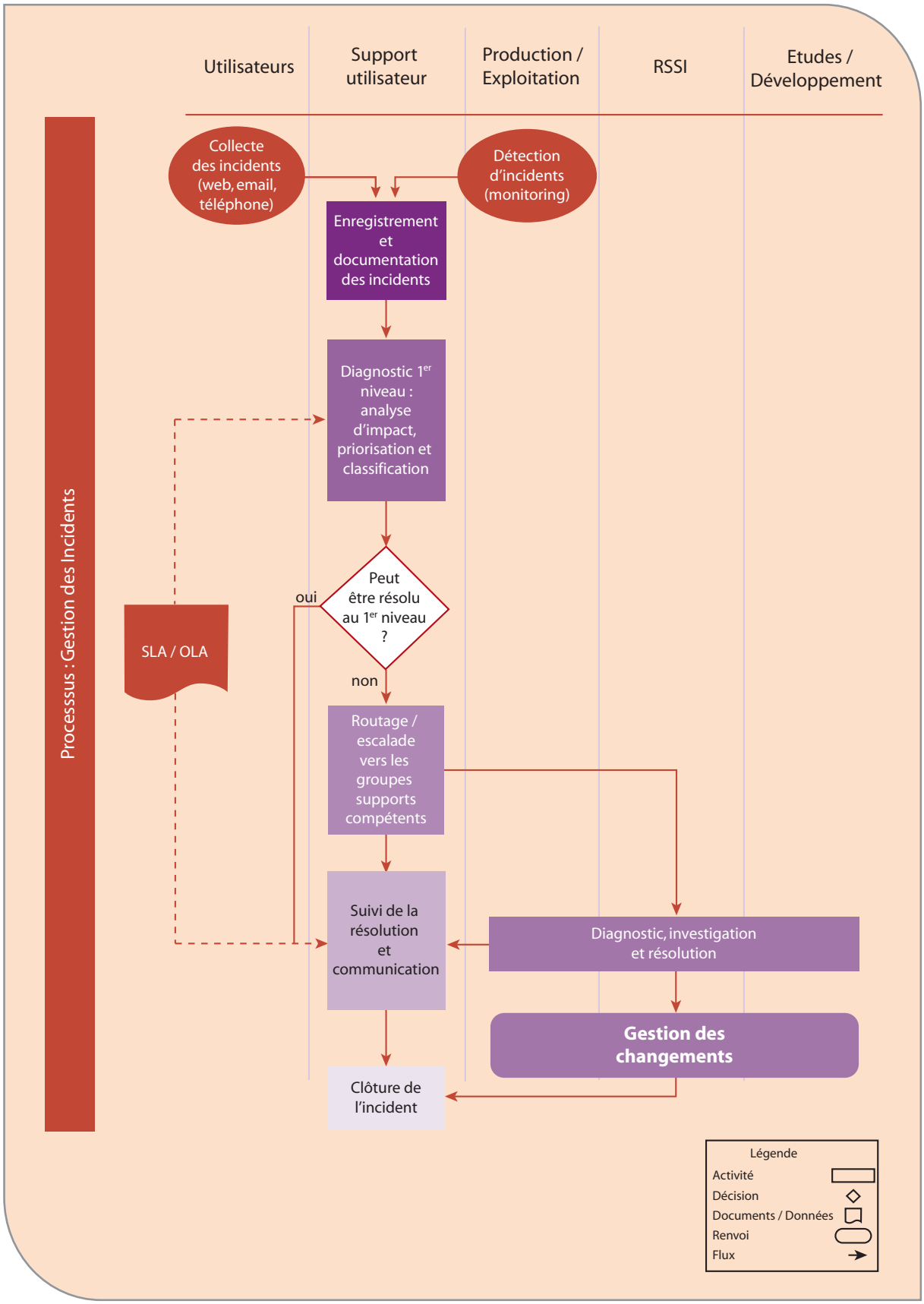
Ce contexte explique que la gestion des incidents s'interface avec de nombreux autres processus informatiques, en particulier la gestion des changements et la gestion de la sécurité.

C'est pourquoi, ce processus doit être supporté par un traitement administratif rigoureux, qui est modélisé de façon simplifiée en s'inspirant des référentiels CobiT (DS8) et ITIL (Soutien des services / Gestion des incidents). Les risques majeurs concernent le mauvais diagnostic, la lenteur de correction de l'incident ou de retour à la situation normale, le découragement des utilisateurs, et in fine l'image de marque de l'informatique.

La maîtrise de ces risques repose sur les points suivants, qui constituent des meilleures pratiques :
1. identification et priorisation des systèmes par criticité (disponibilité et intégrité) ;
2. existence, mise à jour et diffusion d'une documentation en adéquation avec tous les éléments de la chaîne (systèmes et réseaux) ;
3. formalisation, mise à jour et diffusion d'une procédure de gestion des incidents, précisant les responsabilités des différents acteurs et les indicateurs de performance ;
4. déploiement de dispositifs automatiques de surveillance et pilotage de tous les éléments de la chaîne : matériels, réseaux, systèmes d'exploitation, bases de données et applicatifs.

Enfin, notons que la gestion de crise est exclue du champ du processus analysé, en raison de la nature singulière du traitement à appliquer pour préparer et lancer les actions de reprise d'activité.

5.8.1. Flowchart du processus de gestion des incidents



5.8.2. RACI du processus de gestion des incidents

Etapes-clés du processus	Utilisateurs	Support utilisateur	Production / Exploitation	RSSI	Etudes / Développements	Livrables attendus	Processus CobiT
Déclaration d'incident utilisateur	AR	I					**DS8.1**
Déclaration d'incident exploitation (manuel ou automatique)		I	AR				**DS8.1**
Enregistrement et documentation des incidents	I	AR	I			• Fiche d'incident • Base d'inventaire et de suivi des incidents	**DS8.2**
Diagnostic 1er niveau : Analyse d'impact / priorisation classification	I	AR	C	C	C	Compte-rendu de qualification de l'incident	**DS8.2**
Routage / Escalade vers les groupes supports ad hoc	I	AR	R	R	R	Supports de routage (mail, accusé de réception…)	**DS8.3**
Diagnostic / Investigation / Résolution (Production)	I	I	AR	C	C	• Fiche d'incident mise à jour • Base de connaissances mise à jour	**DS8.3**
Diagnostic / Investigation / Résolution (Sécurité des SI / contrôleinterne)	I	I	C	AR	C	• Fiche d'incident mise à jour • Base de connaissances mise à jour	
Diagnostic / Investigation / Résolution (Etudes)	I	I	C	C	AR	• Fiche d'incident mise à jour • Base de connaissances mise à jour	
Suivi de la résolution et communication	I	AR	I		I	• Fiche d'incident mise à jour • Tableau de bord et statuts	**DS8.5**
Clôture de l'incident	R	AR	I		I	• PV d'acceptation par l'utilisateur • Fiche d'incident mise à jour	**DS8.4**

5.8.3. Matrice risques/contrôles du processus de gestion des incidents

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion des incidents	**Enregistrement et documentation des incidents**	DS8.2	S'assurer que tous les incidents connus sont déclarés. S'assurer que la description de l'incident est réalisée selon la procédure en vigueur (contenu, support…).	Non-enregistrement de l'incident. Mauvaise description ou compréhension de l'incident.	Revue périodique des fiches d'incident. Vérification de la documentation de chacun des champs prévus dans la fiche d'incident.	Existence d'une procédure de reporting des incidents à jour et diffusée auprès de tous les utilisateurs des systèmes d'information (avec un point d'entrée unique par mode de communication - téléphone / mèl / web). Existence d'une procédure "support utilisateur" d'enregistrement systématique et de documentation des incidents. Utilisation d'outils de monitoring permettant la déclaration automatisée d'incidents de production. Ces outils ont une interface avec la base des incidents. Utilisation d'un outil pour l'enregistrement et la documentation centralisés des incidents permettant la constitution d'une base d'incidents unique et centralisée ainsi que l'élaboration de tableaux de bord. Formations/informations régulières sur les procédures, les outils, les retours d'expériences et les meilleures pratiques.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion des incidents	Diagnostic de 1er niveau : - analyse d'impact - priorisation et classification de l'incident	DS8.2	S'assurer que le diagnostic est réalisé pour tous les incidents déclarés. S'assurer que le diagnostic est réalisé dans les délais prévus par la procédure en place. S'assurer que l'analyse, la classification et la priorisation sont correctement réalisées.	Analyse d'impact erronée. Priorisation inadéquate de l'incident (sur ou sous-évaluation). Classification erronée de l'incident. Diagnostic non réalisé ou réalisé tardivement. Mauvaise utilisation des systèmes due à l'ignorance de l'incident par les utilisateurs.	Revue régulière du délai de réalisation des diagnostics, identifier les cas d'anomalie de délais (pas de date, délais dépassés…). Utilisation de grilles d'analyses documentées dans la procédure et permettant l'analyse, la classification et la priorisation de l'incident. Vérification régulière de la classification de l'incident et de la priorisation de sa résolution conformes à la typologie de l'incident et au degré de sensibilité des données et/ou du système applicatif concerné.	Existence et diffusion de documentation d'aide au diagnostic incluant des grilles d'analyse. Existence de SLA / OLA en relation avec le degré de sensibilité des systèmes et des données. SLA indiquant les délais maxima pour la réalisation des diagnostics. Communication des mesures conservatoires transitoires, du délai probable de résolution vers tous les utilisateurs concernés des incidents ouverts.
	Routage et escalade vers le(s) groupe(s) support compétent(s)	DS8.3	S'assurer que tous les incidents diagnostiqués, classifiés et priorisés sont orientés vers les groupes support adéquats. S'assurer que l'escalade vers les groupes support adéquats est réalisée dans le respect des procédures en place (canal et modalités d'information, délais…).	Non-traitement des incidents par les groupes support. Traitement tardif des incidents.	Vérifier que tous les incidents diagnostiqués sont affectés à un groupe support. Vérifier l'existence d'incidents ouverts diagnostiqués sans affectation à un groupe support. Existence d'alerte sur les incidents non affectés après un délai prédéterminé selon la priorisation de l'incident.	Procédure de routage indiquant les destinataires de la notification d'incident en fonction des résultats du pré-diagnostic et procédure d'escalade en cas de non-résolution dans des délais prédéfinis (notamment dans la SLA /OLA). Outil de relance automatique.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion des incidents	**Diagnostic, investigation et résolution de l'incident**	DS8.3	S'assurer que le diagnostic, l'investigation et la résolution sont réalisés pour tous les incidents déclarés. S'assurer que le diagnostic, l'investigation et la résolution sont réalisés dans des délais prévus par la procédure en place. S'assurer que les causes primaires des incidents sont effectivement traitées. S'assurer que la résolution de l'incident ne sera pas conflictuelle avec l'activité de l'utilisateur.	Diagnostic erroné. Diagnostic tardif. Résolution non effectuée ou effectuée tardivement. Perte de temps dans la résolution des incidents par manque de capitalisation d'expérience. Récurrence des incidents connus en raison du manque de résolution de la cause primaire. Application de *"workaround / quick fix"* (solution de contourne - ment / réparation rapide) temporaire, en conflit avec les procédures ou activités utilisateurs.	Existence d'alerte sur les délais de traitement et vérification de la réalisation des relances après alerte. Obtention d'accord formel des utilisateurs selon la gravité de l'incident et en cas d'application de *"Workaround / quickfix"* (solution de contournement / réparation rapide temporaire ne réglant pas la cause primaire de l'incident).	Documentation des systèmes à jour, disponible et diffusée auprès des acteurs concernés. Expertise des équipes support (gestion des compétences). Documentation systématique de la résolution d'incident dans une base de connaissance. Documentation systématique des causes primaires des incidents dans une base de connaissance. Corréler les engagements pris vis-à -vis des utilisateurs internes avec ceux négociés avec les fournisseurs externes.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Gestion des incidents	Suivi de la résolution et communication	DS8.5	S'assurer que le statut des incidents est traçable et justifiable à tout moment. S'assurer que les séquences d'évolutions des statuts des incidents sont conformes aux engagements de qualité et de délais figurant dans les SLA et OLA. S'assurer que les engagements pris sont réalistes ou adaptés aux besoins. S'assurer que les utilisateurs sont informés régulièrement de l'avancement de la résolution de l'incident.	Utilisation inadéquate des systèmes. SLA et OLA non mises à jour en fonction des évolutions des besoins métier.	Le suivi des incidents est exploitable (actualisation régulière, en phase avec le statut d'avancement, validé par les acteurs du dispositif, supervisé) et les relances nécessaires effectuées. Analyse régulière du reporting de suivi des incidents pour vérifier si les successions de phases sont en adéquation avec les engagements pris (dont communication aux utilisateurs). Identifier les écarts pour prendre les mesures correctrices nécessaires. Vérifier que les incidents intervenant en dehors des limites fixées par les SLA ou OLA font l'objet d'une alerte.	Outil de workflow de résolution des incidents. Existence d'un tableau de bord de suivi des incidents reprenant les principaux indicateurs de performance (nombre d'incidents par typologie et systèmes concernés, productivité du support utilisateur, % d'incidents nécessitant un déplacement, durée moyenne des incidents classés par gravité, délais de résolution ou de non résolution, % incidents résolus au 1er niveau, % incidents réouverts, % incidents résolus dans les SLA, etc.). Comités de suivi réguliers entre « support utilisateur » et utilisateurs assurant la supervision des tableaux de bord, de la bonne résolution des incidents, des alertes… Mise à jour périodique des SLA/OLA, en accord avec les besoins des métiers. Capitalisation régulière sur les retours d'expérience de résolution des incidents, adaptation régulière des procédures de gestion des incidents (gouvernance ad hoc et processus d'actualisation).
	Clôture de l'incident	DS8.4	S'assurer que la résolution de l'incident est testée et validée par l'utilisateur. S'assurer que tous les incidents résolus validés sont clos.	Clôture d'un incident non résolu. Non-clôture d'un incident résolu induisant une perte de temps par les groupes support.	Signature obligatoire du PV de recette par l'utilisateur pour clôture d'un incident. Vérifier périodiquement le statut d'avancement des incidents non clos. Vérification périodique que tout incident clos a obtenu la validation de l'utilisateur (PV de recette).	Principaux indicateurs de performance (voir suivi). Communication aux utilisateurs de la clôture d'incident. Enrichissement / mise à jour des bases de connaissance et de cause principale. Vérification par le support utilisateur de ces mises à jour.

5.9. Gestion de la sécurité logique et des accès physiques

La sécurité logique et physique est un thème ancien et récurrent dès lors qu'on parle de contrôle interne des systèmes d'information : cette antériorité ne signifie pour autant pas que ce sujet soit parfaitement sous contrôle. Au contraire, il convient dans chaque organisation de comprendre et qualifier les vulnérabilités et les menaces, afin de construire la réponse adéquate en matière d'exigences de sécurité devant peser sur le système d'information.

Notre définition de la sécurité logique comprend la confidentialité, la disponibilité et l'intégrité de l'information, des applications et de l'infrastructure informatique. Le champ de la sécurité physique a été limité au sujet des accès non autorisés.

C'est pourquoi, les activités de contrôle que nous décrivons ont pour finalité de s'assurer que les services informatiques sont capables de résister à des attaques et d'en surmonter les effets, notamment pour garantir la mise à disposition de données intègres, en empêcher une divulgation inappropriée, et contribuer à la continuité de l'activité de l'entreprise.

Les conditions préalables au déploiement du processus de gestion de la sécurité logique et des accès physiques concernent l'existence d'une politique de sécurité SI et la mise en place d'une organisation assurant son déploiement et sa mise à jour.

Les entreprises et les administrations publiques doivent fonder leur approche de la sécurité informatique sur un corps de règles et de directives, visant à structurer et faire connaître « la politique de sécurité des systèmes d'information » et décrivant l'ensemble des principes fondateurs, les vulnérabilités identifiées, les objectifs de protection et les règles à appliquer avec leur niveau d'exigence :

- les directives, dont l'application est impérative ; le non-respect d'une directive ne peut être que transitoire et doit donner lieu à une dérogation formalisée ;
- les recommandations, qui ont pour vocation à s'appliquer le plus largement possible sur le SI de l'entreprise.

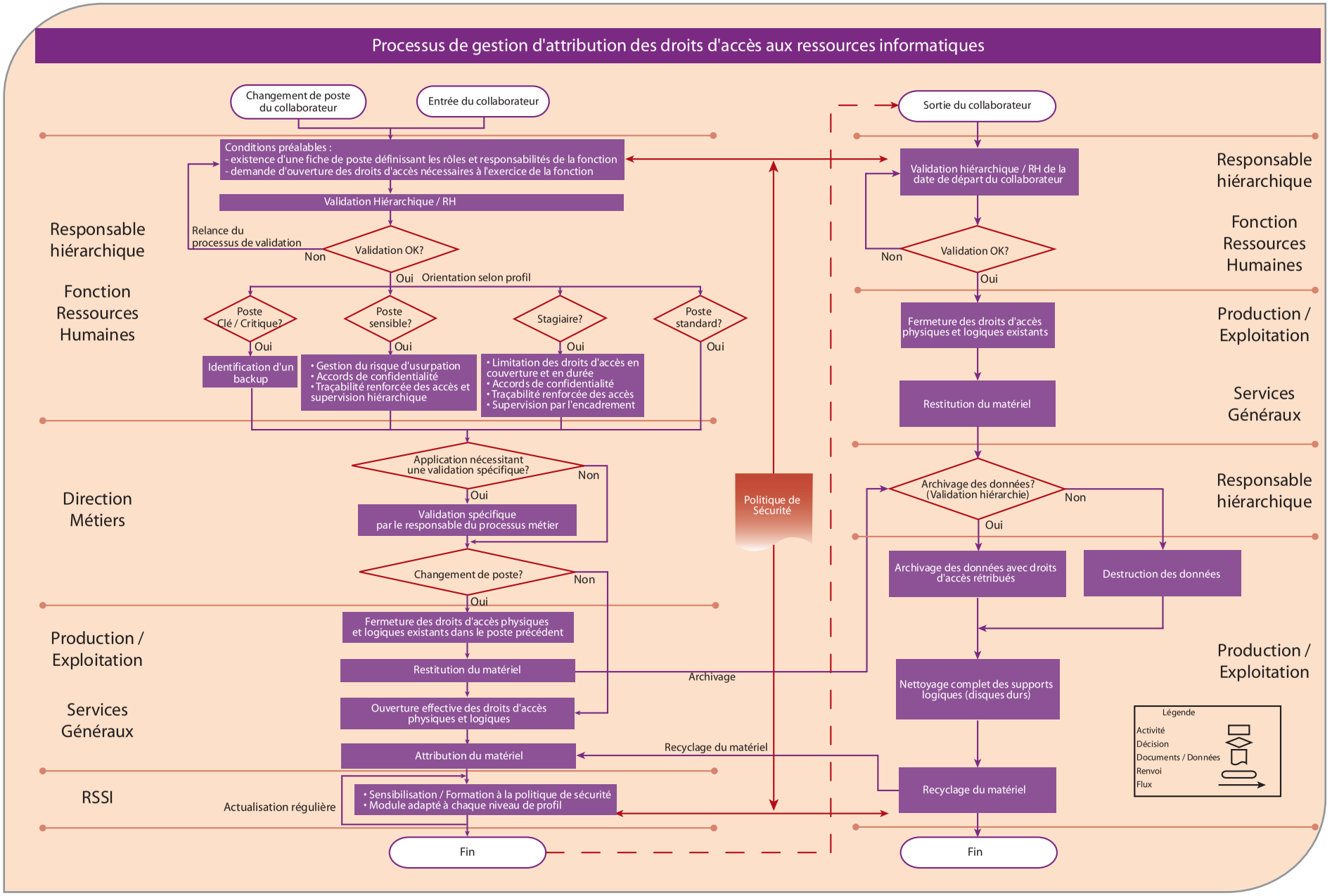
Cette politique est déclinée en objectifs de contrôle permettant d'évaluer la réalité de son déploiement et son efficacité.

La politique définie est déployée et mise à jour par une organisation adaptée, couvrant tout le domaine de la sécurité SI. Cette organisation dédiée est chargée de légiférer et de contrôler la bonne application de la politique. Elle doit disposer d'un rattachement lui garantissant un niveau d'indépendance adéquat, notamment vis-à-vis des opérations.
La politique et l'organisation doivent couvrir quatre thèmes clés :

1. La gestion des risques, fondée sur l'évaluation et la réduction des risques.
2. La qualification de l'information, fondée sur une classification de l'information destinée à adapter le niveau de protection de celle-ci.
3. La conformité des systèmes avec les politiques et standards de sécurité en vigueur.
4. La sensibilisation à la politique de sécurité SI, fondée sur une communication adéquate auprès de chaque employé (en modes *"push et pull"*).

Sur ces quatre thèmes, les managers ont un rôle important pour s'assurer que l'application des procédures dont ils sont responsables est accomplie en pleine conformité avec les référentiels.

5.9.1. Flowchart du processus de gestion d'attribution des droits d'accès



5.9.2. RACI du processus de gestion de sécurité logique et des accès

Etapes-clés du processus	DSI	Etudes / Développements	Production / Exploitation	Directions métiers	RSSI	Commentaires	Processus CobiT
Organisation de la Direction des systèmes d'information	A	R	R	R	I	Définit le rattachement de la sécurité SI	**PO4**
Définition de la politique de sécurité et des règles de sécurité	A	I	I	I	R		**PO6**
Sensibilisation à la politique de sécurité	I	C	C	R	A	Les responsables opérationnels doivent être largement impliqués	**PO6 / DS7**
Conformité des systèmes avec la politique de sécurité	A	R	R	C	I		**DS5**
Gestion des Risques	A	R	R	R	C	Implication directe du DSI dans l'animation du processus	**PO9**
Sécurité physique (accès aux locaux)	A	I	R	C	C		**DS12**
Gestion des accès utilisateurs	I	A	A	R	C	Approuve chaque acteur dans son domaine	**DS5**
Accès aux programmes et aux données	I	A	A	R	C	Approuve chaque acteur dans son domaine	**DS5**
Surveillance des accès logiques	A	I	R	R	I	Les responsables opérationnels doivent être largement impliqués	**DS5**
Sécurité réseaux	A	I	R	I	C		**DS5**
Séparation des infrastructures	A	I	R	I	C		**DS5**
Gestion des failles de sécurité	I	C	R	I	A		**DS5**
Gestion des services rendus par un tiers	A	R	R	R	C		**DS2**
Gestion des certificats	A	C	C	I	R		**DS5**
Gestion des incidents	A	I	R	I	R		**DS5**
Robustesse du dispositif de protection	A	R	A	C	R	Approuve chaque acteur dans son domaine	**DS5**

5.9.3. Matrice risques/contrôles du sous-processus d'accès aux programmes et aux données

Processus	N° de réf CobiT ISO 27001	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Accès aux programmes et aux données	DS5 ISO 11	S'assurer que les processus existants permettent d'identifier tous les utilisateurs (internes et externes) du système.	Les utilisateurs non identifiés peuvent faire des changements non autorisés dans les programmes et les données.	S'assurer que tous les utilisateurs s'identifient pour accéder aux systèmes d'information.	Le principe admis est que toute personne physique doit pouvoir être associée à un et un seul login. Ainsi, il ne devrait pas exister de comptes génériques, utilisés par plusieurs utilisateurs. Toutefois, pour traiter les cas où le principe n'est pas respecté (besoins métiers), une procédure est mise en place afin de recenser et justifier l'ensemble des comptes et de faire valider la liste par le responsable métier. Les comptes de service (comptes applicatifs, réseau) sont nécessaires mais ils ne doivent pas être utilisés en transactionnel par des utilisateurs.
	DS5 ISO 11	S'assurer que les processus existants permettent d'authentifier tous les accès aux programmes et aux données.	Transactions non autorisées par les utilisateurs dont l'accès n'a pas été authentifié.	Vérifier que toute procédure de login (application, système d'exploitation, base de données) prévoit une authentification par mot de passe ou est associée à une authentification forte **en accord avec la politique de sécurité de l'information.**	Système de gestion de certificats ou clés permettant d'authentifier de façon unique un utilisateur, un système ou une application. Pour le cas des authentifications fortes, une politique d'utilisation de dispositifs de cryptage pourra être définie et implémentée. Par ailleurs, en cas de rupture du service de PKI *(private key infrastructure)*, une procédure dégradée, prévoyant des mécanismes d'autorisation, est prévue et mise en œuvre. Le service concerné peut être rendu inaccessible. Toutes les exigences de sécurité identifiées devraient être satisfaites avant d'autoriser l'accès à l'information par des tiers et être prises en compte dans les accords correspondants. Des méthodes d'authentification appropriées devraient être utilisées pour contrôler l'accès des utilisateurs distants. La conformité du système d'information avec la politique de sécurité est vérifiée périodiquement, les rapports sont formalisés, datés et validés.

Processus	N° de réf CobiT ISO 27001	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Accès aux programmes et aux données	DS5 ISO 11.2 & 11.6.1	S'assurer que le management applique les procédures adéquates pour la création, la modification ou la suppression des comptes utilisateurs.	Absence d'assurance que les accès au système (applications, bases de données et systèmes d'exploitation) sont autorisés, appropriés et valides.	Vérifier que les demandes d'attribution de droits d'accès aux utilisateurs nécessitent une autorisation préalable de la part du management. Le processus de création/modification de comptes utilisateur inclut une étape de validation du respect du référentiel de séparation des tâches. S'assurer qu'il existe des contrôles compensatoires pour les éventuelles dérogations à la politique de séparation des tâches (Cf. flowchart « processus de gestion d'attribution des droits d'accès », p. 121). Vérifier qu'un processus de traitement des cas d'urgence est identifié et respecté.	Définition de profils donnant des droits d'accès ou associés à un ensemble de transactions. Attribution des droits d'accès après autorisation et en fonction des besoins métier et des règles de séparation des tâches. Les cas de non-respect de la politique de séparation des tâches devraient donner lieu à une correction immédiate ou à la documentation d'un contrôle compensatoire. Analyse périodique et aléatoire des accès aux données de production par les utilisateurs privilégiés et super privilégiés. Les procédures sont les mêmes pour le personnel informatique et pour les utilisateurs. Sur la base d'une analyse de risque, l'entité peut décider d'inclure ou non la validation des pouvoirs spéciaux (utilisateur privilégié et super privilégié). Une procédure particulière doit être mise en œuvre pour s'assurer de la mise à jour des droits des utilisateurs en cas de changement de fonction ou de départ de l'organisation. L'initiation de ces mises à jour pourra être réalisée par le département RH.
	DS5 ISO 11.2.4	S'assurer que le système de revue périodique des comptes et des accès est opérationnel.	Existence de comptes multiples ou d'anciens droits non compatibles avec la séparation des tâches. Accès étendus qui ne sont pas couramment utilisés.	Vérifier que la DSI adresse régulièrement aux directions métiers des informations sur les comptes et les droits d'accès à leur système. S'assurer que les directions métiers valident ces informations, notamment en ce qui concerne la cohérence de l'affectation des profils et des rôles. Vérifier que la DSI a mis en œuvre les modifications apportées par les métiers.	La gestion d'une date de fin de validité des droits d'accès pour les prestataires (si le système le permet) permet de s'assurer périodiquement que les utilisateurs concernés ne disposent plus d'accès au système après cette date.

Processus	N° de réf CobiT ISO 27001	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Accès aux programmes et aux données	DS5 ISO 10.1.3	Assurer la gestion de la séparation des tâches et des profils. L'application du principe de séparation des tâches doit faire l'objet d'une validation attentive concernant les transactions sensibles.	Non respect du principe de séparation des tâches.	Vérifier qu'une analyse de risques a permis d'identifier les comptes utilisateur pour lesquels la validation du respect du référentiel de séparation des tâches doit exister.	Le contrôle de la séparation des tâches peut être préventif, lors de la création ou de la modification, ou détectif, via des revues périodiques. Le contrôle préventif permet de réduire plus efficacement l'exposition au risque de fraude qu'un contrôle détectif.
	DS5 ISO 11.2.2 & 11.5.4	Assurer la gestion des comptes privilégiés et super privilégiés et l'utilisation des outils système.	Changements inappropriés de la configuration du système et des données critiques.	Vérifier que les accès aux comptes privilégiés et super privilégiés (système d'exploitation, base de données et applications) sont restreints au seul personnel ayant l'autorisation de les utiliser. S'assurer que l'utilisation de programmes capables d'outrepasser les contrôles systèmes et applicatifs est restreinte et rigoureusement contrôlée.	Sur la base d'une analyse de risque, les accès à des transactions sensibles sont soumis au même processus d'autorisation que le processus standard de gestion des droits d'accès. Les profils étendus ne sont pas accessibles en temps normal. La liste des utilisateurs ayant des droits étendus (système et base de données) est révisée tous les mois.
	DS5 ISO 10.1.4	Assurer la séparation des infrastructures hébergeant les activités de développement, de test et d'opérations d'exploitation courantes.	Perturbations de service. Accès non autorisé au système.	Vérifier l'isolement des réseaux supportant l'activité des utilisateurs et des opérations informatiques. S'assurer que les systèmes critiques sont isolés dans un environnement physique et logique dédié.	La sélection des systèmes critiques s'appuiera sur le résultat du processus de qualification des informations.

Processus	N° de réf CobiT ISO 27001	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Accès aux programmes et aux données	DS5 ISO 12.6.1	Maîtriser les vulnérabilités techniques.	Accès non autorisé au système. Indisponibilité du système.	S'assurer que des tests d'intrusion sont régulièrement mis en œuvre pour identifier et réduire les zones de vulnérabilité effectives. Vérifier que les informations sur les vulnérabilités techniques des systèmes d'information sont obtenues à temps, l'exposition de l'organisation à ces vulnérabilités évaluée, et les mesures appropriées mises en place.	Un dispositif de veille approprié doit être mis en place, notamment concernant la stricte implémentation des patches de sécurité recommandés par les constructeurs et les fournisseurs de logiciels.
	DS12 ISO 9.1.2	S'assurer que l'accès aux salles informatiques est restreint et que les règles de sécurité sont définies et respectées.	Pertes sur les données critiques.	Vérifier que l'accès aux locaux informatiques est contrôlé et qu'il existe un processus d'autorisation. La liste des personnes ayant accès aux salles informatiques est revue périodiquement et les corrections nécessaires sont effectuées. Lorsqu'il existe des dérogations aux politiques de gestion des accès, ces dérogations sont documentées.	Les prestataires externes sont accompagnés lors de leurs interventions. La procédure traite des cas d'urgence. La liste des accès est revue tous les mois, elle est datée et signée par le manager approprié. Des mesures spécifiques concernent les interventions de la sécurité, de l'entretien de la DSI et du personnel assurant la maintenance technique. Tout équipement sensible doit être hébergé dans une salle informatique appropriée.
	DS5 ISO 10.1.1 & 10.1.2	S'assurer de la documentation des opérations d'exploitation et de gestion des changements.	L'erreur pouvant entraîner l'indisponibilité du système ou l'altération de données.	Vérifier que les procédures opérationnelles sont documentées, maintenues et rendues disponibles à tous les utilisateurs qui en ont l'utilité. S'assurer que les changements effectués sur les infrastructures sont contrôlés et qu'ils peuvent être tracés.	*Standard Operating Procedure* (SOP) Les procédures standard permettent d'assurer la transmission des pratiques à de nouvelles équipes, notamment à des équipes externes intervenant en cas de crise. Elles favorisent la continuité de service.

Processus	N° de réf CobiT ISO 27001	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Accès aux programmes et aux données	DS5 ISO 10.4.1	Protéger l'intégrité de l'information en limitant notamment la propagation de code malveillant.	Vulnérabilité à la modification, à la destruction, à l'indisponibilité ou au vol des informations hébergées.	Des contrôles de détection, de prévention et de rétablissement sont mis en place pour se protéger des codes malveillants. Vérifier l'existence et la mise en œuvre de procédures d'information des utilisateurs.	Un dispositif antivirus devrait être installé sur l'ensemble des postes de travail de tous les utilisateurs et sur l'ensemble des serveurs. Pour disposer de la base de signature anti virale la plus large, le recours à plusieurs éditeurs de solution est conseillé. Un dispositif permettant la détection de transactions ou d'échanges de données non autorisés devrait être mis en place, notamment au niveau des passerelles entre le réseau d'entreprise et Internet (web et messagerie).
	DS5 ISO 10.7.2	Maîtriser la confidentialité des données lors de la mise au rebut d'un matériel de stockage.	La présence de données résiduelles sur les supports de stockage peut entraîner la divulgation d'informations.	Les supports de stockage de données devraient être mis au rebut de manière certaine et sûre lorsqu'ils ne sont plus utiles, en respectant des procédures formelles de destruction définitive des données contenues.	Cette activité est liée à la notion de classification de l'information. Cet aspect doit également être pris en compte lors de prêt de matériel dont les dispositifs de stockage doivent faire l'objet de nettoyage préalable.
	DS5 ISO 10.8.4	Maintenir la sécurité de l'information échangée à l'intérieur de l'organisation ou avec une entité externe.	La transmission d'informations sensibles par messagerie électronique, en particulier via Internet, peut entraîner leur divulgation.	L'information contenue dans les messages électroniques devrait être convenablement protégée.	Chiffrer les fichiers sensibles échangés. Signature par l'entité externe d'accords de confidentialité *(Non Disclosure Agreement)*.

Processus	N° de réf CobiT ISO 27001	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Accès aux programmes et aux données	DS5 ISO 10.10.1	Permettre la détection d'activités de traitement de l'information non autorisées et tracer les incidents de sécurité.	Sans consignation des évènements liés à un système, la traçabilité des opérations ou des accès effectuées sur ce système n'est pas assurée.	Les journaux contenant l'enregistrement des activités des administrateurs du SI, des utilisateurs, les exceptions, les erreurs et les évènements de sécurité de l'information devraient être produits et conservés pour une période prédéfinie par l'organisation. S'assurer que les traces (log) font l'objet d'analyse régulière, notamment sur les transactions dites "sensibles". Vérifier que les évènements journalisés sont régulièrement revus et analysés.	Les équipements de journalisation et les évènements consignés devraient être protégés contre les accès non autorisés et les falsifications. Les erreurs et les évènements de sécurité doivent déclencher des actions appropriées de traitement des incidents. Les horloges de tous les systèmes de traitement de l'information journalisés devraient être synchronisées sur une source de temps précise et agréée.
	DS5 ISO 11.5.5 & 11.5.6	Limiter les risques d'accès non autorisés à un système laissé sans surveillance.	Sans limitation de la durée du temps de connexion, une session active peut être utilisée pour accéder à une application sensible par une personne non autorisée.	Les sessions inactives devraient être désactivées automatiquement après une période définie d'inactivité. Des restrictions du temps de connexion devraient être utilisées pour fournir un niveau de sécurité additionnel pour les applications les plus sensibles.	Ces principes concernent les accès au réseau et les accès aux applications.

5.10. Gestion de la sous-traitance et infogérance

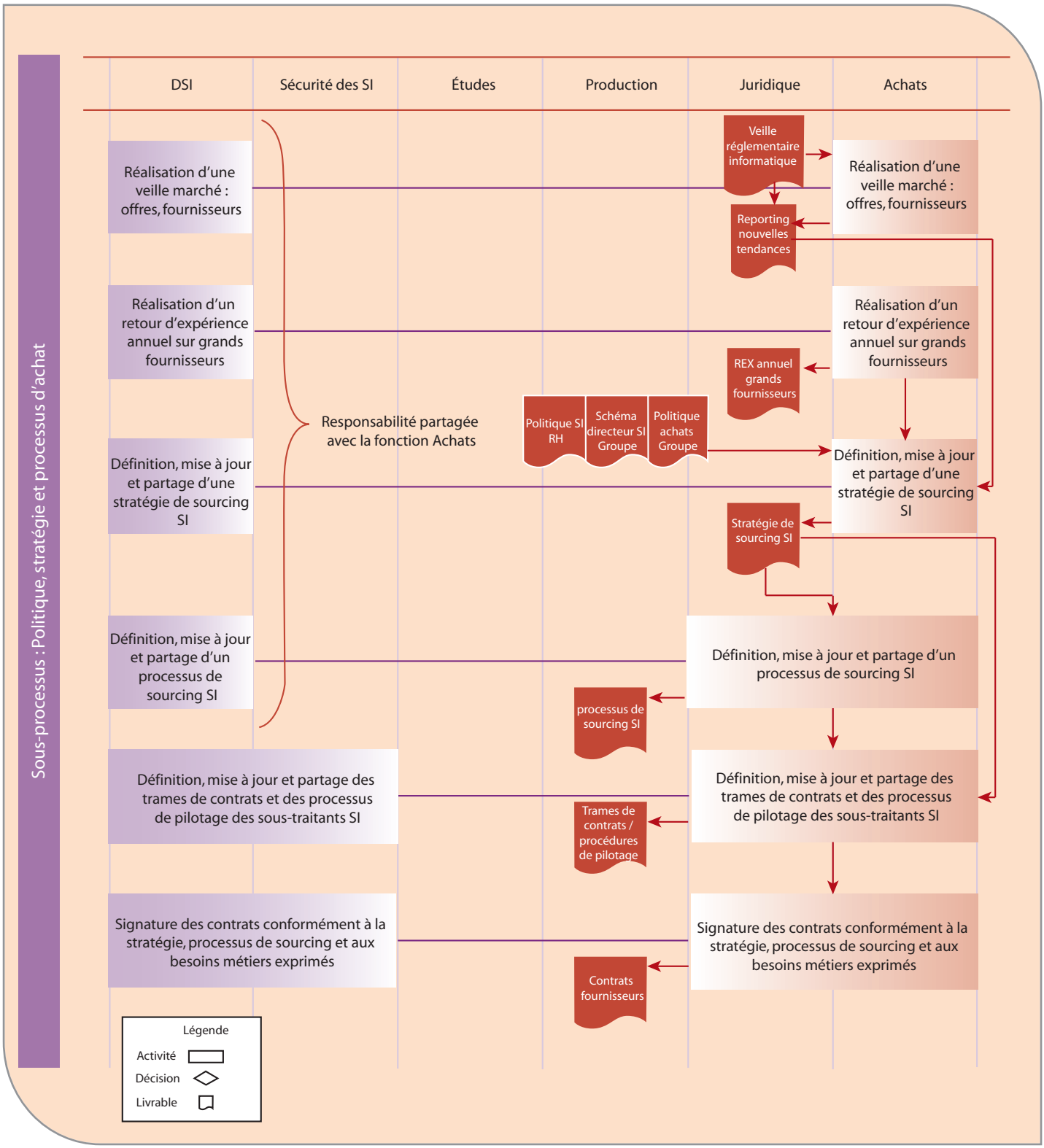
Si la gestion de la sous-traitance est une problématique générale d'entreprise, elle doit faire l'objet d'une gouvernance spécifique au sein de l'informatique, compte tenu de son poids élevé, de son extension à quasiment tous les domaines, et de la complexité des contrats, alors même que croît continûment la criticité du SI dans le fonctionnement global de l'entreprise ou de l'administration. En effet, la sous-traitance informatique est passée d'un mode d'achat de prestations avec obligation de moyens (jadis appelée régie) vers un mode d'achat de services avec obligation de résultats (par exemple, pour les projets d'intégration de systèmes ou d'infogérance récurrente).

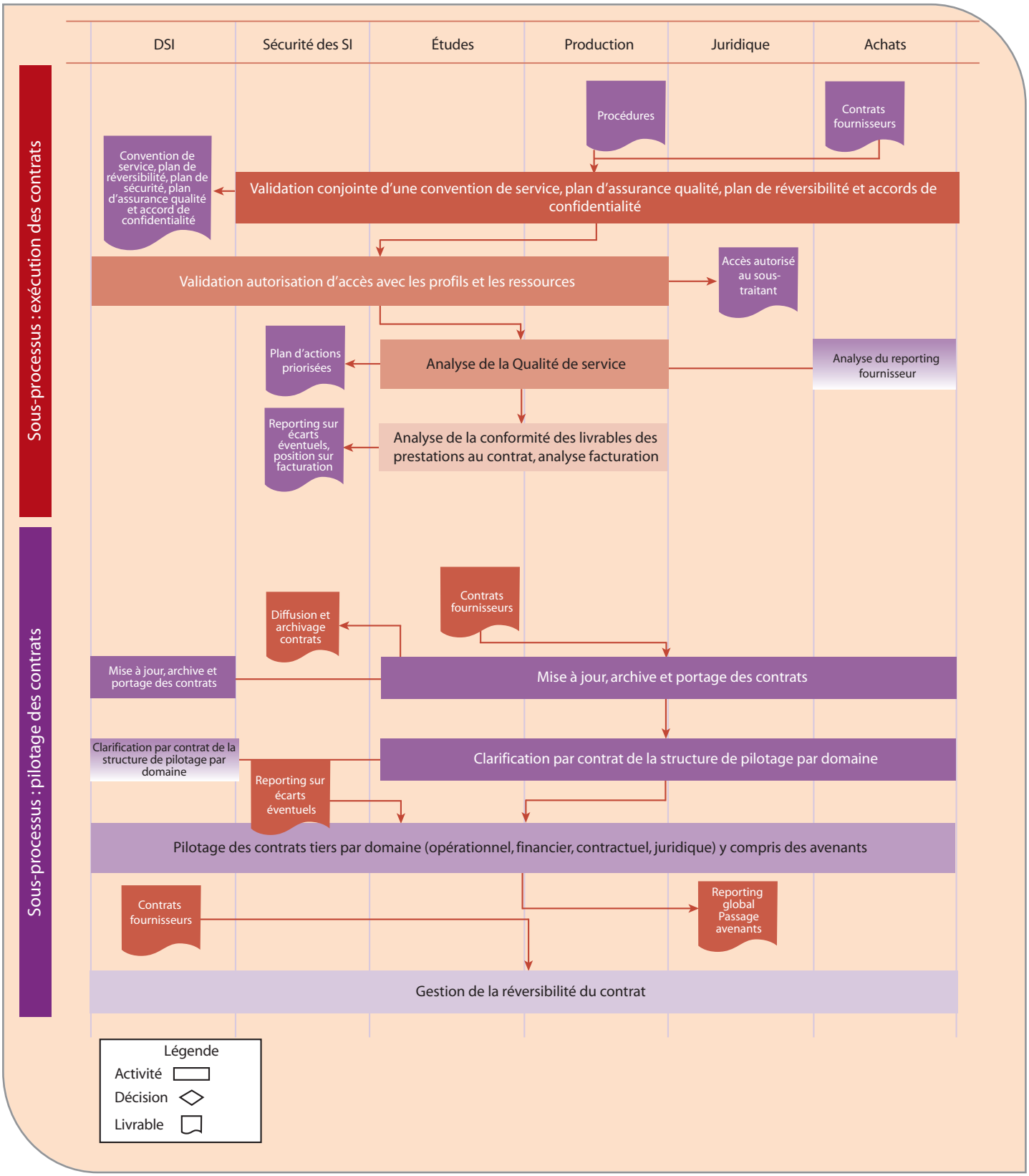
Parallèlement à cette évolution, s'ajoute le phénomène de délocalisation qui, au-delà des effets de mode, peut générer de véritables opportunités en matière de réduction des coûts, à condition de considérer de façon globale et transparente les problèmes des différences culturelles, des barrières linguistiques, des fuseaux horaires, des distances géographiques, voire des expertises techniques, et d'intégrer leur résolution dans la construction des solutions envisagées.

C'est pourquoi, la maîtrise de la sous-traitance est devenue une préoccupation essentielle des DSI, dans l'accomplissement de l'ensemble de leur mission qui vise à concevoir, maintenir et exploiter des systèmes complexes, répondant aux besoins des métiers au meilleur rapport qualité/coût. La sous-traitance moderne s'étend donc à tous les processus de production des systèmes d'information, depuis la réalisation des projets jusqu'à la maintenance et l'exploitation des systèmes, tout en intégrant les aspects de sécurité et de performance.

La gestion de la sous-traitance se fonde sur quatre préalables : un schéma directeur des SI, une politique RH SI, une politique globale d'achats, et une identification des niveaux de service (performance et continuité de fonctionnement) nécessaires aux métiers. Leur combinaison débouche sur la mise en place de contrats de service internes, d'une stratégie « *make or buy* » et d'un processus de « *sourcing* » : on y inclut la sélection des prestataires, la signature des contrats, et le suivi de leur exécution, trois composantes majeures du pilotage de la performance de la sous-traitance.

5.10.1. Flowchart du processus de gestion de la sous-traitance





5.10.2. RACI du processus de sous-traitance

Etapes-clés du processus	DSI	Sécurié des SI	Etudes	Production	Juridique	Achats	Livrables majeurs de sortie	Commentaires
Processus : stratégie et processus de sourcing SI								
Réalisation d'une veille marché : offres, fournisseurs	AC					R	Reporting sur nouvelles tendances, offres, fournisseurs	Les managers informatiques (sous responsabilité DSI), contribuent à cette veille via leurs contacts.
Réalisation d'un retour d'expérience annuel des grands fournisseurs	AC					R	Retour d'expérience annuel grands fournisseurs	Les managers des différentes entités sous la responsabilité DSI, contribuent au retour d'expérience au travers des prestations dont ils avaient la responsabilité du pilotage.
Définition, mise à jour et partage d'une stratégie de sourcing SI	A					R	Stratégie de sourcing SI	
Définition, mise à jour et portage d'un processus de sourcing	A				C	R	Processus de sourcing SI	
Définition, mise à jour et partage de trame de contrats et des processus de pilotage des sous-traitants SI	AC				C	R	Trames de contrats et procédures de pilotage des sous-traitants SI	Les managers informatiques (sous la responsabilité DSI), contribuent à l'établissement / mise à jour des processus de pilotage des sous-traitants au travers des retours d'expérience réalisés sur le pilotage des prestations dont ils ont la responsabilité. Les accords de confidentialité peuvent être proposés dès cette étape.
Signature des contrats conformément à la stratégie, au processus de sourcing et aux besoins Métiers exprimés	AC				C	R	Contrats établis conformément à la politique de sourcing et aux besoins Métiers	Les managers informatiques (sous la responsabilité DSI), contribuent au passage des contrats, lesquels sont validés par le niveau ayant le pouvoir d'engagement financier adéquat.

Etapes-clés du processus	DSI	Sécurié des SI	Etudes	Production	Juridique	Achats	Livrables majeurs de sortie	Commentaires
Processus : exécution des contrats								
Validation conjointe d'une convention de service, d'un plan de réversibilité, d'un plan de sécurité, d'un plan d'assurance qualité et accords de confidentialité	A	R	R	R	C	C	Convention de service, plan de réversibilité, plan de sécurité, plan d'assurance qualité validés Accords de confidentialité signés	
Validation autorisation d'accès avec les profils et les ressources	A	R	C	C			Accès autorisé au sous-traitant	
Analyse de la qualité de service fournisseur			A	A		C	Plan d'action priorisé pour anticiper / remédier aux éventuels dysfonctionnements	
Analyse de la conformité des livrables au contrat, analyse facturation	A	RC	R	R			Reporting sur écarts éventuels avec étude d'impact et plan d'action Position sur facturation	

Etapes-clés du processus	DSI	Sécurié des SI	Etudes	Production	Juridique	Achats	Livrables majeurs de sortie	Commentaires
Processus : pilotage des contrats								
Mise à jour, archivage et portage des contrats	A		I	I	R	C	Diffusion de la liste des contrats cadres Archivage des contrats	
Clarification par contrat de la structure de pilotage par domaine	A		C	C	R	C	Documentation et portage de la structure de pilotage	
Pilotage des contrats tiers par domaine (opérationnel, financier, contractuel, juridique) y compris des avenants	A	C	R	R	R	R	Reporting global intégrant avenants et plan d'actions associé Avenants contrat	
Gestion de la réversibilité du contrat	A		C	C	R	C	Définition et suivi du processus de réversibilité	

5.10.3. Matrice risques/contrôles du processus de sous-traitance

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Stratégie et processus de sourcing	Veille marché : offres, fournisseurs	DS2 : gérer les services tiers	S'assurer de l'existence d'un processus approprié de veille du marché.	Veille inappropriée ou inexistante.	Revue de l'existence d'une non veille fournisseurs. Mesure de satisfaction des managers des livrables fournis par le processus de veille fournisseurs.	Existence d'un processus de veille qui permette d'anticiper des ruptures dans tous les domaines SI pertinents au regard des enjeux Métiers. 90% des managers sont satisfaits des livrables fournis par le processus de veille fournisseurs.
	Retour d'expérience des grands fournisseurs		S'assurer de l'existence et de la pertinence des retours annuels grands fournisseurs réalisés.	Retours d'expériences inexistants ou inadéquats.	Revue de l'existence d'un retour d'expérience annuel par grand fournisseur, qui tient compte des réserves majeures émises et des litiges.	Existence de retours d'expérience annuels réalisés sur l'ensemble des grands fournisseurs et synthétisant de façon objective les forces et fragilités décelées sur la base d'un système de notation partagé.
	Stratégie de sourcing SI		S'assurer de l'existence, de la mise à jour et d'un partage d'une stratégie de sourcing SI, alignée avec le schéma directeur SI Groupe, la politique SI RH et la politique achats.	Stratégie de sourcing SI inadéquate ou inexistante. Stratégie de sourcing SI non partagée.	Revue de l'existence d'une stratégie de sourcing SI , répondant aux points majeurs suivants : • alignement avec les besoins du schéma directeur SI Groupe, la politique SI RH définissant les activités à externaliser, la politique achats ; • clarification par domaine, des spécificités d'achat (prestation clé en main, partenariat), de la liste de fournisseurs, des besoins à couvrir... ; • validation par les membres adéquats : DSI, Dir achat, Dir RH. Mesure de l'appropriation de cette stratégie par les managers de la DSI.	Existence d'une stratégie de sourcing formalisée, correctement validée et mise à jour avec les besoins du schéma directeur SI Groupe et anticipant les besoins, de façon à garantir une massification et des conditions d'achats plus attractives. Stratégie de sourcing connue de l'ensemble des acteurs concernés.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Stratégie et processus de sourcing	Processus de sourcing	DS2 : gérer les services tiers	S'assurer de l'existence, de la mise à jour d'un processus de sourcing SI adéquat et de son portage.	Processus de sourcing inadéquat, non partagé.	Revue de l'existence d'un processus de sourcing SI clarifiant comment se fait l'identification du besoin, les règles de mise en concurrence, l'analyse des offres, la traçabilité de la phase de décision (acteurs impliqués et en ligne avec les processus d'achat). Mesure de l'appropriation des acteurs impliqués dans sa mise en œuvre.	Existence d'un processus de sourcing SI formalisé et déclinant la politique d'achat de l'entreprise ou de l'administration. Appropriation de la politique de sourcing SI par l'ensemble des acteurs concernés.
	Trames de contrats et processus de pilotage des sous-traitants SI		S'assurer de l'existence et d'un partage de trames de contrats adaptés reprenant le processus de pilotage des sous-traitants.	Trames de contrats de sous-traitance inadaptés aux contraintes du donneur d'ordres. Pilotage inapproprié du sous-traitant.	Revue de l'adéquation des contrats types vis-à-vis de la prise en compte de l'ensemble des exigences règlementaires et propres au donneur d'ordres (droit d'auditer, normes de développement...) et des processus et règles (procédures de sécurité...). Revue de la validation des trames de contrats par les parties concernées (opérationnelles, achats, juridiques, sécurité...). Revue de la connaissance des trames de contrats et des processus de pilotage du contrat sous ses différents aspects (création, maintenance, surveillance, renégociation) par les acteurs qui en ont la charge.	Adéquation du processus de pilotage pour maîtriser le sous-traitant et de la mise à jour sur la base de retours d'expérience consolidés. Existence de trames de contrats assurant une relation équilibrée entre le donneur d'ordre et le sous-traitant et enrichis sur la base de retours d'expérience consolidés. Appropriation des processus de pilotage par les acteurs concernés.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Stratégie et processus de sourcing	**Signature des contrats**		S'assurer que la politique de sourcing est correctement implémentée à l'occasion de chaque nouveau contrat passé et tient compte des engagements de service demandés par les métiers.	Implémentation inadéquate de la politique de sourcing. Non implémentation des niveaux de service demandés par le métier.	Rapprochement de toutes les facturations d'un contrat. Revue de la conformité des contrats passés à la stratégie et au processus de sourcing en place par les différents acteurs concernés : DSI/responsable achats/responsable RH. Revue de la prise en compte des besoins métiers pour définir le niveau de service attendu.	Pas d'engagement d'une prestation par un sous-traitant, sans la signature d'un contrat par les 2 parties. Conformité des contrats signés aux trames de contrats, sauf dérogation dûment justifiée. Utilisation autant que faire se peut des contrats cadres en vigueur pour optimiser les coûts. Correcte déclinaison des SLA métier en OLA à chaque niveau de la chaîne, de façon à garantir une correcte implémentation des besoins métiers.
Exécution des contrats tiers	**Convention de service, (SLA), plan d'assurance qualité, plan de réversibilité, plan de sécurité et accords de confidentialité**	DS2 : gérer les services tiers	S'assurer de l'existence : • d'une convention de service, d'un plan de réversibilité, d'un plan de sécurité et d'un plan d'assurance qualité validé par les deux parties ; • d'accords de confidentialité signés par le sous-traitant, répondant aux exigences du client.	Non clarification d'une convention de service, d'un plan de réversibilité, d'un plan de sécurité et d'un plan d'assurance qualité. Des garanties en termes de non-divulgation non définies.	Revue des éléments associés au contrat : existence d'une convention de service, d'un plan de réversibilité, d'un plan de sécurité, d'un plan d'assurance qualité et d'accords de confidentialité signés.	Existence d'une convention de service, d'un plan de réversibilité, d'un plan de sécurité et d'un plan d'assurance qualité établis avant signature du contrat et répondant à l'ensemble des exigences du client. Existence d'un contrat signé avant démarrage. Accords de confidentialité signés dès l'engagement du contrat.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Exécution des contrats tiers	Autorisation d'accès	DS2 : gérer les services tiers	S'assurer que les autorisations d'accès sont conformes au dispositif de gestion des habilitations en place.	Risque d'intrusion dans le SI du donneur d'ordre.	Revue des autorisations d'accès, qui doivent être formalisées et respecter le dispositif de gestion des habilitations en vigueur.	Autorisations d'accès restreintes au seul besoin de la prestation, nominatives et supprimées en fin de prestation.
	Qualité de service		S'assurer de la conformité du reporting par rapport aux engagements : suivi et respect des objectifs, solution de contournement si besoin...	Reporting manquant ou ne permettant pas d'anticiper les dérives à venir.	Revue de l'existence de reporting conforme aux engagements et permettant d'anticiper les dérives.	Existence et adéquation des reportings, pour anticiper toute dérive dans l'exécution du contrat. Existence dans le reporting d'un volet risques mis à jour en termes de maîtrise vis-à-vis des risques dont le sous-traitant est propriétaire.
	Conformité des livrables aux engagements Analyse de la facturation		S'assurer de la conformité des livrables aux engagements contractuels : documentations, programmes… et adéquation de la facturation par rapport aux contrats et aux livrables.	Manque de qualité des livrables, non respect des délais, non conformité aux spécifications, risque financier.	Revue de l'existence de contrôles intermédiaires conformément aux engagements dans la production des livrables. Revue de la validation des facturations en fonction du contrat et des livrables.	Existence d'un processus formalisé et mis en œuvre permettant, au cours de la réalisation du contrat, d'apprécier l'adéquation des livrables par rapport aux objectifs définis et de la facturation associée. Mise en place de retours d'expérience formalisés sur la qualité de la prestation et les litiges fournisseurs.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage des contrats tiers	Contrats	DS2 : gérer les services tiers	S'assurer de l'existence d'une liste de contrats à jour et d'un archivage adapté des engagements fournisseurs.	Mauvaise déclinaison des trames de contrats conclus. Mauvaise maîtrise des contrats.	Revue d'une mise à jour au fil de l'eau de la liste des contrats cadres conclus et d'une correcte diffusion. Identification des contrats n'utilisant pas de contrats cadres et contrôle d'une validation managériale adéquate associée. Revue de la connaissance des engagements fournisseurs par les acteurs assurant le pilotage du contrat.	Mise à jour au fil de l'eau de la liste des contrats cadres conclus et d'une correcte diffusion. Identification des contrats n'utilisant pas de contrats cadres et contrôle d'une validation managériale adéquate associée. Connaissance par l'ensemble des acteurs concernés de la liste des contrats cadres. Existence d'une présentation, dès engagement du contrat des engagements contractuels à l'ensemble des acteurs en charge du pilotage.
	Structure de pilotage par domaine		S'assurer que les acteurs en charge du pilotage du contrat sont correctement définis et acceptent leur mission.	Structure de pilotage insuffisamment clarifiée.	Revue de l'existence dans le contrat d'une disposition clarifiant les rôles et responsabilités des acteurs du pilotage et accepté par les acteurs concernés.	Existence d'un document formalisant la structure de pilotage de chaque contrat, dès le début de la mission, la gestion des interfaces et les modes d'arbitrage si besoin. Partage de ce document par les acteurs concernés.

Processus	Etapes-clés	N° de réf CobiT	Objectifs de contrôle	Risque	Activité de contrôle	Bonnes pratiques
Pilotage des contrats tiers	Pilotage des contrats tiers par domaine (opérationnel, financier, contractuel, juridique) incluant avenants	DS2 : gérer les services tiers	S'assurer d'un pilotage des contrats tiers sous les angles opérationnel, financier, contractuel, juridique et des avenants associés.	Non maîtrise du sous-traitant.	Revue d'un pilotage périodique du contrat et de ses avenants sous les différents angles lors des comités de pilotage du sous-traitant au travers des comptes-rendus établis. Réalisation d'audits de sécurité et de réversibilité. Revue du respect des clauses d'avenants passés.	Existence de comptes-rendus formalisés des réunions tenues entre les acteurs de pilotage et si besoin arbitrées, indiquant la position à tenir en préalable aux comités de pilotage du sous-traitant. Pilotage périodique du contrat et de ses avenants sous les différents angles lors des comités de pilotage du sous-traitant, avec décisions tracées dans les comptes-rendus établis. Réalisation d'audits de sécurité, de réversibilité. Avenants passés avant engagement de toute prestation complémentaire et clarification des préséances vis-à-vis des clauses juridiques entre contrat de base et les différents avenants. Pour les contrats d'infogérance, mise en œuvre des clauses de benchmarking.
	Réversibilité du contrat		S'assurer de la définition d'un processus de réversibilité, de l'estimation de son coût, de la capacité de l'organisation à réaliser cette réversibilité, des conditions de reprise des outils, de documentations…	Mauvaise gestion de la réversibilité.	Revue de l'existence d'un plan de réversibilité associé à chaque contrat clé. Revue d'une appréhension de sa faisabilité dès que des signaux faibles persistants apparaissent. Revue des conditions de déclenchement, lesquelles font l'objet d'une validation formelle par le niveau hiérarchique dûment approprié.	Existence d'un plan de réversibilité associé à chaque contrat clé... Existence d'un suivi périodique de son applicabilité. Existence d'un suivi continu d'une anticipation des dérives pour prévoir des périodes où pourraient survenir des conditions nécessitant une réversibilité. Existence d'une étude d'impact dûment approuvée avant déclenchement de la réversibilité. Prise en compte de l'étude d'impact dans la définition de la solution de réversibilité.

6. Annexes

6.1. Annexe 1 – Charte CIGREF – IFACI

CIGREF — Institut de l'Audit Interne

Charte CIGREF - IFACI

- Crée en 1970, **le CIGREF** - association de Grandes Entreprises Françaises - a pour mission de « *promouvoir l'usage des Systèmes d'Information comme facteur de création de valeur et source d'innovation pour l'Entreprise…* ».

- Fondé en 1965, **l'IFACI** (Institut Français de l'Audit et du Contrôle Internes) est, en France, l'organisme chargé de représenter la profession d'audit interne, de promouvoir son développement et de servir les auditeurs internes.

◆ Préambule

CIGREF & IFACI - associations de référence dans les domaines respectifs des technologies de l'information et de l'audit interne - décident d'unir leurs compétences et leurs efforts pour apporter, ensemble, plus de valeur ajoutée à l'entreprise et à toute organisation des secteurs public et privé.

◆ Contexte

Conscients de l'impact des systèmes d'information (SI) sur le fonctionnement et la performance des organisations ;
Conscients de la nécessité de doter les entreprises et les organisations d'un dispositif de contrôle interne performant :

◆ Finalité

CIGREF et IFACI souhaitent éclairer les organes dirigeants sur le degré de maîtrise des opérations SI. Il s'agit ainsi d'aider l'organisation à atteindre ses objectifs :
- en optimisant - au sein des entreprises - la coopération entre les deux fonctions Audit Interne & Système d'information.
- en évaluant - par une approche systématique et méthodique - les processus de management des risques,
- en formulant des recommandations quant aux comportements à adopter, et aux moyens, procédures et actions à mettre en œuvre pour renforcer leur efficacité.

◆ Cadre de référence

Début 2007, l'AMF a préconisé - pour les sociétés françaises cotées - un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques propres à chaque organisation afin
- d'une part, de contribuer à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources
- et, d'autre part, de lui permettre de prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité.

◆ Moyens d'action

Dans le prolongement des travaux de l'AMF, CIGREF & IFACI décident de créer un groupe de travail mixte, chargé d'élaborer, courant 2008, un guide spécifique d'application relatif au contrôle interne des systèmes d'information.

Fait à Paris, le 9 octobre 2007

Didier LAMBERT
Président CIGREF

Claude CARGOU
Président IFACI

6.2. Annexe 2 - Organismes et référentiels liés au contrôle interne

		Comptabilité	Audit externe / CAC	Contrôle interne	Audit interne	Audit informatique	Informatique	Régulation
International	Organismes	IASB	IFAC	COSO	IIA	ISACA		
	Référentiels	IFRS	Financial Raporting Auditing & Assurance	Internal Control Framework (COSO 1) ERM Framework (COSO 2)	IPPF (GTAG, GAIT)	ITAF (IT assurance framework) COBIT VAL IT		Bâle 2 Solvency
France	Organismes	Autorité de Normes Comptables CSOEC	HCCC CNCC		IFACI	AFAI	CIGREF	AMF Autorité de Contrôle Prudentiel (banque, assurance)
	Référentiels	Plan comptable général	Normes d'exercice professionnel		« Le contrôle interne du SI des organisations »	Le contrôle interne du SI		Cadre de référence de contrôle interne CRBF 97-02

Source : CIGREF - IFACI

6.3. Annexe 3 - Tableau de concordance entre les processus et les objectifs de contrôle du cadre de référence de contrôle interne de l'AMF

Objectifs du dispositif		Compétences	Projet et développement	Maintenance	Incidents	Sécurité	Sous-traitance
Conformité aux lois et règlements	*« Les lois et les règlements en vigueur fixent des normes de comportement. »* *« être informée en temps utile des modifications »* *« connaître les diverses règles … applicables. »*	■				■	■
	« transcrire ces règles dans les procédures internes.» *« informer et former les collaborateurs sur celles des règles qui les concernent. »*	■	■	■	■	■	■
Application des instructions et des orientations fixées par la Direction Générale ou le Directoire	*« permettent aux collaborateurs de comprendre ce qui est attendu d'eux et de connaître l'étendue de leur liberté d'action. »*	■	■	■	■	■	■
	« communiquées aux collaborateurs concernés, en fonction des objectifs assignés.»						
	« établies en fonction des objectifs poursuivis par la société et des risques encourus. »						
Bon fonctionnement des processus internes de la société notamment ceux concourant à la sauvegarde des actifs	*« exige que des normes ou principes de fonctionnement aient été établis. »*	■	■	■	■	■	■
	« des indicateurs de performance et de rentabilité aient été mis en place. »		■	■	■		■
	Concerne aussi les *« actifs incorporels »* tels que le savoir-faire.	■					■
	« ces actifs peuvent disparaître à la suite d'erreurs ou résulter d'une mauvaise décision de gestion. »	■	■	■	■	■	■
Fiabilité des informations financières	*« procédures de contrôle interne susceptibles de saisir fidèlement toutes les opérations. »*		■	■	■	■	
	« séparation des tâches qui permet de bien distinguer les tâches d'enregistrement, les tâches opérationnelles et les tâches de conservation. »		■	■	■	■	
	« identifier les origines des informations produites, et leurs destinataires. »		■	■	■	■	
	« les opérations sont effectuées conformément aux instructions générales et spécifiques. »		■	■	■	■	■

Composante du cadre de référence		Compétences	Projet et développement	Maintenance	Incidents	Sécurité	Sous-traitance
Préalables	*« Les grandes orientations en matière de contrôle interne sont déterminées. »*						
	« fondé sur des règles de conduite et d'intégrité portées par les organes de gouvernance et communiquées à tous les collaborateurs. »						
Organisation appropriée	*« une organisation appropriée qui fournit le cadre dans lequel les activités nécessaires à la réalisation des objectifs sont planifiées, exécutées, suivies et contrôlées. »*						
	« Des responsabilités et pouvoirs clairement définis »						
	« respecter le principe de séparation des tâches ».						
	« une politique de gestion des ressources humaines qui devrait permettre de recruter des personnes possédant les connaissances et compétences nécessaires à l'exercice de leur responsabilité et à l'atteinte des objectifs actuels et futurs de la société. »						
	« des systèmes d'information adaptés aux objectifs actuels de l'organisation et conçus de façon à pouvoir supporter ses objectifs futurs »	Gouvernance des SI non approfondie dans les travaux					
	Des systèmes d'information *« protégés efficacement tant au niveau de leur sécurité physique que logique. »*						
	« la conservation des informations stockées. »						
	La *« Continuité d'exploitation doit être assurée au moyen de procédures de secours ».*						
	« les informations relatives aux analyses, à la programmation et à l'exécution des traitements doivent faire l'objet d'une documentation. »						
	« des procédures ou modes opératoires qui précisent la manière dont devrait s'accomplir une action ou un processus. »						
	« des outils ou instruments de travail qui doivent être adaptés aux besoins de chacun et auxquels chaque utilisateur devrait être dûment formé »						

Composante du cadre de référence		Compétences	Projet et développement	Maintenance	Incidents	Sécurité	Sous-traitance
Diffusion d'informations pertinentes	« assurent la communication d'informations pertinentes, fiables, et diffusées en temps opportun. »						
	« permettre d'exercer leurs responsabilités »						
Système de recensement et d'analyse des risques	« un système visant à recenser, analyser les principaux risques identifiables au regard des objectifs de la société et à s'assurer de l'existence de procédures de gestion de ces risques. »						
Activités de contrôle proportionnées	« des activités de contrôle proportionnées aux enjeux propres à chaque processus, et conçues pour s'assurer que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs. »						
	« les activités de contrôle doivent être déterminées en fonction de la nature des objectifs auxquels elles se rapportent et être proportionnées aux enjeux de chaque processus. »						
	« une attention particulière devrait être portée aux contrôles des processus de construction et de fonctionnement des systèmes d'information. »						
Surveillance Permanente	« une surveillance permanente portant sur le dispositif de contrôle interne ainsi qu'un examen régulier de son fonctionnement. »	Gouvernance des SI non approfondie dans les travaux. Responsabilités des principaux acteurs (DG, CA, AI, DSI, Direction métiers) à définir.					
	« Cette surveillance prend notamment en compte l'analyse des principaux incidents constatés. »						
	« Surveillance et veille conduise, si nécessaire, à la mise en œuvre d'actions correctives et à l'adaptation du dispositif de contrôle interne »						

6.4. Annexe 4 – Exemples de typologies de risques

Figure 31 : Modèle de risques économiques

Source : World Economic Forum - 2006

Economic	Societal	Environmental	Technological	Geopolitical
• Oil prices/Energy • Asset prices / indebtedness • Coming fiscal crisis • China • Critical infrastructures	• Regulation • Corporate Governance • Intellectual Property Rights • Organized Crime • Global pandemics • Slow and chronic diseases (industrialized world) • Epidemic disease (developing world) • Liability regimes	• Tropical cyclones • Earthquakes • Climate change • Loss of ecosystem service	• Convergence of technologies • Nanotechnology • Electromagnetic fields • Pervasive computing	• Terrorism • European dislocation • Current and future hotspots

Figure 32 : Nouvelle taxonomie des risques

Source : Marsh Insurance – Repenser le risque - 2004

Hazard	Financial	Operational	Organizational	Strategic
• Property/ Casualty • Political • Environmental • Regulatory	• Currency • Interest rate • Commodity prices • Credit	• Inventory • Supply chain • Capacity • Information systems	• Governance gaps • Wrong organizational structure • Talent/Morale • M&A integration	• Technology • Brand collapse • One-of-a-kind competition • Industryeconomics collapse • Customer shift • New project / investment • Stagnation • Obsolete business design

Article 4 du Règlement n° 97-02 du 21 février 1997

Typologie des risques relatifs au contrôle interne des établissements de crédit et des entreprises d'investissement.

Risque	Descriptif
Risque de crédit	Le risque encouru en cas de défaillance d'une contrepartie.
Risques de marché	Comprend le risque de change
Risque de taux d'intérêt global	Le risque encouru en cas de variation des taux d'intérêt du fait de l'ensemble des opérations de bilan et de hors-bilan, à l'exception, le cas échéant, des opérations soumises aux risques de marché mentionnés ci-dessus.
Risque de liquidité	Le risque pour l'entreprise assujettie de ne pas pouvoir faire face à ses engagements ou de ne pas pouvoir dénouer ou compenser une position en raison de la situation du marché.
Risque de règlement	Le risque encouru au cours de la période qui sépare le moment où l'instruction de paiement ou de livraison d'un instrument financier vendu ne peut plus être annulée unilatéralement et la réception définitive de l'instrument financier acheté ou des espèces correspondantes.
Risque opérationnel	Le risque résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes ou à des événements extérieurs y compris d'événements de faible probabilité d'occurrence mais à fort risque de perte.
Risque juridique	Le risque de tout litige avec une contrepartie, résultant de toute imprécision, lacune ou insuffisance susceptible d'être imputable à l'entreprise au titre de ses opérations.
Perte potentielle maximale	La mesure de l'impact le plus défavorable sur les résultats de variations des conditions de marché intervenant sur une période donnée et avec un niveau de probabilité déterminé.
Risque d'intermédiation	Le risque de défaillance d'un donneur d'ordres ou d'une contrepartie à l'occasion d'une transaction sur instruments financiers dans laquelle l'entreprise assujettie apporte sa garantie de bonne fin.
Risque de non-conformité	Le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative ou d'atteinte à la réputation, qui naît du non-respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législatives ou réglementaires, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions de l'organe exécutif prises notamment en application des orientations de l'organe délibérant.

6.5. Glossaire

Certaines définitions sont inspirées de Wikipedia

Activité de contrôle : « proportionnées aux enjeux propres à chaque processus, et conçues pour s'assurer que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs » (cf. Cadre de Référence AMF).

AMF (Autorité des Marchés Financiers) : Instaurée par la loi du 1er août 2003, l'AMF est le résultat de la fusion de trois anciennes autorités des marchés financiers : le CMF (Conseil des Marchés Financiers), la COB (Commission des Opérations de Bourse) et le CDGP (Conseil de Discipline de la Gestion des Portefeuilles). L'AMF est aujourd'hui l'autorité chargée de la régulation des marchés financiers.

CMMI (Capability Maturity Model Integration) : Référentiel de bonnes pratiques, développé par l'université Carnegie Mellon, destiné à appréhender, évaluer et améliorer la qualité des développements logiciels. Le modèle CMMI définit une échelle de mesure de la maturité à 5 niveaux.

CobiT (Control Objectives for Business and Related Techonology) : Référentiel de gouvernance et d'audit des SI développé par l'ISACA (Information Systems Audit and Control Association) et promu en France par l'AFAI (Association Française de l'Audit et du conseil Informatique) et le CIGREF. CobiT est une approche orientée processus. CobiT décompose tout système informatique en 34 processus regroupés en 4 domaines.

COSO : Référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission. Il est utilisé notamment dans le cadre de la mise en place des dispositions relevant des lois Sarbanes-Oxley ou LSF pour les entreprises assujetties respectivement aux lois américaines ou françaises.

eSCM (e-Sourcing Capability Model) : Référentiel développé par l'université de Carnegie Mellon et promu en France par l'association a-eSCM . Ce référentiel qui comprend deux volets (un volet interne – client et un volet externe – fournisseurs) permet d'industrialiser et standardiser la relation clients / fournisseurs.

Hot-Line : Premier niveau d'appel au soutien (centre d'appels).

Help-Desk : Chaîne de soutien (deuxième niveau du soutien après la Hot-Line).

ISO 27000 : Ensemble de normes liées à la sécurité des SI. La suite contient des recommandations des meilleures pratiques en management de la sécurité de l'information, pour l'initialisation, l'implémentation ou le maintien de systèmes de management de la sécurité de l'information (SMSI, ou ISMS en anglais).

Incident : Tout événement qui ne fait pas partie des opérations standard et pouvant provoquer une interruption de service ou altérer sa qualité.

ITIL (Information Technology Infrastructure Library) : Ensemble de bonnes pratiques pour la gestion de la production informatique. ITIL est une approche par processus, qui vise à améliorer la qualité des services des SI.

LSF : Loi sur la Sécurité Financière. Loi française adopté le 17 juillet 2003 visant à assurer un meilleur contrôle des entreprises et à renforcer les dispositions légales en matière de gouvernement d'entreprise. Cette nouvelle loi s'applique à toutes les sociétés anonymes ainsi qu'aux sociétés faisant appel à l'épargne publique. La loi de sécurité financière repose principalement sur :

- une responsabilité accrue des dirigeants ;
- un renforcement du contrôle interne ;
- une réduction des sources de conflits d'intérêt.

Objectifs de contrôle : Résultat désiré ou but à atteindre par la mise en œuvre d'une activité de contrôle.

OLA : Operational Service Agreement (contrat de service interne à l'informatique entre un service informatique et un autre service informatique).

OS : Système d'exploitation.

PV (procès verbal) de recette : Document qui valide la conformité du logiciel par rapport aux spécifications avant la mise en production. Il est signé par la Maîtrise d'Ouvrage (MOA).

Bon de livraison : Document fournit par la MOE « développement » à la MOE « exploitation ». Il liste les éléments techniques à installer sur les serveurs de production.

Qualification de l'information : Classification adaptée à la taille de l'entité, en matière de confidentialité, de valeur ou d'amplitude critique et qui permet de s'assurer que l'information bénéficiera du niveau approprié de protection.

Risque : Possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité (Glossaire des normes de l'IIA/IFACI).

RACI : Responsable, Approuve, Consulté, Informé – Méthode permettant d'attribuer des rôles à des acteurs au sein d'une organisation.

RSSI : Responsable Sécurité des systèmes d'information.

Rôles critiques : Rôles essentiels pour le bon fonctionnement de la DSI, et a priori non externalisables.

Rôles clés : Rôles critiques particulièrement rares sur le marché.

SLA : Service Level Agreement (contrat de service entre un service utilisateur et un service informatique).

SOX (Sarbanes Oxley) : Loi fédérale américaine de 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs imposant de nouvelles règles sur la comptabilité et la transparence financière. Elle fait suite aux différents scandales financiers révélés dans le pays aux débuts des années 2000, tels ceux d'Enron et de Worldcom. La loi du 31 juillet 2002 a introduit notamment :

- l'obligation pour les présidents et les directeurs financiers de certifier personnellement les comptes ;
- l'obligation de nommer des administrateurs indépendants au comité d'audit du conseil d'administration ;
- l'encadrement des avantages particuliers des dirigeants.

Cette loi oblige aussi à mettre en œuvre un contrôle interne s'appuyant sur un cadre conceptuel. En pratique le COSO est le référentiel le plus utilisé.

7. Sources

Sites institutionnels :

- www.afai.fr
- www.cigref.fr
- www.ifaci.com
- www.isaca.org

Rapports :

- Rapport de l'AFAI – Contrôle interne et système d'information – Juillet 2008 – www.afai.fr

ISBN : 978-2-915042-02-3

Réalisation : ebzone communication (www.ebzone.fr) - Impression : Imprimerie Compédit Beauregard

CIGREF

21, avenue de Messine - 75008 Paris
Tél. : 01 56 59 70 00 - Fax : 01 56 59 70 01
Mel : cigref@cigref.fr - Internet : www.cigref.fr

IFACI Institut de l'Audit Interne

12 bis, place Henri Bergson - 75008 Paris
Tél. : 01 40 08 48 00 - Fax : 01 40 08 48 20
Mel : institut@ifaci.com - Internet : www.ifaci.com