GTAG®

GUIDE PRATIQUE D'AUDIT DES TECHNOLOGIES DE L'INFORMATION

Audit des projets SI

The Institute of Internal Auditors

Cette série de guides, rédigés dans des termes simples et traitant chacun d'un thème d'actualité concernant la gestion, le contrôle et la sécurité des SI, constitue un précieux outil pour les responsables de l'audit interne, qui peuvent ainsi s'informer sur les différents risques associés aux technologies de l'information et sur les pratiques recommandées.

Les contrôles des systèmes de l'information
Les sujets abordés passent en revue les concepts du contrôle des SI, l'importance de ces contrôles, les rôles et responsabilités dans l'organisation susceptibles d'assurer l'efficacité du contrôle des SI et des techniques de supervision.

Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation
Décrit les sources de changements et leurs impacts probables sur les objectifs de l'entreprise, explique en quoi le contrôle du processus de gestion des changements participe à la réduction des risques et des coûts des SI, et indique ce qui, dans la pratique, fonctionne ou pas.

Audit continu : Répercussions sur l'assurance, le pilotage et l'évaluation des risques
Traite du rôle de l'audit continu dans l'environnement actuel d'audit interne, de la relation entre audit continu, surveillance continue et assurance continue, précise où s'applique l'audit continu et examine la mise en place de l'audit continu.

Management de l'audit des systèmes d'information
Définit les risques liés aux SI et l'univers d'audit, explique comment conduire un audit des SI et gérer les ressources d'audit.

Le management et l'audit des risques d'atteinte à la vie privée
Présente les principes et le cadre de protection de la vie privée, un modèle de risques d'atteinte à la vie privée et le contrôle du respect de la vie privée, le rôle de l'audit interne, les dix questions à se poser concernant la protection de la vie privée lors de la mission d'audit, et bien plus encore.

Gérer et auditer les vulnérabilités des technologies de l'information
Analyse, entre autres, le cycle de gestion des vulnérabilités, la délimitation de l'audit des vulnérabilités et des indicateurs qui permettent d'évaluer les pratiques de gestion des vulnérabilités.

L'infogérance
Examine comment choisir le bon prestataire de services d'infogérance et présente les principaux éléments à prendre en compte pour la maîtrise de l'infogérance, du point de vue des activités du client et de celles du prestataire de services.

Audit des contrôles applicatifs
Définit la notion de contrôles applicatifs et les compare aux contrôles généraux informatiques, et indique comment déterminer l'étendue des revues de contrôles applicatifs.

Gestion des identités et des accès
Couvre les principaux concepts relatifs à la gestion des identités et des accès, les risques y afférents, détaille l'audit du programme de gestion des identités et des accès et présente un exemple de liste de contrôles à l'intention des auditeurs.

Gestion de la continuité d'activité
Définit la continuité d'activité, examine les risques pour l'entreprise et propose une analyse détaillée des impératifs associés au programme de continuité d'activité

Élaboration d'un plan d'audit des SI
Explique pas à pas la manière d'élaborer un plan d'audit des SI : de la compréhension de l'activité, la définition de l'univers d'audit des SI et l'évaluation des risques jusqu'à la formalisation du plan d'audit des SI.

Si vous souhaitez de plus amples informations et ressources sur l'audit des technologies de l'information, veuillez vous rendre sur le site Web de l'IIA : www.theiia.org/technology.

Audit des projets SI

Auteurs

Karine Wegrzynowicz, Lafarge SA

Steven Stein, Hewlett-Packard

Mars 2009

Copyright © 2009 par l'Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201, États-Unis. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de consultation ou transmise sous quelque forme que ce soit, ni par aucun moyen (électronique, mécanique, reprographie, enregistrement ou autre), sans l'autorisation préalablede l'éditeur.

L'IIA publie ce document à titre informatif et pédagogique. Cette publication entend donner des informations, mais ne se substitue en aucun cas à un conseil juridique ou comptable. L'IIA ne fournit pas ce type de service et ne garantit, par la publication de ce document, aucun résultat juridique ou comptable. En cas de problèmes juridiques ou comptables, il convient de recourir à l'assistance de professionnels.

Sommaire

1. RÉSUMÉ 2

2. INTRODUCTION 4

2.1 Qu'appelle-t-on exactement « projet SI » ? 4

2.2 Comprendre les répercussions 4

2.3 Quelques exemples de projets SI non aboutis 4

2.4 Statistiques historiques sur la réussite et l'échec des projets SI 5

2.5 Dix facteurs clés de réussite d'un projet 6

2.6 Objectifs et avantages de l'implication des auditeurs internes 6

3. CINQ THÈMES CENTRAUX DANS L'AUDIT DES PROJETS 7

3.1 Alignement des objectifs et des SI 7

3.2 Gestion de projet 8

3.3 Opérationnalité des solutions SI 12

3.4 Gestion des changements au niveau de l'organisation et des processus 13

3.5 L'après projet (Post-implémentation) 14

4. PLANIFICATION DE L'AUDIT DE PROJET 15

4.1 Projets SI et plan annuel d'audit interne 15

4.2 Rôle de l'audit interne 16

4.3 Types d'audits de projet 17

4.4 Remarques des auditeurs externes 18

5. CONCLUSION 20

ANNEXE A : GESTION DE PROJET 21

A.1 Méthodologies de gestion de projet 21

A.2 Cycle de vie de gestion du projet 21

ANNEXE B : PARTICIPANTS AUX PROJETS SI 22

ANNEXE C : STRUCTURE, RÔLES ET RESPONSABILITÉS DES INSTANCES DE PILOTAGE DE PROJET 23

Sommaire *(suite)*

ANNEXE D : MODÈLES DE MATURITÉ 24

D.1 Modèle de maturité des capacités 24

D.2 Modèles de maturité de la gestion de projet 24

D.3 Modèles de maturité du développement de systèmes 24

ANNEXE E – BONNES PRATIQUES GÉNÉRALES DE GESTION DE PROJET 25

E.1 PMBOK et PRINCE2 25

E.2 Normes de l'ISO 25

E.3 Sections du référentiel CobiT applicables à la gestion de projet 26

E.4 VAL IT 26

ANNEXE F – POINTS À VÉRIFIER LORS DE LA REVUE DES PROJETS SI PAR LES AUDITEURS INTERNES 27

À PROPOS DES AUTEURS 41

Lettre du Président de l'IIA

Comme la plupart des auditeurs internes de ma génération, j'ai été le témoin privilégié de l'évolution remarquable des technologies. Dans les années 1970, frais émoulu de l'université, l'outil technologique le plus complexe auquel j'avais régulièrement affaire était une calculatrice à dix touches. Aujourd'hui, nous vivons et travaillons dans un monde bien différent.

Grâce aux progrès incessants des systèmes d'information depuis que j'ai intégré le monde du travail, les technologies sont désormais omniprésentes dans tout ce qui nous entoure. Quel que soit le secteur ou l'entreprise considéré, elles jouent un rôle majeur dans la compétitivité, la gestion des risques et la réalisation des objectifs de l'entreprise ; et les organisations du monde entier allouent des ressources considérables à des projets SI vitaux.

Qu'ils soient développés en interne ou en collaboration avec des prestataires externes, les projets SI comportent des difficultés dont il faut tenir compte pour garantir leur succès. Un contenu et des objectifs mal définis, l'absence de soutien de la direction, une implication insuffisante des utilisateurs, des choix technologiques erronés ou inadaptés, une mauvaise connaissance de l'évolution des technologies peuvent avoir des conséquences fâcheuses. Si l'on accorde trop peu d'attention à ces problèmes ou aux difficultés techniques, on aboutira à un gaspillage d'argent et de ressources, à une perte de confiance et à entacher la réputation ; autant de risques énormes et inacceptables.

L'une des caractéristiques inhérentes aux systèmes d'information est leur transversalité. Ils doivent impliquer des personnes et des processus à tous les niveaux de l'organisation. Et parce que les auditeurs internes ont une perspective et un positionnement unique au sein de l'organisation, leur participation en amont peut aider à atteindre les résultats fixés, avec tous les avantages que cela entraîne. Ils peuvent servir de relais entre les différentes directions métiers et la DSI, remonter des risques qui n'avaient pas encore été identifiés et recommander des contrôles pour améliorer les résultats.

Pour toutes ces raisons, j'accueille avec un grand plaisir la publication du nouveau GTAG de l'IIA, Audit des projets SI. Ce guide bien actuel présente un aperçu des techniques qui permettent de collaborer efficacement avec les équipes projet et la direction sur l'évaluation des risques liés aux projets SI. Ce guide pratique aborde les points suivants :

- Comment définir un cadre d'évaluation des risques liés au projet ?
- Les principaux risques de gestion de projet.
- Comment l'audit interne peut participer activement à l'examen des projets tout en conservant son indépendance ?
- Cinq éléments clés des projets SI que les auditeurs internes doivent prendre en compte dans l'élaboration d'une méthodologie d'audit.
- Dix principaux facteurs de réussite du projet.
- Les types d'audits de projet.
- Un exemple de programme d'audit comprenant une liste de questions utiles lors de l'évaluation d'un projet SI.

L'élaboration de ce Guide pratique a été un véritable travail d'équipe. Nous remercions l'*Advanced Technology Committee* de l'IIA d'avoir choisi ce sujet et mis au point ces recommandations. Nous exprimons notre profonde gratitude aux deux principaux auteurs, Karine Wegrzynowicz, CIA, responsable de l'audit interne chez Lafarge SA, et Steve Stein, CIA, responsable mondial de l'audit des SI chez Hewlett-Packard, d'avoir consacré autant de temps et d'énergie à ce projet.

Je vous encourage vivement à utiliser ce guide de référence pour développer vos connaissances pratiques sur la gestion de projets SI, car il contribuera très certainement au succès des futures initiatives de votre organisation dans le domaine des SI.

Bien sincèrement,

Richard F. Chambers, CIA
Président de l'IIA
Siège mondial

1. Résumé

Les organisations investissent des budgets considérables pour financer la mise en œuvre de nouveaux systèmes d'information, pénétrer de nouveaux marchés, développer de nouveaux produits et gérer des alliances et des acquisitions. Pour piloter ces initiatives, on crée souvent des équipes projet. Ces investissements, s'ils ont des effets positifs pour l'organisation, comportent aussi des risques élevés. Ainsi, leur réussite ou leur échec peut être critique pour la stratégie de l'organisation et se répercuter sur ses performances et sur sa réputation.

Un grand nombre de projets et d'investissements concernent les systèmes d'information (SI). Dans le passé, des études, comme *The CHAOS Report* réalisé par *The Standish Group*, ont montré que, pour les projets SI en particulier, le taux d'échec pouvait atteindre 50 %[1]. L'échec des projets se résume souvent à deux causes : excès d'optimisme pour l'aspect humain ou pannes technologiques au niveau des systèmes. Étant donné leur degré de risque, l'audit interne doit absolument être informé des projets en cours de réalisation dans l'organisation et déterminer à quel stade il doit intervenir pour recommander des contrôles ou pour évaluer, en toute indépendance, si les résultats attendus ont été obtenus.

Parce qu'il en évalue les risques, l'audit interne peut contribuer à la réussite des projets SI. Les auditeurs peuvent se concentrer sur des domaines tels que la sécurité et le dispositif de contrôle interne, et participer à l'évaluation de la gestion globale du projet. En aidant les équipes projet à tenir compte des risques, l'audit interne peut augmenter les chances de réussite du projet. Comme l'indiquait le *GTAG 8 : Audit des contrôles applicatifs*, l'audit interne peut apporter de la valeur, par ses missions classiques d'assurance et de conseil[2].

Dans un article du magazine *Internal Auditor* paru en 2002, Richard B. Lanza écrivait : « Pour réussir, les auditeurs doivent faire la preuve, aussi bien auprès de la direction générale que des chefs de projet, de la valeur que peut apporter un consultant indépendant. Même si la direction générale leur permet d'accéder aux projets, ils seront plus efficaces si les chefs de projet croient en leur contribution et leur accordent un accès plus large.[3]»

Ce GTAG a pour objectif d'offrir aux auditeurs internes et à leur responsable une vue d'ensemble des techniques permettant de collaborer efficacement avec les équipes projet et les instances de pilotage de projet sur l'évaluation des risques liés aux projets SI. Le champ de la gestion de projet étant extrêmement vaste, l'objet de ce guide est de définir un cadre d'évaluation des risques liés aux projets, de donner des exemples de risques courants liés à la gestion de projet et d'étudier comment l'audit interne peut participer activement à l'examen des projets sans perdre son indépendance. Le document de l'IIA intitulé *Normes internationales pour la pratique professionnelle de l'audit interne* donne des recommandations basées sur des principes pour mener à bien ces missions.

Nous avons choisi, dans le cadre de ce GTAG, de nous concentrer sur cinq éléments clés des projets SI pour lesquels nous recommandons de construire une approche d'audit (voir la figure 1) :

1. Alignement des objectifs de l'entreprise et des SI
2. Gestion de projet
3. Opérationnalité de la solution SI
4. Gestion des changements au niveau de l'organisation et des processus
5. L'après-projet (Post-implémentation)

La figure 1 montre que la gestion de projet est la notion centrale qui fait le lien entre ces différents éléments. Lors de la préparation de l'approche d'audit du projet, l'auditeur doit tenir compte de ces cinq éléments pour être certain que tous les risques majeurs sont pris en compte.

Ce guide ne prétend pas être un guide complet d'audit ou d'évaluation des risques, mais il présente les grandes lignes des principaux points à prendre en compte lors de l'audit de projets SI. L'audit des projets constitue une excellente occasion, pour les auditeurs internes, de donner une assurance sur les risques stratégiques. Un certain nombre d'études montrent que les auditeurs internes consacrent

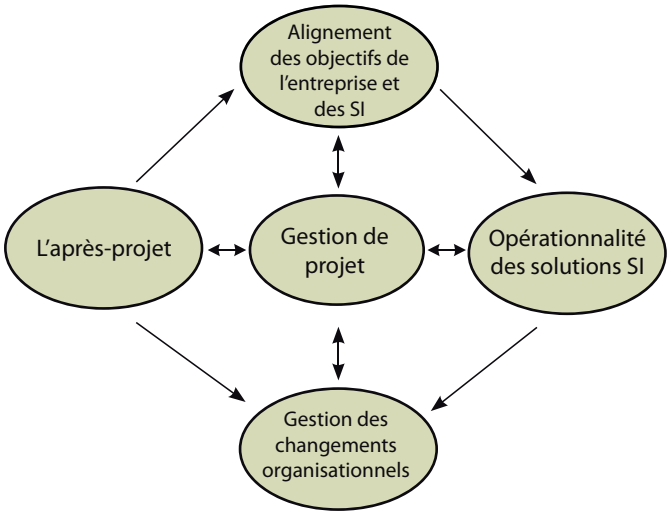


Figure 1. Cinq thèmes centraux de l'audit.

[1] *CHAOS Report 2007, The 10 Laws of CHAOS, The Standish Group, 2007.*
[2] *GTAG 8 : Audit des contrôles applicatifs*, p. 5.
[3] « *Technology Projects: The Riskiest Parts of the Business.*» *Internal Auditor*, 15 mai 2002, Richard B. Lanza, CPA, PMP.

beaucoup de temps à l'audit des risques opérationnels, et pas assez à l'audit des risques stratégiques. Les audits de projet donnent la possibilité d'élargir le champ d'études des risques.

2. Introduction

2.1 Qu'appelle-t-on exactement « projet SI » ?

Le terme *Projet SI* n'est pas vraiment adapté. En réalité, la plupart des projets de mise en œuvre ou de maintenance de systèmes sont des initiatives de plus en plus complexes qui font participer ou touchent bien d'autres domaines que la DSI. Pour cette raison, ils devraient être considérés comme des projets d'entreprise et pas seulement comme des projets SI. Au sens courant, un projet est un ensemble d'activités, avec un début et une fin définis, qui est entrepris pour atteindre un objectif donné dans des contraintes précises de calendrier, de contenu et de ressources. Si ce GTAG est consacré aux projets qui incluent une solution technologique, les principes sont très semblables à ceux d'autres types de projets.

Les investissements dans les SI représentent depuis de nombreuses années un poste de dépenses important. Ces investissements interviennent généralement par vagues qui touchent les organisations du monde entier. Les grands projets SI peuvent facilement coûter des dizaines de millions de dollars. Les principales vagues de projets SI de ces quinze dernières années portaient sur les systèmes PGI (progiciels de gestion intégrés ou ERP), la résolution du bug de l'an 2000, les solutions de commerce électronique/sociétés par Internet et les systèmes de gestion de la relation client. Ces projets peuvent inclure la création de nouvelles infrastructures, le développement de nouveaux produits (on parle généralement de recherche et développement ou R&D) et la mise en œuvre de nouveaux processus ou de transformations de l'activité. Lors de l'évaluation de ces projets, il faut bien comprendre les principaux risques et définir un ensemble de critères d'évaluation du projet à différents stades.

2.2 Comprendre les répercussions

Aujourd'hui, pour déterminer si un projet est un succès, il ne suffit plus de mesurer si les délais et le budget ont été respectés. Les projets qui échouent ou qui sont menacés peuvent avoir un impact considérable sur l'organisation, selon les besoins métiers qui les sous-tendent. Voici quelques exemples des risques potentiels :

- perturbation des services fournis aux clients ;
- perte d'avantage concurrentiel ;
- amendes pour non-respect de la réglementation ;
- baisse du chiffre d'affaires ;
- impacts négatifs sur la réputation ;
- retard dans la mise en œuvre de produits ou de processus critiques et stratégiques ;
- baisse du retour sur investissement prévu ;
- départ du personnel stratégique dans les directions métiers et la DSI ;
- altération ou suppression de services ;
- retrait d'actionnaires/investisseurs.

De nombreux chercheurs et cabinets de conseil ont réalisé des études dont les conclusions montrent que les projets SI sont régulièrement menacés ou se soldent par un échec : budget dépassé, délais non tenus, objectifs non atteints, annulation. Ce qui explique le nombre d'idées, d'articles et de livres blancs sur le sujet. Quelle que soit la façon d'interpréter les données, une multitude d'éléments montrent que les projets présentent des difficultés considérables. En fin de compte, c'est à la direction générale qu'il incombe de veiller à ce que le projet aboutisse et que les résultats attendus soient atteints.

2.3 Quelques exemples de projets SI non aboutis

La plupart des grands *projets SI* qui se soldent par un échec sont passés sous silence, en raison de l'impact négatif que pourrait avoir l'information sur la réputation de l'organisation concernée et sur ses actionnaires. Voici toutefois quelques exemples d'échecs retentissants connus.

- En août 2005, la revue *CIO Magazine* signalait qu'une grande agence gouvernementale américaine avait dû abandonner son projet de développement d'un système de gestion de dossiers virtuels d'un montant de 170 millions de dollars pour cause de retards sur le calendrier, de dépassement des coûts et de difficultés techniques[4].
- En 2004, l'une des plus grosses entreprises de télécommunications au monde assistait à l'échec de son projet de mise à niveau du système de gestion de la relation client. Les problèmes provoqués se sont propagés à l'ensemble de l'environnement SI, entraînant des perturbations dans les services sans fil aux clients. À cause de cet incident, l'entreprise a perdu de nombreux clients, avec un manque à gagner estimé à 100 millions de dollars. Le cours de l'action a chuté et, avant de pouvoir rebondir, l'entreprise a été vendue à la concurrence pour un montant inférieur à la moitié de la valeur initiale de l'action[5].
- En 1999, l'une des plus grosses entreprises agroalimentaires au monde a subi un grave problème de mise en œuvre de son système PGI, donnant lieu à

[4] *« Why the G Men Aren't IT Men », Allan Holmes, CIO Magazine Online, 15 août 2005.*

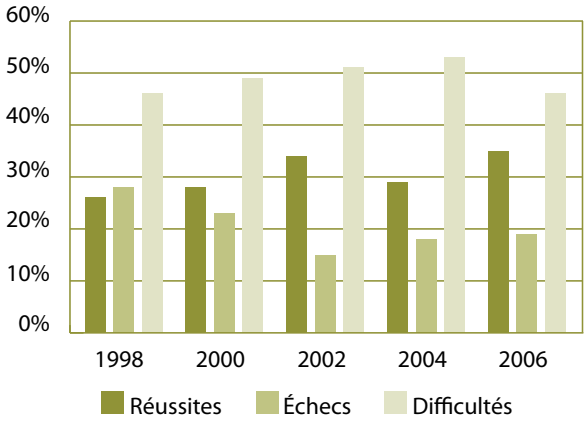
[5 et 6] *20 questions que les administrateurs devraient poser sur les projets SI, 2007. Adapté avec l'autorisation de l'Institut Canadien des Comptables Agréés, Toronto, Canada. Toute modification apportée au document d'origine relève de la responsabilité exclusive de l'éditeur et n'a été ni revue, ni validée par l'ICCA.*

deux alertes sur résultats au cours du dernier trimestre de l'exercice. Ce problème a entraîné de grandes difficultés au niveau de la distribution des produits pendant la période cruciale des fêtes de fin d'année. À la fin de l'exercice, le cours de l'action avait chuté de 27 %, un résultat d'autant plus décevant que la Bourse était alors en forte hausse[6].

2.4 Statistiques historiques sur la réussite et l'échec des projets SI

Ces vingt dernières années, les chiffres concernant les échecs des projets SI ont été systématiquement étudiés et publiés par de nombreux analystes et consultants, notamment les cabinets Gartner Group, Forrester Group, The Standish Group et KPMG. Il existe bien trop de rapports et de statistiques pour les étudier ici, mais le responsable de l'audit interne doit avoir connaissance de ces études pour bien comprendre les risques inhérents aux projets SI. Les auditeurs ont intérêt à examiner les statistiques et les échecs qui s'appliquent à leur organisation et à leur secteur. Ces statistiques peuvent être présentées à la direction générale lorsqu'est évoqué la nécessité de réaliser des audits de projet.Voici quelques exemples de recherches pertinentes sur l'échec de certains projets.

- Le CHAOS Report 2007 du Standish Group[7] récapitule les résultats des recherches menées par le groupe entre 1998 et 2006. Ces données montrent que la réussite d'un projet n'est jamais garantie. En 2006, 65 % des projets ont soit échoué, soit été menacés, autrement dit une partie des objectifs n'a pas été atteinte ou le projet n'a pas respecté toutes les contraintes de calendrier et de coût.
- La société CA, Inc. a financé au Royaume-Uni un groupe de recherche indépendant, Loudhouse, pour enquêter sur 100 directeurs des SI au Royaume-Uni et en Irlande. L'étude a conclu qu'une mauvaise visibilité de l'état des projets SI et le manque de maîtrise des projets par la direction générale coûtait chaque année 250 millions de livres sterling (350 millions de dollars) aux entreprises britanniques. Un tiers des projets mis en œuvre chaque année sont hors budget, le dépassement étant généralement de 10 à 20 % par rapport au budget initial. L'enquête a également mis en avant la complexité croissante des projets SI : à tout moment, une entreprise ordinaire a en moyenne 29 projets en cours, et son budget SI moyen est compris entre 1 et 5 millions de livres sterling[8] (entre 1,4 et 7,03 millions de dollars).



	1998	2000	2002	2004	2006
Réussites	26%	28%	34%	29%	35%
Échecs	28%	23%	15%	18%	19%
Difficultés	46%	49%	51%	53%	46%

Tableau 1. Étude CHAOS

- Une étude de KPMG sur la gestion des projets SI dans le monde, publiée en 2005, indiquait que 49 % des personnes interrogées avaient assisté à au moins un échec au cours des douze mois précédents. Ce rapport révélait en outre que 59 % des organisations ne disposent d'aucun processus ou simplement d'un processus informel pour déterminer si un projet est en passe de fournir les bénéfices attendus[9].

Ce ne sont là que quelques exemples. Si l'on peut contester dans le détail la précision de ces statistiques, le fait est que l'échec d'un grand nombre de projets a été régulièrement signalé.

[7] *The CHAOS Report 2007, The 10 Laws of CHAOS, The Standish Group, 2007.*

[8] *Over Budget IT Projects Cost UK Plc £256m Per Year, CA Inc., 12 septembre 2007.*

[9] *Global IT Project Management Survey.* © 2005 KPMG International. KPMG International est une coopérative suisse qui coordonne tout un réseau de sociétés indépendantes travaillant sous la marque KPMG. KPMG International ne fournit aucun service aux clients. Chaque société membre de KPMG International est une entité juridiquement distincte et indépendante et se présente comme telle. Tous droits réservés. Imprimé à Hong Kong. KPMG et le logo KPMG sont des marques déposées de KPMG International, coopérative de droit suisse. Août 2005.

2.5 Dix facteurs clés de réussite d'un projet

Pour lutter contre ces échecs, de nombreux groupes de recherche suggèrent des mesures pour s'assurer les meilleures chances de succès. Le Standish Group publie un rapport annuel qui s'appuie sur l'étude des raisons de la réussite de certains projets. Les dix règles suivantes sont tirées du dernier rapport Standish sur la gestion de projet, « The CHAOS Report 2007.[10]»

1. **Participation des utilisateurs –** Les utilisateurs des directions métiers et des SI participent aux principaux processus de réalisation d'un consensus, de prise de décision et de collecte d'informations.
2. **Soutien de la direction générale –** Les dirigeants assurent la cohérence avec la stratégie de l'organisation, ainsi qu'un soutien financier et psychologique et une assistance dans la résolution des conflits.
3. **Clarté des objectifs de l'organisation –** Les partenaires comprennent l'intérêt intrinsèque du projet et sa cohérence par rapport à la stratégie de l'organisation.
4. **Souplesse de l'optimisation –** Le projet emploie des processus itératifs de développement et d'optimisation pour éviter les éléments inutiles et s'assurer que les éléments essentiels sont bien intégrés.
5. **Maturité psychologique –** Le chef de projet gère les émotions et les actions des partenaires du projet et évite certaines attitudes (ambition, arrogance, ignorance, abstention et déloyauté).
6. **Connaissance de la gestion de projet –** L'organisation fait appel à des chefs de projet qui ont les compétences et connaissent les pratiques de base, par exemple des chefs de projets titulaires de la certification PMP (Project Management Professional) du Project Management Institute (PMI) ou d'une certification équivalente.
7. **Gestion financière –** Le chef de projet est capable de gérer les ressources financières, de justifier le budget ou les dépenses et d'expliquer l'intérêt du projet.
8. **Compétences des ressources –** Des personnes compétentes sont recrutées, dirigées, retenues et contrôlées afin de pouvoir continuer à avancer en cas de problèmes de personnel, notamment de rotation du personnel.
9. **Formalisation de la méthodologie –** Il existe un ensemble prédéfini de techniques basées sur les processus qui constituent une feuille de route où sont indiqués les événements qui doivent se produire, quand, comment et dans quel ordre.
10. **Outils et infrastructure –** L'infrastructure du projet est élaborée et gérée à l'aide d'outils permettant la gestion des tâches, des ressources, des exigences, des changements, des risques, des fournisseurs, de l'adhésion des utilisateurs et de la qualité.

2.6 Objectifs et avantages de l'implication des auditeurs internes

Si tous les facteurs de réussite indiqués plus haut relèvent de toute évidence de la direction générale, les auditeurs internes peuvent apporter beaucoup en évaluant l'efficacité de la gestion des risques pour les aspects aussi bien technologiques qu'organisationnels des projets SI. L'audit interne est une activité indépendante qui permet de déterminer si une organisation ou une fonction atteint les objectifs fixés. Les auditeurs internes analysent les processus et les opérations de façon méthodique afin de mettre en lumière les problèmes et de proposer des mesures correctives. Étant donné les risques associés aux projets SI indiqués précédemment, la participation des auditeurs internes tôt dans le processus, avec leur expérience et leur méthode, permet d'augmenter les chances de réussite. La participation des auditeurs internes présente plusieurs avantages, parmi lesquels :

- L'apport de conseils indépendants tout au long du projet.
- L'identification précoce des principaux risques et problèmes, ce qui permet à l'équipe du projet d'agir de façon préventive pour atténuer les risques.

[10] *The CHAOS Report 2007, The 10 Laws of CHAOS, The Standish Group, 2007.*

3. Cinq thèmes centraux dans l'audit des projets

Si les recherches indiquent la nature de certains risques, elles montrent aussi qu'une intervention précoce est la clé du succès. Comme nous l'avons vu en introduction, ce GTAG se concentre particulièrement sur cinq grands thèmes qui peuvent servir de base à l'élaboration d'une méthodologie d'audit. Les cinq catégories suivantes correspondent logiquement aux thèmes à étudier, le choix s'est fait d'après différentes recherches et à partir de l'expérience des auteurs dans les diverses méthodologies d'évaluation des risques des projets.

1. Alignement des objectifs de l'entreprise et des SI.
2. Gestion de projet.
3. Opérationnalité des solutions SI.
4. Gestion des changements au niveau de l'organisation et des processus.
5. L'après-projet (Post-implémentation).

Les paragraphes suivants apportent des éléments de réflexion sur chacun des cinq thèmes centraux. L'annexe F propose une liste de questions utiles lors de l'audit, ainsi que des exemples de risques et de contrôles spécifiques à chacun de ces cinq thèmes.

3.1 Alignement des objectifs et des SI

Alignement signifie simplement que la vision et les objectifs de l'organsation et des SI sont bien compris, qu'ils concordent entre eux et que le projet s'inscrit en droite ligne de la stratégie de l'organisation. Presque tous les projets présentent des interdépendances entre différents niveaux et fonctions d'une organisation. Autrement dit, réaliser cet alignement et le maintenir est une véritable gageure pour toute la durée du projet ! Des réunions régulières avec toutes les parties prenantes présentes ainsi que l'existence de canaux permettant un flux de communication ouvert, sont essentiels, de même que l'implication totale de *sponsors* apportant l'orientation, le temps et l'énergie exigés par le projet. Outre celui du *sponsor*, le choix de l'équipe de projet est aussi crucial. Une équipe peu motivée et sans l'expérience et les compétences nécessaires est un obstacle fréquent à la réussite de l'opération. L'alignement du projet comporte de multiples facettes qui sont, pour la plupart des organisations, intégrées à l'analyse de rentabilité.

Évaluation de l'analyse de rentabilité

Avant de lancer un projet, la direction générale a besoin d'informations pour déterminer si l'idée de départ est viable. Suivie par une équipe dédiée, la préparation de l'analyse de rentabilité fournit les informations permettant de décider de réaliser le projet ou non. La décision finale peut être prise par le comité de pilotage du projet ou à un niveau supérieur de l'organisation. En fait, des guides d'audits entiers sont consacrés à l'examen de l'analyse de rentabilité. Nous nous attacherons donc simplement, dans ce GTAG, à quelques-unes des catégories de risque courantes.

L'analyse de rentabilité doit notamment indiquer :

- Les bénéfices attendus, qui doivent être réalistes, compris et mesurables.
- Les problèmes liés au contexte, notamment le paysage règlementaire, la compatibilité architecturale, etc.
- Des questions relatives à l'organisation, par exemple les personnes à impliquer et leur fonction d'origine.
- Un périmètre de projet clairement défini.
- Les livrables du projet, en termes de processus et de fonctionnalités.
- Les ressources requises (financières et humaines).
- L'analyse des risques concernant la viabilité des partenaires ou des fournisseurs.
- La mesure ou les probabilités de succès.

Lors de l'élaboration de l'analyse de rentabilité, il est essentiel de préciser non seulement l'impact du projet, mais aussi qui en est le *sponsor*. Dès le début du projet, les *sponsors* doivent en comprendre toutes les implications et veiller à ce que toutes les parties prenantes, internes et externes, soient prises en compte. Les parties prenantes directes sont, entre autres, les services et fonctions internes à l'organisation qui utiliseront le nouveau système, les clients ou fournisseurs externes susceptibles d'interagir avec celui-ci et toute autre personne ayant un intérêt dans le projet. Il est également important de veiller à ce que les partenaires indirects soient consultés rapidement (il peut s'agir de services liés à la finance, à l'audit interne, à la sécurité des SI, au service juridique, aux achats ou chargé de la réglementation). Tous les groupes concernés doivent donner leur avis, même ceux pour lesquels l'impact risque d'être minime, afin que toutes les remarques puissent être prises en compte.

L'analyse de rentabilité doit s'assurer que toutes les alternatives possibles sont envisagées. Les choix les plus courants sont le développement d'une solution en interne ou l'achat d'une solution auprès d'un fournisseur tiers ; l'utilisation de ressources internes ou le recours à l'externalisation ; et, bien entendu, la réponse à une obligation réglementaire ou la recherche de la performance opérationnelle. Dans l'examen des alternatives, une analyse de rentabilité solide permet à la direction générale de prendre une décision en connaissance de cause, en tenant compte des avantages et des inconvénients. Enfin, l'analyse de rentabilité doit évaluer la capacité de l'organisation à entreprendre le projet, son niveau de priorité et déterminer si l'organisation dispose de personnes avec les compétences nécessaires pour le réaliser.

3.2 Gestion de projet

Comprendre la gestion de projet

Comme le montre la figure 1 (p.2), la gestion de projet est au cœur des cinq thèmes centraux. Comme l'audit interne, la gestion de projet est une profession avec ses propres bonnes pratiques, sa terminologie et ses normes. (Étant donné la quantité et l'ampleur des guides disponibles sur cette profession, nous donnons dans les annexes de ce GTAG un résumé des documents de référence sur la gestion de projet, ses bonnes pratiques et ses normes). Les auditeurs devront veiller à bien comprendre les risques liés à la gestion de projet. Même avec une expérience solide du SI et du métier, l'auditeur risque de s'apercevoir qu'un grand nombre de bonnes pratiques de gestion de projet ne lui sont pas familières. Les auditeurs internes consacreront du temps à l'étude et à la compréhension des processus et de la terminologie propres à cette activité.

Voici quelques termes fondamentaux de la gestion de projet :

- **Portefeuille de projets –** Ensemble de projets d'une organisation. Un programme peut comporter plusieurs projets. Pour planifier, définir le périmètre ou évaluer un projet ou un programme, les auditeurs doivent comprendre les notions de gestion de projet, de gouvernance de projet et de méthodologie de gestion de projet telles qu'elles sont utilisées dans leur secteur et leur organisation.
- **Gestion de projet –** Activité consistant à organiser et gérer des ressources (par exemple, les ressources humaines et le budget) afin que le projet soit réalisé conformément aux contraintes de périmètre, de qualité, de délais et de coût prévues.
- **Gouvernance de projet –** Point de rencontre entre les projets et la gouvernance de l'organisation, elle régit la gestion de projet au niveau de l'entité. Elle veille à ce que l'organisation entreprenne les projets utiles, contrôle le portefeuille de projets, établisse des priorités, affecte l'autorité au niveau qui convient et dispose de processus adaptés de prise de décision. Une bonne gouvernance de gestion de projet relie entre eux tous les domaines illustrés à la figure 2 (p. 9) et leur assure le soutien nécessaire pour fonctionner efficacement.
- **Méthodologies de gestion de projet –** Vastes ensembles intégrés de politiques, normes, méthodologies, cycles de vie, procédures, outils, techniques, parties prenantes et organisations permettant de piloter la planification et l'exécution d'un projet. Le Standish Group rappelle que la méthodologie intègre également ce qu'il appelle « les 90 % restants de l'environnement du projet » (à savoir, l'affectif, la culture, la formation des parties prenantes et la maturité de l'organisation hors processus et procédures)[11].

Auditeurs et méthodologies de gestion de projet

De même qu'il n'existe pas deux organisations semblables, il n'existe pas non plus deux méthodologies de gestion de projet identiques. Chaque organisation utilise une combinaison différente de méthodologies, de cycles de vie, de bonnes pratiques, d'outils, etc.

Par exemple, les grandes entreprises de défense peuvent employer une méthodologie complexe, comme la gestion de la valeur acquise (EVM) qui permet de mesurer la progression du projet de façon objective en fonction à la fois du périmètre, du calendrier et du coût[12], pour assurer les gros contrats avec l'État. Une petite organisation, en revanche, utiliserait plutôt une feuille de calcul ou un logiciel de gestion de projet simple et prêt à l'emploi pour suivre les tâches du projet et leur statut.

Avant de réaliser un audit de projet, le responsable de l'audit interne et son équipe doivent d'abord bien cerner la méthodologie de gestion de projet de l'organisation (on parle également d'écosystème ou de cycle de vie). Ils doivent aussi connaître les bonnes pratiques, les risques et les contrôles liés à la fois à la gestion de projet et au développement de systèmes. Si ces relations ne sont pas bien comprises, le périmètre de l'audit de projet SI défini par l'auditeur risque de ne pas intégrer tous les risques possibles.

La figure 2 présente les éléments susceptibles d'être inclus dans une méthodologie et l'emplacement des principaux contrôles. Elle souligne également les relations entre les niveaux et les services existants, et montre jusqu'à quel niveau l'audit peut devoir aller pour donner une vision exacte de l'ampleur du projet. La méthodologie de gestion de projet de l'organisation donne le contexte dont l'auditeur a besoin pour réaliser l'audit. Pendant la planification et l'exécution des audits, l'auditeur pourra s'y appuyer pour identifier les principaux groupes de gouvernance de projet et les principaux points de contrôle de gestion du projet, et déterminer les politiques, les normes et les bonnes pratiques à utiliser comme références.

Le tableau 2 (p.10), Éléments de la méthodologie de projet et leur intérêt pour l'auditeur, souligne les principaux éléments de la méthodologie et précise leur utilité pour l'auditeur.

[11] *CHAOS Chronicles Online, v14.2.1, Glossary Definition of Ecosystem, The Standish Group, 2008.*
[12] *Practice Standard for Earned Value Management, Project Management Institute, mars 2005.*

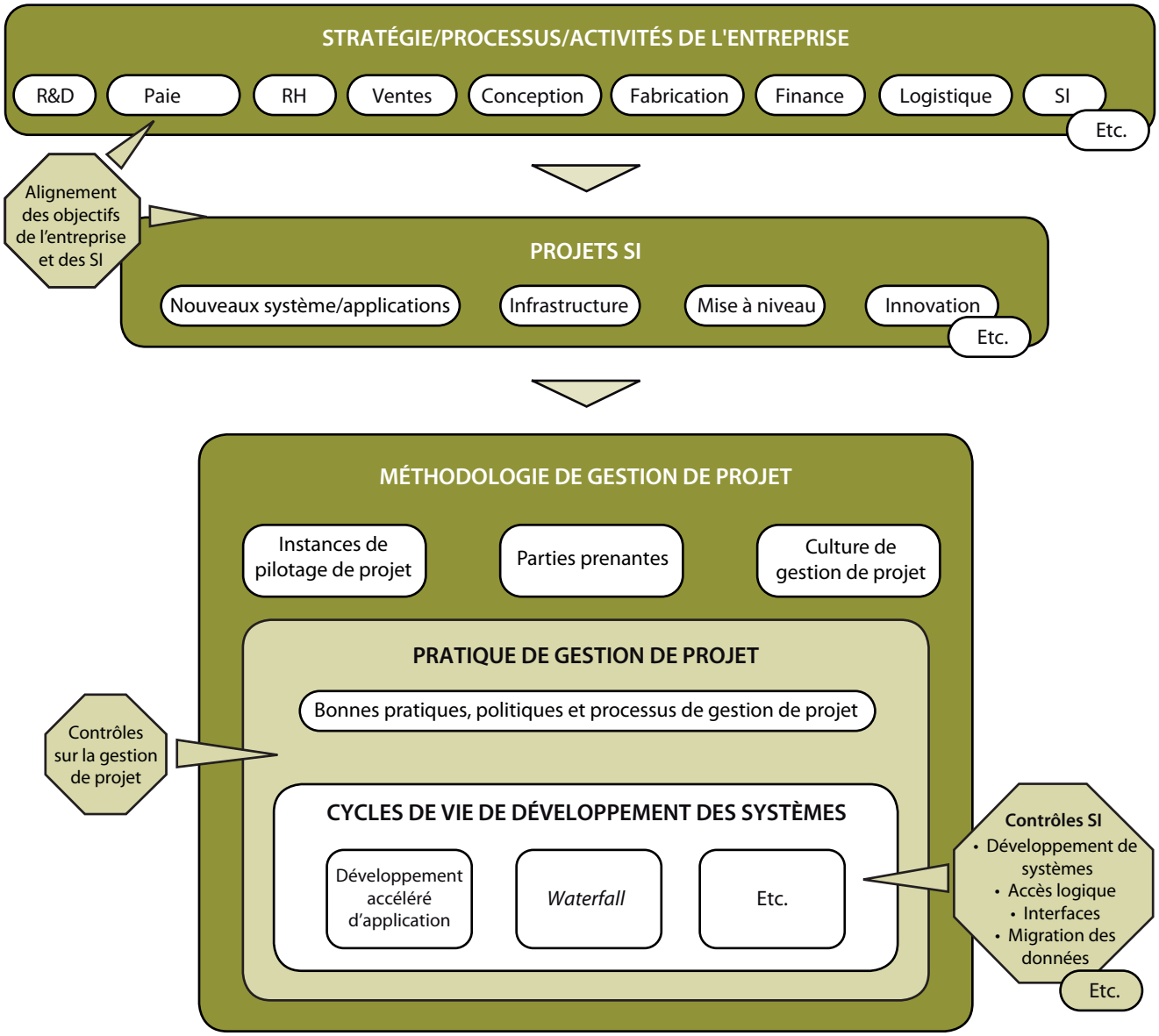


Figure 2. Méthodologie de gestion de projet. Adapté et révisé d'après le document *IT Control Objectives for Sarbanes-Oxley, Second Edition,* utilisé avec la permission de l'ITGI (IT Governance Institute) © 2006 ITGI. Tous droits réservés.

Élément de la méthodologie	Intérêt pour les auditeurs	Exemples
Organisation		
Parties prenantes du projet	Apporter aux auditeurs des points de vue multiples (métier, SI, sous-traitants, etc.) sur les risques et les problèmes associés à chaque projet.	• Responsable métier • Responsable SI
Bureaux de gestion de projet	Offrir un lieu central pour l'identification et l'examen de toutes les méthodologies de projet et des obligations concernant les livrables, pour faciliter la planification annuelle des audits et la définition de leur périmètre, l'élaboration de programmes d'audit, etc.	• Stratégique/Global • Projet unique • Directions métiers
Modèles et méthodes		
Gestion du portefeuille de projets	Offre un lieu central pour l'identification et l'examen de tous les projets, pour faciliter la planification annuelle des audits, leur classement par ordre de priorité, etc.	• Stratégique/Global • Projet unique
Modèles de maturité de la gestion de projet	Offre une « référence » pour la planification des audits de projet. Les auditeurs peuvent évaluer les méthodologies de projet et les processus pour identifier les failles et proposer des améliorations.	• Modèle P3M3 (*Portfolio, Program, and Project Management Maturity Model* ou modèle de maturité de gestion de portefeuilles, de programmes et de projets) • Modèle OPM3 (*Organizational Project Management Maturity Model* ou modèle de maturité organisationnelle de gestion de projet)
Modèles de maturité de développement des systèmes	Offre une « référence » permettant de définir le périmètre des audits de projet et de les planifier. Les auditeurs peuvent évaluer les méthodologies et les processus du projet pour identifier les écarts à comble.	• Modèle CMMI (*Capability Maturity Model Integration for Development*) • Norme SPICE (*Software Process Improvement and Capability dEtermination*)
Cycle de vie de développement des logiciels (SDLC)	Offre une base pour l'identification et l'évaluation du respect des processus de développement des systèmes, et indique quand suivre ou non une démarche donnée.	• *Waterfall* • Méthode RAD (*Rapid Application Development* ou développement accéléré des applications)
Guides de bonnes pratiques de gestion de projet	Offrent une base pour le développement d'une démarche d'audit et pour l'évaluation des performances de l'organisation et du projet.	• PMBOK (*Project Management Body of Knowledge*) • Méthode PRINCE2 (*Projects in Controlled Environments*)
Outils automatiques	Permettent l'examen des calendriers d'audit, des dépenses, de l'allocation des ressources, des problèmes, etc. Si des outils de gestion du portefeuille sont utilisés, ils permettent à l'auditeur d'établir des rapports contenant tous les projets, afin de les classer par niveau de risque en fonction des budgets et des calendriers, et d'utiliser des indicateurs afin d'identifier les «projets menacés ».	• Gestion du calendrier • Gestion des ressources • Suivi des problèmes

Tableau 2. Éléments de la méthodologie de projet et leur intérêt pour l'auditeur

Parties prenantes du projet

Les auditeurs internes doivent comprendre comment les parties prenantes sont choisis par l'organisation et intégrés aux projets SI. Les parties prenantes sont l'ensemble des personnes et des groupes qui font exister le projet. Les projets ne peuvent tout simplement pas être menés à bien si les parties prenantes concernés ne collaborent pas de façon coordonnée. Parmi eux, les cadres doivent apporter des conseils stratégiques ainsi qu'un soutien financier, politique et psychologique. Au niveau des métiers et des SI, les parties prenantes doivent veiller à ce que les spécifications et le produit final répondent bien aux besoins métiers prévus. Le nombre et le type de parties prenantes varient selon les organisations et les projets (voir la liste des parties prenantes habituelles à l'annexe B).

Les instances de pilotage de projet (IPP) et l'auditeur interne

Si l'organisation a des instances de pilotage de projet, ce sera un point de départ important pour l'auditeur interne pour comprendre la culture, les méthodologies, les normes et les processus de gestion de projet de l'organisation. De nombreuses organisations créent des instances de pilotage de projet pour qu'il contribue à la gouvernance et à la réussite des projets dans l'ensemble de l'organisation. Selon les études réalisées par le *Project Management Institute*, les principales raisons de créer des instances de pilotage de projet sont la volonté d'améliorer le taux de réussite des projets, de normaliser les pratiques et de réduire les coûts. Si les petites organisations peuvent gérer leurs projets efficacement sans instances de pilotage de projet, les grandes organisations ayant un grand nombre de projets, auront du mal à les mener à bien en l'absence d'instances de pilotage de projet.

Compte tenu du rôle critique que peut jouer les IPP dans une méthodologie de gestion de projet, l'auditeur doit absolument établir et entretenir des liens étroits avec elle. Les IPP peuvent tenir une place importante pendant les audits de projet et constituer un intermédiaire précieux entre l'équipe d'audit interne et les chefs de projet. De leur côté, les auditeurs peuvent avoir un rôle de conseillers auprès des IPP, avec qui ils partageront leur vision des risques du projet SI et fixeront les attentes de l'audit concernant les IPP et chacun des projets. Les auditeurs des projets SI tenteront de comprendre les points suivants :

- rôles et fonctions des IPP ;
- méthodologies de gestion de projet ;
- données et tendances concernant le budget et le calendrier du projet SI ;
- taux de réussite/échec des projets SI, statistiques, indicateurs et enseignements ;
- tendances induisant la réussite ou l'échec de l'ensemble des projets SI.

Ils essaieront également d'obtenir la liste annuelle des projets SI approuvés et financés, classés par budget, niveau de risque ou d'autres facteurs clés, ainsi que la liste des étapes majeures et des dates de mise en service des principaux systèmes déployés.

Gestion du portefeuille de projets

La gestion de portefeuille de projets renvoie à la gestion collective des projets, dont l'objectif est de s'assurer que les décisions d'investissement sont solidement étayées. Les organisations ont recours à la gestion du portefeuille de projets pour fonder leurs décisions d'investissements dans les SI, garantir un financement adapté pour les différents besoins de l'organisation et souligner le rôle des SI dans l'organisation en mettant en exergue l'intérêt de toutes les initiatives et de tous les projets SI. Les auditeurs internes peuvent se servir de cet outil pour identifier les projets à haut risque et les grandes priorités de l'organisation.

Les auditeurs internes et les modèles de maturité

De manière générale, les modèles de maturité servent à aider les organisations à évoluer vers des processus de plus en plus matures. Ils favorisent l'identification des défauts et des lacunes dans les capacités à faire et précise son niveau de maturité actuel, puis contribuent à l'élaboration d'une stratégie pour passer au niveau de maturité suivant. L'idée générale est de développer des processus bien définis, solides et reproductibles. Il existe des modèles de maturité spécifiques pour le développement de logiciels et la gestion de projets (voir la présentation des modèles de maturité à l'annexe D).

Les auditeurs peuvent s'appuyer sur les modèles de maturité pour évaluer les processus de gestion de projet et/ou de développement de systèmes de l'organisation. Mais cela n'a sans doute de sens que si l'organisation a déjà choisi son modèle de maturité et structure ses processus en fonction de ce modèle. Si l'organisation envisage de mettre en œuvre son premier modèle de maturité, l'équipe d'audit interne peut réaliser un premier audit en prenant pour référence la norme de maturité proposée. Cet audit fournira à l'organisation des données de référence pour commencer à utiliser le modèle de maturité en question.

Les auditeurs devront considérer l'utilisation de modèles de maturité par l'organisation comme une démarche très positive, propre à améliorer la gestion de projets SI. Toutefois, rien n'oblige une organisation à les utiliser, et beaucoup s'en passent pour des raisons de coût et de complexité.

Bonnes pratiques de gestion des projets SI

Les bonnes pratiques sont pour les auditeurs le point de départ idéal pour structurer la démarche d'évaluation des risques et d'audit. Les bonnes pratiques sont issues à la fois de guides généralistes de gestion de projet et de guides

spécifiques au développement SI. Les normes suivantes sont parmi les plus largement acceptées :

- PMBOK (Project Management Body of Knowledge)[13] ;
- PRINCE2 (PRojects IN Controlled Environments)[14];
- CobiT (Control Objectives for Information and related Technology)[15];
- Normes ISO (Organisation internationale de normalisation)[16].

Les auditeurs internes ne doivent pas compter sur la mise en œuvre par l'organisation de la totalité des normes PMBOK, PRINCE2, CobiT ou d'autres grands référentiels de bonnes pratiques. Mais ils doivent s'attendre à voir ces pratiques personnalisées et intégrées à la méthodologie de gestion de projet de l'organisation. L'annexe E, Bonnes pratiques générales de gestion de projet, donne plus de détails sur chacune de ces bonnes pratiques et sur ces cadres de référence.

Outils de gestion de projet et automatisation

Les auditeurs devront s'attendre à trouver un certain nombre d'outils automatisés de gestion de projet ou collaboratifs utilisés dans les projets. Ces logiciels peuvent servir pour la gestion de portefeuilles entiers contenant des centaines de projets et/ou pour des projets individuels. Avec l'aide de ces outils, les auditeurs pourront obtenir :

- des informations sur les problèmes liés au coût, au calendrier et aux techniques,
- des points de vue sur les prises de décision et le suivi des problèmes relatifs au projet,
- des informations sur l'utilisation des ressources.

[13] *Project Management Body of Knowledge (PMBOK), Project Management Institute, 2008.*
[14] *PRojects IN Controlled Environments (PRINCE2), Office of Government Commerce (OGC) du Royaume-Uni, 2008.*
[15] *Control Objectives for Information and related Technology (CobiT), IT Governance Institute, 2008.*
[16] *Normes ISO (Organisation internationale de normalisation), ISO, 2008.*

Voici quelques aspects du projet qui peuvent bénéficier de l'automatisation et des outils logiciels.

Gestion de projet

- Gestion du planning.
- Gestion des coûts.
- Gestion des exigences.
- Suivi des problèmes.
- Gestion des ressources.
- Gestion des risques.
- Gestion de la qualité.
- Collaboration de l'équipe/partage des connaissances.

Développement de systèmes

- Suivi des bogues logiciels.
- Test des logiciels.
- Gestion du code source et suivi des versions.

3.3 Opérationnalité des solutions SI

Les solutions SI ont un cycle de développement naturel qui comprend différentes étapes dont l'ordre doit être respecté pour que le besoin métier puisse être transformé en système ou en application et pour que la maintenance du système puisse être maîtrisée. En général, on parle de cycle de vie ou de cycle de vie du développement du logiciel (voir la figure 3 : Cycle de vie du développement générique de logiciels).

Les organisations peuvent utiliser leur propre méthodologie de cycle de vie pour des développements spécifiques, ou une méthodologie proposée par les consultants ou les fournisseurs (à utiliser avec leurs produits). Les cycles de vie de développement des logiciels peuvent varier selon le type de technologie développée. Ils peuvent être adaptés aux scénarios de développement ou de mise en œuvre suivants :

- Développement spécifique à l'aide de ressources internes.
- Développement personnalisé à l'aide de ressources entièrement ou partiellement externalisées, sur site ou hors site (implantation locale ou site délocalisé)
- Solutions logicielles achetées à un fournisseur et mises en œuvre en l'état, sans personnalisation préalable.

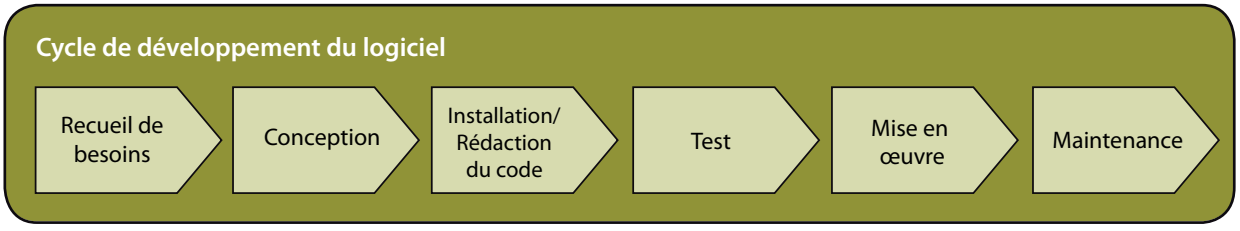


Figure 3. Cycle de vie générique de développement de logiciels

- Solutions logicielles achetées à un fournisseur et personnalisées pour répondre à des exigences précises.

Les modèles les plus connus de cycle de vie du développement du logiciel sont *Waterfall* et la méthode RAD (développement accéléré d'applications).

Dans tous les cas, les auditeurs internes peuvent s'attendre à une forme ou une autre de cycle de développement et pourront établir s'il est correctement suivi, en fonction des étapes du cycle de vie. Ils détermineront le moment pour réaliser l'audit du projet et les contrôles à tester.

La phase de mise en œuvre du projet n'est souvent envisagée qu'au moment où le nouveau système est « lancé » en production ; toute une série d'actions et de décisions critiques intervient pourtant pendant le projet. De nombreux échecs peuvent être attribués à l'absence de jalons, qui devraient être définis dans la méthodologie de gestion du projet, pour que l'équipe projet puisse prendre des décisions délibérées pour la bonne conduite du projet. Les projets par essence complexes, notamment les systèmes PGI (progiciels de gestion intégrés), devraient inclure des étapes de décision spécifiques pour chaque séquence majeure, qui permettent de s'assurer que le projet est en bonne voie.

Évaluation par un consultant extérieur

Pendant la phase de mise en œuvre de la solution ou du système, il n'est pas rare que l'équipe projet s'associe avec une société ou une ressource extérieure, notamment pour les gros logiciels tels que les systèmes PGI. Les auditeurs devraient s'assurer que la viabilité du prestataire externe a été revue, en particulier pour les projets qui s'inscrivent dans la durée. En outre, il faut absolument que les rôles et les responsabilités des différents intervenants soient bien définis dès le départ afin que chacun sache qui est responsable des livrables du projet.

Conception de la solution

Pendant la phase de conception de la solution, les auditeurs devraient vérifier que les besoins de l'organisation ainsi que les processus présents et à venir sont bien pris en compte. Au terme de cette étape, le périmètre du projet doit être gelé, et toutes les fonctionnalités devraient être classées par ordre d'importance pour le lancement du système. Il s'agit de distinguer les éléments indispensables des éléments utiles mais secondaires. C'est aussi généralement pendant cette étape que l'équipe projet prend la décision de développer la solution en interne ou de l'acheter à l'extérieur. Quelle que soit la décision prise, il est impératif de veiller à ce que les contrôles fonctionnels comme les contrôles de sécurité soient pris en compte et inclus dès le départ dans la solution.

Code, installation et données

Après la phase de conception, il devrait y avoir un processus permettant de vérifier le code ou d'installer le système à proprement parler. Dans le cycle de vie d'un système, il peut exister un grand nombre de règles ou de recommandations internes différentes applicables à l'audit. On peut, par exemple, procéder à une vérification du processus de développement du code pour déterminer si des méthodes de programmation solides et sécurisées sont suivies. Après l'installation du système, les configurations et les localisations ont lieu, elles-mêmes suivies de la conversion et/ou du chargement de données nouvelles ou héritées. C'est aussi à ce moment-là que sont établies les interfaces ou les connexions avec d'autres systèmes de l'organisation. La question du chargement des données est essentielle, en particulier pour tout ce qui concerne la préparation des données principales comme les fichiers de salariés, de clients ou de fournisseurs. Bien qu'il soit important de veiller à la continuité des informations issues du système précédent, il est impératif d'identifier clairement les données prioritaires avant de les charger dans le nouveau système. En d'autres termes, si l'ancien système contient des données obsolètes ou des doublons, il faut si possible les éliminer avant de procéder à une conversion.

Tests et mise en service

L'étape clé suivante est la phase de test. Il faut absolument déterminer si les tests doivent inclure non seulement les utilisateurs finaux, mais aussi les flux de tâches, la sécurité et la connectivité avec d'autres systèmes. Lorsque les tests sont terminés, un point de contrôle permet de décider si le système est prêt à être mis en service ou envoyé en production. La mise en service n'est pas un événement, mais une phase. Cette étape comprend un plan de transition pour transmettre le nouveau système de l'équipe du projet à l'équipe chargée de son fonctionnement quotidien et de l'assistance. Pendant cette étape, il est important de tenir compte des urgences et des stratégies de secours afin de limiter les imprévus susceptibles de survenir lors de la mise en œuvre finale. C'est une étape qui se caractérise par de fortes pressions pour afficher les progrès et respecter les délais, et, de fait, des aspects importants de la planification détaillée risquent d'être oubliés.

3.4 Gestion des changements au niveau de l'organisation et des processus

Quel que soit le projet, la gestion du changement au niveau de l'organisation et des processus sont souvent le plus important à gérer et, en fait, ce qui présente le plus de risques pour le projet. Les scenarii les plus complexes intègrent à la fois la modification des processus et des systèmes

d'information associés. Les processus de bonne gouvernance de la gestion de projet, tels qu'ils sont illustrés à la figure 2, permettent une gestion efficace. La gestion du changement concerne plutôt les aspects informels ou intangibles d'un projet, notamment la perception de son impact sur l'organisation et des modifications qu'il entraînera dans les habitudes de travail. Du point de vue de l'audit, c'est là qu'une équipe d'audit intégrée, capable de veiller, avec le bon niveau de compétences, à l'évaluation des aspects opérationnels et techniques, prend tout son sens.

Gestion de la communication

L'un des aspects les plus délicats de la gestion du changement tient au maniement de la communication au sens large : d'abord, il faut obtenir l'adhésion et la participation de toutes les parties prenantes, vendre les avantages ou les raisons d'être du projet, et gérer les attentes des utilisateurs finaux. Par exemple, quels seront les processus concernés par le nouveau système, et quelles répercussions les changements auront-ils sur les fournisseurs ou les clients ? Ces points devront être clairement établis au début du projet et être gérés bien au-delà du projet.

État de préparation organisationnelle

L'état de préparation organisationnelle suppose d'évaluer les changements apportés par le nouveau projet dans l'organisation et de gérer la résistance à ces changements. Cela s'applique particulièrement aux projets de centralisation des traitements, par exemple un centre de services partagé associé à la mise en œuvre d'un système PGI, ou ceux qui nécessitent une externalisation. Il est important de réaliser une évaluation des compétences du personnel existantes par rapport aux rôles créés ou modifiés, et de déterminer si les processus ou les flux de tâches sont clairement définis pour que l'organisation accepte le changement.

Formation

Quand un nouveau système est mis en œuvre, le succès de l'opération exige une formation adaptée pour tous les utilisateurs concernés. L'équipe d'audit devra évaluer si la formation est complète, si elle intervient au bon moment et si elle fait appel à des manuels d'utilisation adaptés. Elle doit aussi vérifier si la formation proposée à l'équipe SI et / ou au personnel d'assistance est suffisante pour leur permettre de prendre en charge le nouveau système.

Support post-lancement

Il est important que les auditeurs s'assurent qu'un plan de support après mise en service est établi. Ce plan devra couvrir l'organisation de l'équipe d'assistance, pour les problèmes aussi bien fonctionnels que techniques. Il convient de déterminer si l'équipe d'assistance a une taille adaptée à la charge de travail pendant et après la mise en service, cette charge étant généralement bien plus lourde qu'en temps normal. Par ailleurs, des plans d'urgence devraient être établis en cas de problème lors de la mise en service.

3.5 L'après projet (Post-implémentation)

La mise en service du système est inévitablement suivie d'une période de stabilisation. Pendant cet intervalle, les utilisateurs s'habituent au système ou aux nouvelles fonctionnalités et les problèmes en suspens sont résolus. C'est aussi pendant cette période qu'il faut prendre garde à certains risques majeurs, liés pour la plupart à la gestion du changement. En d'autres termes, les auditeurs doivent déterminer si le nouveau système est correctement utilisé et si les fonctionnalités répondent bien aux exigences. Si la mise en place du nouveau système s'est accompagnée d'un grand nombre de changements au niveau des processus métiers, la période de stabilisation peut durer un certain temps. Il est important d'identifier si la résistance au changement se prolonge. Par exemple, les utilisateurs trouvent-ils le moyen de contourner ou de court-circuiter le système parce que celui-ci n'est pas aussi convivial que son prédécesseur ? Pour le savoir, il peut être utile de discuter ou de mener des entretiens avec les utilisateurs.

L'examen d'après projet peut être abordé de différentes façons. La section 4.3, p. 17, donne plus de détails sur la conduite de cet examen.

4. Planification de l'audit de projet

Les projets SI devraient être inclus de façon systématique dans le plan annuel d'audit interne. La figure 4, Processus de planification des projets SI, illustre la progression logique des étapes permettant, selon une approche descendante, de déterminer les projets à auditer. Cette progression est conforme au processus général de planification des audits décrit dans le *GTAG 11: Élaboration d'un plan d'audit des SI*[17].

Les auditeurs internes peuvent apporter beaucoup en évaluant à la fois les aspects technologiques et organisationnels des projets SI. Voici quelques-unes des principales questions que l'auditeur interne devrait envisager :

- Comment intégrer les audits de projets SI au plan d'audit annuel ?
- Quel est le rôle de l'auditeur interne ?
- Quels projets devraient être audités et pourquoi ?
- Quel type d'audit de projet l'auditeur interne doit-il réaliser ?

4.1 Projets SI et plan annuel d'audit interne

Pour inclure des projets dans le plan annuel ou à l'univers d'audit, l'audit interne doit avoir accès à la liste complète des projets SI ou technologiques de l'organisation. Dans l'absolu, il faudrait qu'une liste de tous les projets soit conservée sur un système centralisé dans lequel les auditeurs pourraient exécuter des rapports basés sur les facteurs de risque (coût du projet, planning, risques du projet, durée du projet, etc.). Si cette liste n'existe pas, les questions sur les projets SI ou technologiques pourront être posées au cours de la planification annuelle des audits, auprès à la fois des responsables SI et des principaux services de l'organisation. En outre, les auditeurs qui développent l'univers d'audit et le plan annuel ou qui planifient l'audit d'un projet particulier, trouveront toutes les informations utiles auprès des instances de pilotage de projet. Les auditeurs internes se rapprochent des instances de pilotage de projet pour délimiter et planifier l'audit d'un projet SI avant de passer à la phase d'exécution.

Les auditeurs pourront s'appuyer sur les points suivants lors de l'évaluation des risques du projet au niveau organisationnel, et pour déterminer comment inclure les projets SI au plan d'audit annuel :

- Aucun inventaire complet et précis de tous les projets (avec suffisamment d'informations complémentaires pour évaluer globalement les risques) n'est disponible.

[17] *GTAG 11 : Élaboration d'un plan d'audit des SI, p. 3.*

Comprendre la démarche de gestion de projet et le rôle de l'audit	**Définir l'univers de Projet SI**	**Effectuer une évaluation des risques**	**Formaliser le plan d'audit de projets**
• Déterminer si l'auditeur devrait assumer un rôle d'assurance ou de conseil. • Obtenir l'adhésion de la direction générale quant au rôle de l'audit interne dans les projets. • Déterminer la place des projets SI dans la mise en œuvre de la stratégie de l'organisation. • Comprendre le rôle des principaux groupes concernés par la gouvernance du projet (IPP, comités de suivi ?, etc.). • Comprendre la méthodologie de gestion du projet, les livrables, les étapes, etc.	• Identifier tous les projets SI dans l'organisation. • Vérifier que les listes de projets sont complètes et actualisées.	• Élaborer des processus d'identification des risques. • Évaluer les risques et classer les projets en fonction des facteurs de risque SI. • Évaluer les risques et classer les projets en fonction des facteurs de risque de l'organisation. • Prendre en compte les cinq principales catégories de risque identifiées dans ce guide.	• Identifier les projets à auditer, en fonction des risques. • Déterminer le type d'audit de projet à réaliser (état d'avancement du projet, etc.). • Déterminer le meilleur moment pour que l'audit soit le plus efficace (pré-projet, etc.)

Figure 4. Processus de planification des projets SI, d'après le *GTAG 11 : Élaboration d'un plan d'audit des SI.*

- Il existe un grand nombre de projets SI répartis dans toute la société.
- L'organisation ne dispose pas de méthodologies ni de processus centralisés pour la gouvernance de projet (en particulier, aucune méthodologie de gestion de projet ni de cycle de vie de développement des systèmes).
- La direction générale est trop confiante dans sa capacité à réaliser efficacement les projets, mais est incapable de démontrer l'existence d'inventaires de projets ou de méthodes centralisées.
- Les chefs de projet et la direction générale pensent que les auditeurs internes ne peuvent rien apporter aux projets et que les équipes projet sont trop occupées (du fait du manque de ressources, de l'imminence des échéances, etc.) pour apporter leur contribution à un audit.

4.2 Rôle de l'audit interne

À propos du rôle de l'auditeur interne, l'un des points à garder à l'esprit est la nature de l'organisation de l'audit interne. Il faut aussi se demander si l'auditeur interne a uniquement une mission d'assurance ou si des activités d'ordre plus opérationnel ou consultatif sont également permises. Les documents *Normes internationales pour la pratique professionnelle de l'audit interne* de l'IIA fournissent des conseils aux auditeurs internes pour remplir ces missions.

Les auditeurs internes peuvent apporter beaucoup au projet en s'engageant assez tôt et en soutenant l'équipe projet tout au long du cycle de vie de celui-ci. Ils peuvent être invités à participer au projet de plusieurs façons, des examens consultatifs aux audits internes. Mais cela peut être perçu comme une atteinte à l'indépendance de l'auditeur. L'auditeur informatique doit donc pouvoir garantir que s'il a un intérêt quelconque dans la solution SI, cet intérêt n'aura aucune incidence sur l'objectivité de l'examen, et que sa contribution se limite à apporter des conseils, non à prendre des décisions. L'auditeur informatique peut également s'appuyer sur une autre ressource, la directive G17 de l'ISACA (*Information Systems Audit and Control Association*), Effet d'un rôle de non-audit sur l'indépendance de l'auditeur SI[18].

Plus l'auditeur interne s'investit précocement dans le projet, mieux c'est. Les audits internes ou les évaluations réalisés en début de projet sont souvent les plus utiles, car ils permettent d'identifier rapidement les problèmes et d'en réduire le coût. Lorsque les auditeurs détectent des problèmes, ils recommandent souvent l'ajout de contrôles automatiques ou éventuellement des modifications dans la conception. Les études du développement logiciel montrent clairement que les corrections et les réglages des logiciels sont beaucoup moins coûteux en début de projet, par exemple pendant la phase de conception, que pendant les dernières étapes. L'identification et la correction d'un

[18] *Directive d'audit des SI : Effet d'un rôle de non-audit sur l'indépendance de l'auditeur des SI, Information Systems Audit and Control Association, 2003.*

[19] Reproduit avec l'autorisation de Steven Rakitin, *Software Verification and Validation: A Practitioner's Guide*, Norwood, MA: Artech House Inc., 2001. © 2001 Artech House Inc.

[20] D'après *Software Verification and Validation for Practitioners and Managers*, Seconde édition.

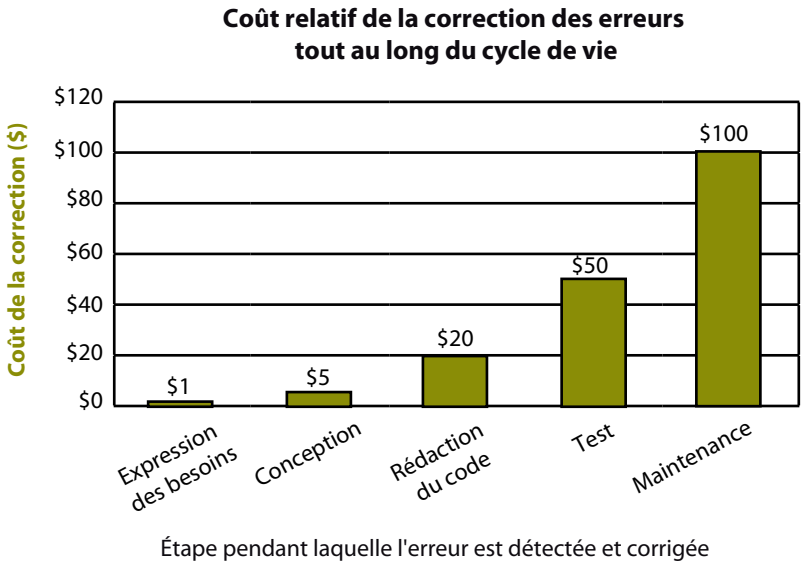


Figure 5. Coût relatif de la correction des erreurs tout au long du cycle de vie[20].

problème logiciel, après qu'il ait été livré, revient souvent cent fois plus cher que s'il avait été identifié et corrigé pendant la phase d'expression des besoins ou de conception[19]. La figure 5, Coût relatif de la correction des erreurs selon l'étape du cycle de vie, montre les dramatiques différences dans le coût de correction et de modification du logiciel selon l'avancement du projet. Ce peut être un argument de poids s'il faut convaincre la direction générale de soutenir une implication précoce des auditeurs internes dans le projet.

4.3 Types d'audits de projet

Les auditeurs internes peuvent réaliser différents types d'examens, selon les risques inhérents au projet et les besoins de l'organisation. Ce GTAG privilégie cinq types d'audits de projet ou d'évaluations parmi les plus courants :

- évaluation des risques du projet pour estimer les chances de réussite ;
- évaluation de la préparation pendant les principales étapes ou avant le lancement ;
- revue post-projet ;
- audit d'une étape clé au cours du cycle de vie du projet ;
- évaluation de la méthodologie de gestion du projet.

Des exemples d'éléments d'appréciation pour chaque type d'audit sont fournis à l'annexe F.

Quel que soit le type de revue, l'essentiel est de s'assurer qu'un ensemble de compétences adéquat a été affecté à la mission. Les avantages d'une équipe d'audit interne intégrée deviennent alors évidents, puisqu'elle permet de garantir que tous les risques inhérents au projet, qu'ils soient fonctionnels ou techniques, sont inclus dans le périmètre de la revue. Une équipe d'audit intégrée devrait inclure des compétences sur le plan métier et technique.

Évaluation des risques

L'évaluation des risques comprend généralement un tour d'horizon de tous les aspects du projet, afin d'identifier les principaux risques susceptibles d'influer son exécution et de déterminer l'efficacité du suivi et des mesures d'atténuation de ces risques. Ce type de revue est également fréquent si la direction générale pense que le projet n'avance pas correctement, que les coûts dépassent le budget alloué ou que le projet a déjà pris du retard.

Évaluation de l'état de préparation

L'évaluation de l'état de préparation est une revue qui a lieu à une étape majeure du projet, en général après l'achèvement de l'analyse de rentabilité ou pendant la phase d'alignement, de conception de la solution ou de pré-lancement. Le but principal de ce type de revue est de garantir objectivement la réalisation de chaque phase et de s'assurer que la direction générale a bien été informée des derniers risques ou problèmes identifiés avant de passer à l'étape suivante.

Revue d'après-projet

La revue d'après-projet est réalisée à un moment prédéfini, après la mise en service du nouveau système. De nombreux éléments sont à prendre en compte pour fixer le moment de cet audit : laps de temps nécessaire au système pour se stabiliser, disponibilité de l'équipe projet pour corriger les problèmes, clauses du contrat avec le fournisseur et problèmes soulevés par les utilisateurs après le lancement du système.

Il existe différentes façons d'aborder la revue d'après-projet. L'objectif est soit d'évaluer si le projet a bien respecté la méthodologie de l'organisation ou le cycle de développement logiciel, soit de mesurer si le nouveau système fonctionne correctement. La revue d'après-projet prend généralement la forme d'un audit intégré car il est préférable d'examiner conjointement le système et les processus associés.

Pendant la mise en route du projet et l'élaboration de l'analyse de rentabilité, on signale les nombreux effets positifs que doit apporter le projet. Le bilan de réalisation des effets positifs est un autre type de revue d'après-projet, dont l'objectif est de déterminer si le projet a apporté les bénéfices, les économies ou les gains d'efficacité prévus. La recommandation G29 de l'ISACA sur la revue d'après projet donne des conseils spécifiques à ce type de bilan[21].

Une autre démarche consiste à auditer les résultats obtenus par rapport aux objectifs initialement fixés ou d'évaluer le déroulement du projet afin d'en tirer des enseignements applicables pour les projets suivants. L'équipe d'audit interne peut également réaliser une revue des processus de bout en bout qui inclura tous les aspects ou toutes les fonctionnalités ou encore les processus et le nouveau système d'information. Quelle que soit la méthode, il est essentiel de prévoir une période de stabilisation suffisante après le lancement.

La durée de cette période de stabilisation devra être déterminée à l'avance dans le plan du projet. En général, il faut compter trois à six mois selon la complexité du système. Les auditeurs internes tiennent aussi compte du délai de dissolution de l'équipe projet et identifient la personne en charge de la documentation du projet et en charge de la transition vers une phase normale de maintenance ou de perfectionnement permanent. Si l'on ne dispose pas d'une documentation suffisante, il peut être très difficile d'auditer un projet ou de comprendre pourquoi certaines décisions ont

[21] *IS Auditing Guideline G29: Post Implementation Review, Information Systems Audit and Control Association, 2004.*

été prises une fois que l'équipe projet est passée à autre chose.

Revue d'une étape clé

La revue d'une étape clé, entreprise au cours d'un projet, est une démarche proactive souvent appliquée aux projets à haut risque. Cette revue peut comporter une analyse du cycle de vie de développement logiciel ou de la conception du système, ou un bilan, avec la participation de l'auditeur interne, à une étape charnière du projet par exemple. Le principal objectif est généralement dévaluer si les méthodologies de gestion de projet ou la méthode SDLC sont strictement observées. Comme nous l'avons indiqué précédemment, l'auditeur interne peut collaborer avec les équipes projet à la résolution des problèmes tant que la correction des erreurs reste relativement peu coûteuse, avant que le système ne passe dans l'environnement de production. Si l'équipe d'audit interne s'implique assez tôt dans le projet, elle peut soulever des questions et émettre des suggestions susceptibles d'influer sur le projet de façon plus ou moins formelle. Pour les revues de cette nature, les auditeurs informatiques pourront se référer à deux des recommandations de l'ISACA sur l'audit des SI :

(1) Directive G17 : Effet d'un rôle de non-audit sur l'indépendance de l'auditeur des SI[22] et

(2) Directive G23 : System Development Life Cycle (SDLC) Review[23].

Évaluation de la méthodologie de gestion de projet

Un audit de la méthodologie globale de gestion du projet permet d'identifier les risques et de pointer les faiblesses de la méthodologie, ce qui peut contribuer à apporter des améliorations au niveau de toute l'organisation. Pour les organisations qui comptent trop de projets pour pouvoir les contrôler individuellement, ce type de revue est de portée plus générale. En outre, s'il a déjà vérifié la méthodologie, l'auditeur interne sera mieux préparé à auditer les projets individuels, puisque l'audit des instances de pilotage de projet lui servira de base solide pour comprendre les pratiques de l'organisation.

Quelques objectifs possibles de l'audit des méthodologies de projet :

- Évaluer la pertinence des méthodologies de gestion de projet.
- Déterminer si la méthodologie peut s'appliquer à tous les projets SI de l'organisation, des plus limités aux plus étendus.
- Évaluer l'efficacité du soutien administratif des instances de pilotage de projet (qui peut être défini dans la charte des instances de pilotage de projet ou dans un énoncé de mission).
- Déterminer si les politiques, normes, méthodologies et processus définis par les instances de pilotage de projet sont systématiquement appliqués et exécutés sur tous les projets de l'organisation.
- Évaluer la capacité des instances de pilotage de projet à apporter la valeur ajoutée prévue.
- Déterminer si les instances de pilotage de projet disposent d'un inventaire complet de tous les projets de l'organisation.
- Déterminer si les processus de gestion du portefeuille de projets fonctionnent efficacement.

Rapports d'audit de projet

Le rapport établi par l'équipe d'audit varie selon le type de revue effectuée et selon l'étape du projet à laquelle elle intervient. La *série 2400* des *Normes internationales pour la pratique professionnelle de l'audit interne* de l'IIA donne des conseils sur la communication des résultats. Toutefois, il convient de bien tenir compte du type de revue réalisée avant de déterminer le meilleur format pour l'organisation. Si, par exemple, l'équipe d'audit est impliquée sur toute la durée du projet, des états d'avancement ou des notes adressées au comité de pilotage du projet peuvent être une bonne solution. Pour une revue d'après projet, surtout s'il évalue l'ensemble des fonctionnalités du système et des processus métiers sous-jacents, le format classique de rapport peut être préférable.

4.4 Remarques des auditeurs externes

Comme les projets SI et technologiques peuvent avoir un impact déterminant sur les états financiers et les opérations de l'organisation, les auditeurs externes veulent généralement connaître les gros projets qui vont commencer. Plus précisément, ils s'intéressent aux projets SI qui peuvent avoir un impact important sur :

- l'élaboration des états financiers (par exemple, nouveau système Grand livre SAP),
- la génération de revenus (par exemple, système de traitement des commandes),
- la gestion des stocks,
- les grandes transformations, au niveau des métiers ou des SI, qui ont une incidence sur les données financières ou sur les systèmes qui les produisent,
- les grandes obligations règlementaires, notamment la loi Sarbanes-Oxley de 2002.

[22] Directive d'audit des SI G17 : Effet d'un rôle de non-audit sur l'indépendance de l'auditeur des SI, Information Systems Audit and Control Association, 2003.

[23] Directive d'audit des SI G23 : System Development Life Cycle (SDLC) Review, Information Systems Audit and Control Association, 2003.

Le responsable de l'audit interne collaborera avec les auditeurs externes pour comprendre leur vision des risques associés aux projets SI. L'un des principaux risques pour l'organisation est que l'auditeur externe n'ait pas connaissance des projets majeurs et qu'il ne souligne les principaux problèmes de contrôle qu'une fois que le nouveau système est en production, lorsque la modification des contrôles existants ou la mise en œuvre de nouveaux contrôles est beaucoup plus coûteuse.

5. Conclusion

En conclusion, « les auditeurs doivent considérer les projets comme l'occasion d'exploiter leurs principales compétences dans de nouveaux domaines, et, en même temps, de participer à une gestion efficace des risques, à la maîtrise des coûts et à la réussite des projets au niveau organisationnel », note Richard B. Lanza dans un article consacré aux risques des projets technologiques paru dans le magazine *Internal Auditor* en 2002[24] et toujours d'actualité. Grâce à l'intégration des projets dans l'univers d'audit, les auditeurs internes peuvent s'associer à la fois aux chefs de projet et à la direction générale pour contribuer à la réussite des projets.

[24] *« Technology Projects: The Riskiest Parts of the Business », Internal Auditor, 15 mai 2002, Richard B. Lanza, CPA, PMP.*

Annexe A : Gestion de projet

A.1. Méthodologies de gestion de projet

La méthodologie de gestion de projet SI est comparable à une boîte à outils destinée aux équipes projet. Une bonne méthodologie décrit les relations entre tous les processus de gestion de projet et d'organisation concernés. C'est une structure détaillée de processus reproductibles qui propose une feuille de route avec la nature des événements à venir, leurs échéances et leurs modalités. Pour les projets SI, la méthodologie s'appuie à la fois sur les bonnes pratiques de gestion de projet et de développement de systèmes. En général, elle se compose de phases, d'activités et de tâches interdépendantes qui mettent en jeu des jalons, des recommandations, des techniques/méthodes, des modèles, des échantillons et des rôles et responsabilités parfaitement documentés.

Une méthodologie est nécessaire pour :

- proposer un modèle de démarche normalisée et reproductible permettant de réaliser un projet ;
- promouvoir l'emploi de bonnes pratiques susceptibles d'augmenter les chances de réussite du projet ;
- définir l'environnement afin de pouvoir apporter des améliorations. D'après le SEI (Software Engineering Institute), un processus ne peut être amélioré ou reproduit que s'il a d'abord été défini ;
- augmenter les probabilités de réussite du projet et réduire les catégories de risque connues ;
- proposer une structure de gestion du projet aux chefs de projet ;
- garantir que les bonnes pratiques sont systématiquement appliquées sur tous les projets ;
- proposer un cadre pour évaluer l'efficacité des résultats du projet et de mettre à jour la méthodologie à partir des enseignements tirés du projet ;
- proposer un cadre pour contrôler systématiquement les performances du projet en se référant à un ensemble cohérent d'exigences concernant les livrables et les mesures de performance.

Éléments généralement présents dans une méthodologie :

- **Cadres :** composés d'étapes, d'activités et de tâches.
- **Recommandations :** définissent les activités nécessaires pour générer les livrables.
- **Techniques/méthodes :** donnent des conseils sur la façon de réaliser les activités.
- **Modèles et échantillons :** facilitent l'application des techniques recommandées.
- **Rôles :** indiquent qui est responsable de quoi.
- **Plan de projet :** répertorie les activités concernant le projet, globalement et en détail.

A.2. Cycle de vie de gestion du projet

D'après le *Project Management Institute*, le cycle de vie d'un projet comprend cinq étapes liées entre elles par les résultats produits, qui deviennent le point de départ de l'étape suivante.

1. **Mise en route :** autorisation du projet.
2. **Planification :** définition et mise au point des objectifs et sélection, parmi les démarches possibles, de celle qui permettra le mieux d'atteindre les objectifs prévus pour le projet ou pour l'étape.
3. **Exécution :** coordination des personnes et d'autres ressources pour mettre le plan à exécution.
4. **Contrôle :** vérification de la réalisation des objectifs du projet, par un suivi régulier et par la mesure des progrès réalisés, afin d'identifier les écarts par rapport au plan et de prendre les mesures correctives nécessaires.
5. **Clôture :** formalisation de la validation du projet ou de l'étape et finalisation dans les règles.

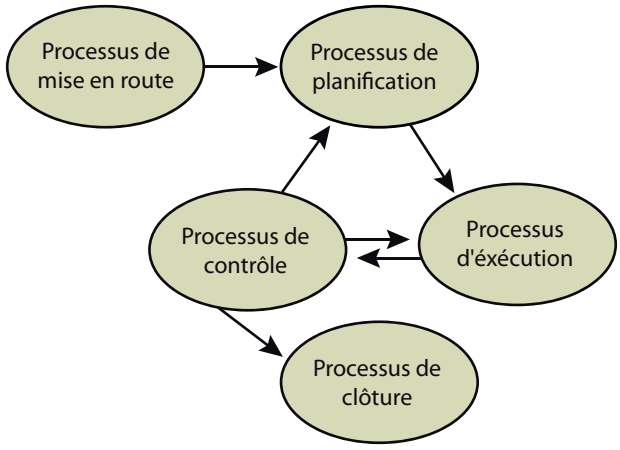


Figure 6. Principaux groupes de processus du cycle de vie du projet. Source : Project Management Institute, *Guide du Référentiel des connaissances en Management de projet (Guide du PMBOK®)* - Édition 2000, Project Management Institute Inc., 2000. Droits d'auteur et autres droits réservés. Les éléments de cette publication ont été reproduits avec l'autorisation du PMI.

Annexe B : Participants aux projets SI

La liste suivante indique les personnes susceptibles de participer au projet et la responsabilité qui leur incombe. Il existe beaucoup d'autres rôles possibles, et tous les rôles ne participent pas forcément à un même projet.

Parties Prenantes	Responsabilité
Comité de pilotage (exécutif ou technique)	Responsables exécutifs (métier et SI) qui influent sur les principes directeurs, la stratégie et les décisions importantes.
Sponsor	Personne qui apporte les ressources financières ou qui entérine le projet.
Chef de projet	Personne chargée de la responsabilité globale du projet. C'est le responsable hiérarchique à qui l'on doit des comptes.
Utilisateurs (métier, SI, etc.)	Personnes qui utiliseront le résultat du projet.
Équipe projet	Équipe qui travaille quotidiennement sur le projet et qui réunit des personnels SI et métiers.
Influenceurs	Personnes qui ne sont pas directement liées à l'utilisation du projet, mais qui, du fait de leur position, peuvent avoir une influence négative ou positive.
Instances de pilotage de projet (IPP)	Instances qui fournissent les chefs de projet ou les autres membres de l'équipe, et qui peuvent être directement ou indirectement responsable de l'issue du projet.
Comité de contrôle de la conformité	Équipe chargée d'évaluer le respect d'obligations ou de politiques particulières, par exemple la loi Sarbanes-Oxley de 2002, la législation locale, etc.
Sécurité des SI	Personnes qui veillent à ce que le système final intègre des fonctions de sécurité des SI conformes aux politiques de sécurité de l'organisation ou aux bonnes pratiques.
Comité d'architecture SI	Équipe qui veille à ce que le système soit compatible avec l'infrastructure actuelle ou future.
Consultants et fournisseurs	Consultants en développement ou fournisseurs du système concerné (par exemple, SAP, Peoplesoft, etc.).
Auditeurs (financiers, SI, externes et internes)	Personnes chargées de réaliser des audits et de donner leur vision des risques.
Achats	Personnes chargées de l'achat des pièces et des ressources nécessaires au projet.

Annexe C : Structure, rôles et responsabilités des instances de pilotage de projet

L'organisation des instances de pilotage de projet et le soutien apporté sont généralement de trois ordres :

Niveau organisationnel	Type de soutien apporté
Projet unique	Soutient ou gère entièrement un projet unique et très important, par exemple la résolution du bug de l'an 2000 ou la mise en œuvre d'un système global de planification des ressources de l'entreprise.
Directions métiers	Soutient différents projets au sein d'une même direction métier, généralement dans une organisation plus vaste, mondiale, comptant un grand nombre de directions métiers.
Niveau stratégique/global	Soutient tous les projets d'une organisation, quelle que soit la direction métiers propriétaire du projet..

Les rôles et les responsabilités des instances de pilotage de projet varient selon l'organisation. Ils peuvent inclure une partie ou la totalité des éléments suivants :

- proposer des rapports et un suivi du projet ;
- garantir un recadrage et une assistance pour les cadres et/ou les utilisateurs ;
- piloter un processus cohérent et reproductible ;
- proposer des missions de conseil et d'accompagnement du projet ;
- développer, mettre en œuvre et mettre à jour un cadre pour une gestion efficace du projet et incluant notamment des politiques, des normes et des méthodologies ;
- proposer une formation et un accompagnement des chefs de projet ;
- constituer un vivier de chefs de projets capables de gérer les projets de l'organisation ;
- analyser les projets qui ont échoué pour en tirer des enseignements utiles pour l'avenir ;
- participer à la préparation des différents projets en vue d'un audit ;
- soutenir la gestion de l'ensemble des projets de l'organisation, car il est associé à la gestion du portefeuille de projets.

Annexe D : Modèles de maturité

D.1. Modèle de maturité des capacités

Le premier modèle de maturité largement reconnu a été le modèle de maturité des capacités (ou modèle CMM-*Capability Maturity Model*) développé aux États-Unis par le *Software Engineering Institute* de l'université Carnegie Mellon. Ce modèle était axé sur le développement logiciel.

Le modèle de maturité des capacités, et désormais un grand nombre d'autres modèles, utilisent les niveaux de maturité suivants, avec pour objectif de passer du niveau 1 au niveau 5.

- **Niveau 1 :** Initial : peu de processus sont définis.
- **Niveau 2 :** Reproductible : les processus élémentaires de gestion du projet sont établis.
- **Niveau 3 :** Défini : les projets utilisent une version adaptée et approuvée du processus de développement standard de l'organisation.
- **Niveau 4 :** Maîtrisé : des mesures détaillées sont définies et contrôlées.
- **Niveau 5 :** Optimisé : un processus d'amélioration continue est en place.

D.2. Modèles de maturité de la gestion de projet

Les modèles de maturité de la gestion de projet fournissent un processus et un cadre pour l'évaluation des capacités actuelles de gestion de projet et pour le développement d'une stratégie d'amélioration. Voici deux exemples parmi bien d'autres de modèles de maturité de gestion de projet.

Modèle de maturité	Source	Description
Modèle P3M3 (*Portfolio, Program, and Project Management Maturity Model* ou modèle de maturité de management de portefeuilles, de programmes et de projets).	Office of Government Commerce (OGC), Royaume-Uni.	Utilise 32 domaines de performances critiques comme base d'évaluation et de passage d'un niveau de maturité à l'autre parmi les cinq niveaux standard.
Modèle OPM3 (Organizational Project Management Maturity Model ou modèle de maturité organisationnelle de management de projet).	Project Management Institute (PMI).	Suit une méthode extrêmement structurée pour évaluer la maturité d'une organisation en fonction de trois éléments interdépendants : connaissance, évaluation et amélioration.

D.3. Modèles de maturité du développement de systèmes

Les modèles de maturité de développement de systèmes fournissent un processus et un cadre permettant d'évaluer les capacités actuelles de développement de systèmes et de développer une stratégie d'amélioration. Voici deux exemples parmi bien d'autres de modèles de maturité de développement de systèmes.

Modèle de maturité	Source	Description
Modèle CMMI (Capability Maturity Model Integration for Development).	Software Engineering Institute (SEI).	Le SEI a développé le premier grand modèle de maturité de développement de logiciels, et il s'agit là de la nouvelle génération de ce modèle.
Modèle SPICE (Software Process Improvement and Capability determination).	Organisation internationale de normalisation (ISO).	Également connue sous le nom ISO 15504, cette norme fournit un cadre d'évaluation des processus logiciels, et a pour objectif de définir un modèle explicite pour la comparaison des processus.

Annexe E – Bonnes pratiques générales de gestion de projet

E.1.PMBOK et PRINCE2

La plupart des bonnes pratiques de gestion de projet sont énoncées dans les deux guides suivants :

Bonnes pratques	Source	Description
The Project Management Body of Knowledge (PMBOK).	Project Management Institute (PMI).	Norme reconnue internationalement (Norme IEEE 1490-2003). C'est l'ensemble de pratiques de gestion de projet la plus largement acceptée au monde.
Projects in Controlled Environments (PRINCE2).	Office of Government Commerce (OGC) du Royaume-Uni.	Approche structurée de la gestion de projet. Norme de fait au Royaume-Uni et dans d'autres régions d'Europe.

Aucun de ces deux guides ne concerne spécifiquement les projets SI, ni ne se veut un outil autonome de gestion de projet. Il s'agit de deux vastes ensembles de pratiques et de recommandations fondamentales applicables à différents secteurs et services, qui doivent être adaptés en fonction des besoins de chaque organisation. Qu'elle travaille à la construction d'un pont, au développement d'un nouveau service ou à la mise en œuvre d'une nouvelle application logicielle, l'organisation peut les utiliser. PMBOK et PRINCE2 se distinguent à plusieurs égards, mais tous deux offrent des bases valables pour le développement d'un cadre de gestion de projet SI.

PMBOK

Selon le PMI, le guide PMBOK décrit les connaissances de base généralement acceptées parmi les professionnels de la gestion de projet. Par « généralement accepté », on entend que les connaissances et les pratiques décrites s'appliquent à la plupart des projets, la plupart du temps, et que leur valeur et leur utilité réunissent un large consensus. L'objectif global du guide PMBOK est de fournir aux professionnels et aux praticiens de la gestion de projet un lexique commun pour parler et écrire sur ce sujet.

Le guide PMBOK commence par neuf grands domaines de connaissances sur le projet :

- gestion de l'intégration ;
- gestion du périmètre ;
- gestion des délais ;
- gestion du coût ;
- gestion de la qualité ;
- gestion des ressources humaines ;
- gestion de la communication ;
- gestion des risques ;
- gestion de l'approvisionnement.

Ces différents domaines sont encore divisés en 44 processus détaillés. Le guide PMBOK donne également des conseils sur la gestion de portefeuilles de projets et sur les bureaux de gestion de projet.

Le guide PMBOK est cohérent par rapport aux normes de l'Organisation internationale de normalisation (ISO) et au modèle CMM. C'est aussi le PMI qui gère la certification PMP (Project Management Professional) exigée par de nombreux organismes publics et institutions financières des États-Unis et du Royaume-Uni pour leurs responsables.

PRINCE2

PRINCE2 est conçu comme une méthodologie de gestion de projet générique, personnalisable et complète. Il se compose de huit catégories de processus :

- analyse de rentabilité ;
- organisation ;
- planification ;
- contrôles ;
- gestion du risque ;
- qualité ;
- gestion de la configuration ;
- contrôle des changements.

PRINCE2 intègre chaque processus à un cadre comprenant les principaux éléments à appliquer à l'ensemble du projet. Il couvre les modes d'organisation, de gestion et de contrôle des projets.

E.2.Normes de l'ISO

Les normes de l'ISO portent sur les bonnes pratiques de gestion de projet pour des secteurs ou des processus spéci-

fiques, par exemple la gestion de la qualité ou de la construction. En revanche, l'ISO ne dispose d'aucune norme dédiée aux pratiques générales de gestion de projet. Voici trois normes ISO qui traitent en partie des pratiques de gestion de projet.

- **La norme ISO 1006:2003** fournit des recommandations sur la qualité dans les processus de gestion de projet.
- **La norme ISO 9001** : 2005 porte sur la qualité dans le cadre du développement de services et de produits.
- **La norme ISO 15504** a pour objet la maturité de la gestion de projet.

Les auditeurs internes des organisations utilisant les normes de l'ISO veilleront à bien identifier les normes qui s'appliquent à leur secteur et à leur organisation. Les normes de l'ISO sont trop nombreuses pour être toutes examinées dans ce GTAG.

E.3. Sections du référentiel CobiT applicables à la gestion de projet

Le référentiel CobiT (Control Objectives for Information and related Technology) a été développé par l'ITGI (*IT Governance Institute*), en collaboration avec l'ISACA (*Information Systems Audit and Control Association*). Le référentiel CobiT est un cadre de gouvernance des SI vaste et complet qui inclut les objectifs de contrôle utilisables dans la gestion des projets SI.

S'il utilise le référentiel CobiT pour planifier les audits de projet, l'auditeur interne doit déterminer quels sont, parmi les objectifs de contrôle spécifiques de ce référentiel, ceux qui s'appliquent le mieux aux objectifs de l'audit. Nous insistons ici sur les thèmes des quatre domaines du CobiT les plus susceptibles d'être pertinents lors d'un examen de projet, mais d'autres peuvent aussi s'appliquer.

Planification et organisation

- Garantir la conformité avec les obligations extérieures
- Gérer les projets
- Gérer la qualité

Acquisition et implémentation

- Identifier les solutions automatisées
- Acquérir et mettre à jour les logiciels d'application
- Acquérir et gérer l'infrastructure technologique
- Élaborer et mettre à jour les procédures
- Installer et homologuer les systèmes
- Gérer les changements

Exécution et assistance

- Définir et gérer les niveaux de service
- Gérer les services tiers
- Gérer les performances et la capacité
- Assurer la continuité du service
- Assurer la sécurité du système
- Former les utilisateurs
- Surveillance et évaluation
- Surveiller et évaluer les performances SI
- Surveiller et évaluer le contrôle interne

E.4. VAL IT

Le cadre de référence Val IT, élaboré par l'ITGI (*IT Governance Institute*), est pour les auditeurs un outil puissant d'évaluation de la valeur d'un projet pour l'organisation. Le cadre Val IT constitue une méthode complète, uniforme et cohérente qui peut aider les responsables de tous niveaux à optimiser la rentabilité des investissements dans les SI[25]. Les auditeurs peuvent s'appuyer sur ce cadre pour structurer leur programme d'audit et évaluer l'intérêt du projet pour l'entreprise.

[25] Val IT, *IT Governance Institute, 2008.*

Annexe F – Points à vérifier lors de la revue des projets SI par les auditeurs internes

Le tableau suivant contient une liste de propositions de points d'audit qui peuvent être utiles lors de l'évaluation des cinq thèmes centraux mis en relief dans ce GTAG. Ces questions ont été adaptées à partir d'un programme de travail d'audit interne de la société Lafarge.

Analyse de rentabilité et alignement		
Domaine		**Critères**
1 — Analyse de rentabilité - Investissement/Réalisation des bénéfices		
1.1	Gestion de l'analyse de rentabilité	Une analyse de rentabilité du projet a été réalisée et approuvée.
		Cette analyse est mise à jour et détaillée à mesure que de nouvelles informations sont disponibles.
		Les hypothèses concernant les coûts et les bénéfices sont réalistes.
		Les hypothèses sont documentées et acceptées par tous.
		Les hypothèses sont expressément validées ou invalidées à mesure que le projet avance, et des mesures sont prises en conséquence.
1.2	Coût du projet	L'équipe de gestion du projet se fie aux estimations.
		Un modèle d'estimation standard est appliqué à tous les éléments de travail courants.
		Les personnes qui doivent comprendre et accepter le modèle sont clairement identifiées.
		Des fonds supplémentaires ont été alloués pour accélérer les projets de développement et permettre de tester la méthode, l'environnement, etc.
		Le budget comprend une estimation des frais de personnel et des autres dépenses (ressources matérielles/logicielles externes/internes, développements, tests complets, assurance qualité, suivi de la réalisation des bénéfices, coûts liés aux fournisseurs, frais d'exploitation, etc.).
		Les mesures d'urgence sont bien définies. En cas de problème, il existe un plan indiquant comment réagir.
		Les estimations ont été vérifiées par un tiers qualifié.
1.3	Historique	Le coût du projet a été modifié depuis l'analyse de rentabilité initiale.
		Des modifications ont été apportées. Si c'est le cas, comprendre pourquoi.
1.4	Échéancier	L'estimation de l'échéancier des dépenses est valable. Déterminer s'il est possible de repousser certaines dépenses.
		L'échéancier des dépenses a été modifié. Dans ce cas, comprendre pourquoi.

Analyse de rentabilité et alignement		
Domaine		**Critères**
1.5	Types de bénéfices	Les bénéfices attendus (par exemple, réduction des coûts, augmentation des revenus, amélioration de la qualité) sont clairement définis.
		La réalisation des bénéfices dépend de facteurs externes.
		La façon de traiter les interdépendances est bien définie.
		Les bénéfices attendus correspondent bien au contenu actuel du projet.
1.6	Réalisation des bénéfices	Les moyens de mesure des bénéfices sont clairement définis (par exemple, réduction des coûts directement répercutée dans le résultat, diminution du personnel ou réallocation des dépenses).
		Les personnes responsables de la réalisation des bénéfices sont clairement identifiées (on sait qui fait quoi).
		Les propriétaires considèrent que les bénéfices attendus sont raisonnables et réalistes.
1.7	Calendrier	Un délai est fixé pour la réalisation des bénéfices.
		Le délai paraît raisonnable.
		Déterminer s'il est possible d'accélérer la réalisation des bénéfices.
2 — Planification et façon d'aborder le projet		
2.1	Objectif et périmètre du projet	Le périmètre du projet est clairement défini et suffisamment détaillé.
		Une charte de projet a été élaborée, actualisée et diffusée.
		Le périmètre du projet est compris de la même façon par les responsables de l'entreprise et par l'équipe du projet.
		Une procédure a été établie d'un commun accord pour toute modification du périmètre défini au démarrage du projet.
2.2	Estimations, calendrier et périmètre	Les estimations actuelles sont clairement communiquées à l'équipe projet, au sponsor, au comité de pilotage et au bureau du projet.
		Déterminer si les estimations ont évolué au fil du temps et pourquoi.
		Le projet a été réévalué à partir des mises à jour de l'analyse de rentabilité.
2.3	Organisation	Chaque rôle est défini dans le cadre du projet.
		L'organisation du projet est définie.

Analyse de rentabilité et alignement		
Domaine		**Critères**
2.3 (Suite)	Organisation	Chaque personne impliquée dans le projet connaît et comprend son rôle.
		Déterminer s'il existe des mesures d'incitation associées à la réussite du projet et quel est leur impact.
2.4	Livrables	Le contenu et la structure des livrables des différentes étapes sont documentés.
		L'objectif des livrables est clairement compris et documenté.
		Tous les signataires du projet savent que les livrables requis doivent être approuvés.
		Le format des livrables a été étudié et établi avec les signataires.
		Des spécialistes ont examiné les principaux livrables.
2.5	Dépendances	Les tâches extérieures au projet sont clairement documentées et compri-ses. Des plans concernant ces tâches ont été développés et acceptés.
		Des points de contrôle sont définis à l'avance, avec les éléments à produire.
		Les hypothèses de planification sont comprises, documentées et acceptées.
2.6	Calendrier et activités	Il existe un plan de projet global reliant tous les plans des sous-projets.
		Chaque branche du projet est associée à un plan détaillé où sont définis des jalons clairs. Vérifier si cela ne s'applique qu'aux éléments critiques.
		Chaque domaine offre une vision claire du résultat final et des conditions nécessaires pour l'atteindre.
		Les principales tâches ont été identifiées et les relations entre ces tâches sont docu-mentées.
		Chaque tâche a une cible et un propriétaire clairement définis.
		Toutes les dépendances entre projets et avec l'extérieur ont été identifiées ; les dates d'échéance et les propriétaires sont bien définis.
		Il existe un projet pilote ou accéléré permettant de valider la méthodologie, les livra-bles, l'environnement, etc.
		L'exécution du projet pilote est courte, précise et représentative.
		Les plans ont été acceptés par les propriétaires des tâches.
		Les jours/ semaines de travail planifiés tiennent compte des périodes de congé/ formation.

Analyse de rentabilité et alignement		
Domaine		**Critères**
2.6 (suite)	Calendrier et activités	Le plan tient compte des courbes d'apprentissage/ transferts de connaissances.
		Le plan tient compte des imprévus entre chaque tâche principale et à la fin de chaque étape.
		Le plan prévoit suffisamment de temps pour les tâches préliminaires (environnement, normes, procédures, etc.).
		Le plan prévoit suffisamment de temps pour les examens et l'approbation.
3 — Communication et coordination du projet		
3.1	Communication et gestion du changement	Tout le monde connaît les raisons du projet ainsi que le calendrier des opérations.
		Chacun sait en quoi il ou elle sera concerné(e).
3.2	Organisation	Chaque rôle est défini dans l'organisation du projet.
		Chacun connaît sa place dans l'ensemble du processus.
3.3	Dépendances	Toutes les dépendances entre les services et vis-à-vis de l'extérieur ont été identifiées.
		La direction générale dégage les ressources nécessaires pour travailler sur le projet.
		La direction générale accepte d'interrompre d'autres projets/ catégories de travaux s'ils interfèrent.
3.4	Programmes partagés	Le projet a des sponsors ou des représentants dans chaque domaine concerné.
3.5	État d'avancement	Déterminer l'état d'avancement actuel du projet en termes de calendrier, de coût et de périmètre, et identifier les écarts éventuels par rapport à la définition initiale du projet.
		Identifier les principaux problèmes relatifs à l'avancement du projet.
		Comprendre les raisons des écarts éventuels.
		Déterminer si, avant de se produire, les raisons des écarts avaient été identifiées comme des risques.
		Des mesures correctives ont été prises pour traiter les écarts, les risques et les problèmes.
3.6	Programme de travail	Le programme de travail a été régulièrement mis à jour.
		Les estimations sont exactes et les principaux jalons ont été respectés.

Analyse de rentabilité et alignement		
Domaine		**Critères**
3.6 (suite)	Programme de travail	Les principales tâches à réaliser sont recensées, et le chemin critique ou la liste des conditions indispensables à la mise en service ont été identifiés.
		Un plan a été élaboré pour gérer les dépassements éventuels.
3.7	Gestion du risque	Une évaluation des risques a été réalisée, documentée et diffusée.
		Elle comprend des mesures d'atténuation des risques/plans d'urgence et identifie les personnes qui en ont la charge.
		Les risques sont compris par l'entreprise.
		Les risques et les mesures permettant de les atténuer sont gérés de façon proactive.
		Les risques sont régulièrement examinés avec les responsables des directions métiers.
		La personne chargée de résoudre les problèmes est clairement identifiée.
3.8	Dépendances par rapport à d'autres projets/ domaines	Le plan intègre un dispositif de coordination des changements résultant d'autres projets au niveau des métiers/ des systèmes.
		Des accords de niveau de service ont été établis pour l'assistance.

Solution SI et gestion de changement		
Domaine		**Critères**
4 — Conception des processus		
4.1	Périmètre pour l'entreprise	Le périmètre (en termes d'unités d'affaires, sites et de règles) est défini et validé.
4.2	Conception des processus et des éléments auxiliaires	Le plan intègre un dispositif de coordination des changements résultant d'autres projets au niveau des métiers/ des systèmes.
		Les scénarios sont documentés, testés avec succès, et approuvés par les responsables des directions métiers.
5 — Configuration et développement		
5.1	Traduction	Tous les écrans et leur adaptation sont documentés.
5.2	Configuration	L'exhaustivité de la configuration des tables stratégiques est vérifiée et entièrement documentée.
5.3	Programmes	La conception fonctionnelle est complète, actualisée et acceptée par les responsables des directions métiers.
		La conception technique est complète et conforme aux spécifications, les essais unitaires ont été concluants et les tests de réception sont réalisés par l'équipe projet.
		Des programmes spécifiques sont développés conformément aux normes en vigueur.
		Les programmes spécifiques font l'objet d'essais unitaires.
		Les programmes sont transférés vers la plateforme ou l'environnement de production.
5.4	Interfaces	La conception fonctionnelle des interfaces est complète, actualisée et acceptée.
		La conception technique des interfaces est complète et actualisée.
		Les rapports sont élaborés conformément à la conception, les tests unitaires sont concluants, et ils sont acceptés par l'équipe projet.
		Les interfaces sont testées de bout en bout sur la plateforme de production.
		Un processus de gestion des erreurs fonctionnelles est défini, développé et testé.
		Il ne reste aucun problème urgent ou important à régler au niveau des interfaces.
6 — Tests de réception par les utilisateurs		
6.1	Tests de réception par les utilisateurs	Tous les scenarii ont été réalisés avec succès et approuvés. Tous les tests de réception par les utilisateurs sont achevés et les scripts approuvés.

Solution SI et gestion de changement		
Domaine		**Critères**
6.1	Tests de réception par les utilisateurs	Les métiers sont suffisamment impliqués pour garantir la fiabilité des essais.
6.2	Liste de problèmes	Toutes les lacunes fonctionnelles relevées dans la liste des problèmes sont comblées et les solutions sont acceptées.
6.3	Calendrier de traitement par lots	Les calendriers de traitement quotidien, hebdomadaire, mensuel, trimestriel et annuel sont conçus et validés avec l'équipe du projet et les équipes techniques.
		En cas d'échec fonctionnel d'une tâche, la démarche à suivre est indiquée (passer la tâche, la relancer le lendemain ou se conformer au calendrier).
6.4	Problèmes non résolus à la mise en service	Les chefs d'équipe fonctionnel se sont mis d'accord avec les principaux responsables des directions métiers sur les problèmes à résoudre seulement après la mise en service. Si nécessaire, des solutions provisoires sont établies.
		Le cas échéant, des solutions provisoires ont été établies et communiquées aux équipes de formation et d'assistance.
7 — Conversion des données et mise en service		
7.1	Plan de conversion des données	Le plan de conversion des données est établi et la qualité des données converties est confirmée par des exercices et des essais de conversion. Les propriétaires de toutes les données converties sont identifiés.
		Les données converties correspondent bien aux données des systèmes hérités.
		La qualité des données converties lors des exercices est vérifiée par leur propriétaire.
		Les dépendances du plan de conversion et le chemin critique sont testés.
		Les profils requis pour le chargement manuel de données ou leur vérification sont disponibles et confèrent les accès nécessaires.
		Il ne reste aucun problème urgent ou important à régler au niveau de l'exercice.
7.2	Mise à jour parallèle des données	Les procédures relatives à toutes les données nécessitant une mise à jour parallèle sont consignées par écrit.
		Des vérifications sont prévues pour s'assurer que la mise à jour parallèle est correctement effectuée.
7.3	Chargement des données	Tous les chargements de données préalables à la mise en service sont effectués.
		Les données converties correspondent bien aux données des systèmes hérités.
		La qualité des données converties est vérifiée par leur propriétaire.

Solution SI et gestion de changement		
Domaine		**Critères**
7.3 (suite)	Chargement des données	Il ne reste aucun problème urgent ou important à traiter au niveau du chargement des données.
7.4	Plan de mise en service	Le plan de mise en service est élaboré et communiqué à tous les personnels concernés au niveau du projet et métiers.
		Le calendrier hérité de traitement par lots est prêt.
		Les profils d'accès hérités sont modifiés pour éviter que les utilisateurs n'utilisent par mégarde les anciens systèmes.
		Le calendrier des réunions de validation de l'état de fonctionnement et la liste des participants sont fixés d'un commun accord.
		Des plans de secours sont élaborés et acceptés.
7.5	Rapprochement	Les bilans financiers sont rapprochés des systèmes hérités. Les bilans sont chargés et peuvent être rapprochés des systèmes hérités.
		Des procédures ont été établies pour justifier ou corriger les écarts.
8 — Infrastructure technique		
8.1	Interface utilisateur	L'emplacement de tous les utilisateurs est recensé.
		L'interface utilisateur a été installée et vérifiée sur chacun des ordinateurs.
		Les procédures d'ouverture de session sont vérifiées.
		Toutes les procédures de mise à jour sont documentées et communiquées.
8.2	Imprimantes	L'emplacement de toutes les imprimantes est identifié, et les imprimantes sont configurées et testées.
		Toutes les imprimantes sont configurées pour les différents systèmes.
		Toutes les imprimantes sont en mesure d'imprimer depuis les différents systèmes.
8.3	Sortie électronique	Tous les formats de télécopie et autres formats de sortie électronique sont validés et testés.
		Un test de production est réalisé sur la ligne de télécopie extérieure et sur les destinataires d'échange de données informatisé (EDI).
8.4	Ordonnancement des traitements	Les calendriers de traitement nocturnes et mensuels sont vérifiés.
		Toutes les destinations (serveur/ répertoire) des interfaces sont configurées de façon à pointer sur les systèmes de production.

Solution SI et gestion de changement		
Domaine		**Critères**
8.4 (suite)	Ordonnancement des traitements	Il ne reste aucun problème urgent ou important à régler.
8.5	Procédures de traitement des erreurs	Il existe des procédures permettant de vérifier que les erreurs sont tracées (traitements d'interface).
		Les procédures de redémarrage après interruption d'un traitement sont établies et testées.
		Les procédures de communication des erreurs aux métiers ont été établies.
8.6	Liaisons de communications	Toutes les liaisons de communications (LAN, WAN, etc.) sont testées.
		La bande passante accepte les volumes maximum de données.
		Des procédures de secours sont établies et testées.
8.7	Dimensionnement du système	Tous les éléments d'infrastructure qui forment l'architecture technique globale sont dimensionnés et réglés de façon à pouvoir gérer les pointes d'activité et les taux de croissance prévus.
		Le matériel, les logiciels et les applications sont réglés pour la mise en service.
8.8	Tests de fonctionnement	Des tests de fonctionnement ont été réalisés et la performance des principaux processus est acceptable.
8.9	Fonctionnement du système	Des procédures de surveillance et de réglage sont en place pour le fonctionnement après mise en service, le fonctionnement en ligne et les traitements par lots.
8.10	Plan de secours	Des procédures ont été établies en cas d'interruption, et un plan de secours est défini.
		Les procédures ont été testées avec succès.
8.11	Disponibilité des systèmes en ligne et plages de maintenance	La disponibilité des systèmes en ligne et les plages de maintenance sont fixées avec les responsables de l'entreprise.
8.12	Profils de sécurité	Les profils de sécurité du personnel d'assistance SI sont définis et mis en œuvre.
		L'environnement de production est sécurisé.
8.13	Interfaces	La configuration technique des interfaces est achevée et testée.

Préparation des directions métiers et des utilisateurs		
Domaine		**Critères**
9 — Simulation		
9.1	Préparation	Tous les scénarios métiers sont consignés par écrit (à partir des tests de réception par les utilisateurs).
		L'environnement technique est prêt.
		Toutes les données requises sont converties dans l'environnement de simulation.
		Les utilisateurs et les profils sont prêts.
9.2	Achèvement	Tous les scénarios comportant des problèmes « urgents » ou « importants » sont exécutés avec succès.
		Les directions métiers sont suffisamment impliquées pour garantir la fiabilité des essais.
10 — Mise à jour des données après mise en service		
10.1	Utilisateurs propriétaires	Les types de données sont inventoriés et les propriétaires définis.
		Les personnes chargées de la mise à jour sont désignées et formées.
10.2	Mise à jour des données	Il existe des procédures pour chaque type d'ajout/ de mise à jour.
		Les procédures couvrent également la mise à jour de toutes les tables de conversion de code.
		Les procédures ont été communiquées à tous les utilisateurs concernés.
11 — Rôles et profils		
11.1	Profils d'utilisateur	La conception des profils est fixée par l'équipe du projet et par les représentants des métiers.
		Les profils ont été développés et testés avec succès.
		Il ne reste aucun problème urgent ou important à régler au niveau des profils.
11.2	Risques	Les risques majeurs sont identifiés et pris en charge par certaines fonctionnalités du système ou certaines procédures.
		Il ne reste aucun problème important à régler.
11.3	Accès au système	Tous les profils sont développés et testés pour les environnements de production notamment.
		Les responsables métier approuvent les accès accordés aux utilisateurs.

Préparation des directions métiers et des utilisateurs		
Domaine		**Critères**
11.3 (suite)	Accès au système	Les responsables métier contrôlent l'approbation de la séparation des fonctions..
		Tous les profils d'utilisateur sont définis, y compris pour les rôles de conversion et d'assistance.
11.4	Mise à jour des profils	Les procédures de mise à jour des profils après mise en service sont développées, approuvées et diffusées auprès du personnel concerné.
12— Préparation et formation des utilisateurs		
12.1	Impact sur les utilisateurs	Tous les utilisateurs comprennent les répercussions de la solution sur leur travail.
		Tous les utilisateurs concernés ont reçu des informations sur l'évolution de leur travail.
12.2	Formation et compétences des utilisateurs	Tous les utilisateurs concernés ont bénéficié d'une formation.
		Les exercices réalisés par les stagiaires dans le cadre de leur formation montrent qu'ils sont capables d'utiliser la solution.
		Un accompagnement et une assistance supplémentaires sont prévus pour ces utilisateurs après la mise en service.
12.3	Erreurs d'interface	Les utilisateurs chargés de corriger les erreurs d'interface ont été identifiés et ont reçu une formation sur les procédures applicables.
12.4	Outils d'assistance	Les utilisateurs ont accès aux outils d'assistance.
12.5	Nouveaux codes et nouvelle présentation des formulaires	Les clients/fournisseurs sont informés des changements au niveau des codes, de la présentation des formulaires, etc.
		Mise en place – Transition – l'après projet

Mise en place – Transition – Après projet		
Domaine		**Critères**
13 — Affectation des ressources et rôles clés		
13.1	Compétences exigées et assurées	Les compétences requises sont comprises, documentées et mises à jour.
		Les personnes affectées au projet offrent les compétences requises.
		Le projet entre en concurrence avec d'autres projets/initiatives sur des compétences/ ressources critiques. Si c'est le cas, identifier les répercussions.
		Il existe un programme de formation permettant d'acquérir les compétences manquantes.
13.2	Localisation des compétences	Les principales ressources ont été localisées sur le site du projet et/ou les membres de l'équipe projet sont tous réunis au même endroit.
13.3	Répartition des ressources	Des ressources à plein temps en nombre suffisant ont été affectées au projet.
		La répartition est claire entre les ressources internes et externes. Si l'assistance externe est importante, le processus de transfert des connaissances est clairement défini.
		Des accords ont été établis pour les ressources externes (par ex., paiement des pièces et main-d'œuvre, ou rémunération en fonction des bénéfices réalisés).
13.4	Recrutement pour les rôles clés	Quel que soit le domaine, la dotation en personnel est-elle suffisamment prioritaire, ou bien le personnel qualifié est-il concentré dans un domaine clé ?
		Les ressources les plus expertes sont placées à des postes où elles pourront contribuer au mieux au projet.
		Les rôles suivants sont remplis par des personnes possédant les compétences nécessaires : architecte technique, architecte de données, architecte métier, architecte fonctionnel et architecte de la conversion/ migration.
14 — Mise en place dans les directions métiers		
14.1	Rôle des directions métiers	Le métier connaît son rôle dans chaque étape du projet et est prêt pour la mise en œuvre.
		Chaque métier dispose d'une ressource dédiée qui collabore au projet.
		Le processus décisionnel est clairement défini.
		Le métier connaît son rôle dans le processus décisionnel.
14.2	Plans et ressources	Il existe des plans et des ressources pour la formation, le déploiement, le suivi et l'approbation.

Mise en place – Transition – Après projet		
Domaine		**Critères**
15 — Mise en production et maintenance SI		
15.1	Production SI	Il existe un plan de transfert des connaissances.
		L'équipe de production a approuvé le plan de déploiement.
		Il existe des plans pour garantir la capacité.
15.2	Maintenance SI	Il existe un plan de transfert des connaissances.
		L'équipe de maintenance a approuvé le plan de déploiement.
		Il existe des plans pour garantir la capacité.
15.3	Mise en place	Les dates de conversion ont changé. Si c'est le cas, pourquoi ?
16 — Transition vers la phase d'assistance		
16.1	Stratégie d'assistance	La stratégie globale d'assistance est fixée.
		Les intervenants pour le support de premier niveau sont identifiés et ont reçu une formation sur les outils requis.
		Les intervenants pour le support de second niveau sont identifiés et ont reçu une formation sur les outils requis.
16.2	Demandes de modification et procédures de correction	Le processus d'évaluation et de mise en œuvre des demandes de modification est établi et communiqué (par ex., analyse d'impact, financement).
		Le processus d'application des correctifs et des demandes de modification est établi et communiqué.
16.3	Processus d'assistance et contacts	Les numéros d'assistance et les informations à enregistrer si un problème est détecté ont été communiqués aux utilisateurs.
		Les métiers savent qui contacter pour l'assistance sur site.
16.4	Utilisation du système, mesures de contrôle et réunions de bilan	Les instruments de mesure de l'utilisation du système (permettant de vérifier que le système est utilisé et qu'il fonctionne) sont définis et acceptés. Des procédures sont établies pour recueillir et consigner les informations.
		Après la mise en service, des réunions d'examen quotidiennes sont organisées.

Mise en place – Transition – Après projet		
Domaine		**Critères**
17 — Plans de continuité d'activité		
17.1	Production SI	En cas d'interruption du système, des plans de continuité d'activité sont élaborés en concertation avec l'équipe projet et les directions métiers.
		Des plans de secours sont établis, ils indiquent les procédures à suivre lorsque le système redevient disponible pour éviter que certains éléments ne soient traités deux fois et s'assurer que les données financières sont bien mises à jour.
		Des formulaires manuels ou d'autres systèmes de soutien au plan de secours sont établis.
		Le processus de déclenchement des plans de secours (qui prend la décision et qui communique) est défini et accepté.

À propos des auteurs

Steve Stein, CIA, PMP, CISA, CISSP, CFE, CGE IT

Steve Stein est responsable groupe de l'audit SI pour le service d'audit interne de Hewlett-Packard. Il est chargé de la planification stratégique et de la gestion du service d'audit SI pour le monde entier. Steve Stein a 20 ans d'expérience dans la gestion de projets SI, le conseil et l'audit pour différents secteurs, notamment l'administration américaine, les hautes technologies et l'industrie pharmaceutique. Il possède une grande expérience de la mise en œuvre et de l'audit d'applications SAP R/3 pour des multinationales et de l'évaluation de la valeur acquise des systèmes de gestion de projet. Steve Stein a été directeur du groupe de gestion des risques liés aux SI de KPMG. En 2004, il a reçu le William S. Smith Certificate of Honor de l'IIA, qui récompense l'examen de certification des auditeurs internes (CIA). Il a été capitaine dans l'U.S. Air Force et est diplômé de l'U.S. Air Force Academy, où il a étudié l'ingénierie et les sciences.

Karine Wegrzynowicz, CIA, CISA

Karine Wegrzynowicz est directrice de l'audit interne au sein du groupe Lafarge, leader mondial des matériaux de construction basé à Paris. Elle est notamment chargée de superviser les audits SI et les audits d'autres fonctions opérationnelles au niveau mondial. Karine Wegrzynowicz a une expérience de plus de 20 ans dans l'audit interne, les SI et les opérations dans différents secteurs (transport aérien, automobile et services financiers). Elle a collaboré avec l'IIA (Institute of Internal Auditors) et l'ISACA (Information Systems Audit and Control Association) au niveau local et international, et est actuellement membre de l'Advanced Technology Committee de l'IIA.

Réviseurs

L'IIA tient à remercier les personnes et organisations suivantes pour leurs précieux commentaires et leurs apports à cet ouvrage :

- Professional Practices Advisory Council :
  - Advanced Technology Committee.
  - Board of Regents.
  - Committee on Quality.
  - Internal Auditing Standards Board.
  - Professional Issues Committee.
  - Ethics Committee.
- IFACI (Unité de recherche informatique), France ;
- The IIA Norway (NIRF) IT Audit Speciality Group (IT nettverket) ;
- The Institute of Internal Auditors – Royaume-Uni et Irlande ;
- Ken Askelson, États-Unis ;
- Clyde Batten, Nedbank Group Limited, Afrique du Sud ;
- Lily Bi, The Institute of Internal Auditors, États-Unis
- Anders Blix, EDB Business Partner, Norvège ;
- Lionel Guillou, Euroclear, Belgique ;
- F. M. Hallinan, Chevron Phillips Chemical Co. LLP, États-Unis ;
- David Lione, Consultant, États-Unis ;
- Michael Lynn, AXA Technology Services, États-Unis
- Steve Mar, Resources Global Professionals, États-Unis ;
- Tom Margosian, Ford Motor Co., États-Unis ;
- Kurt Milne, IT Process Institute, États-Unis ;
- Dr. Ulrich Hahn, auditeur indépendant, Allemagne
- Jacques Lourens, Nedbank Group Limited, Afrique du Sud ;
- Cesar Martinez, City of El Paso, États-Unis ;
- Steve Hunt, Crowe Horwath LLP, États-Unis ;
- James Reinhard, Simon Property Group Inc., États-Unis ;
- Joe Zhou Xiaowei, General Motors, Chine.

L'IFACI tient à remercier pour leurs précieux commentaires à la traduction de cet ouvrage :

- Eric RICHARD, Auditeur Informatique, Crédit Logement ;
- Philippe HERVIAS, Responsable Audit Sécurité & Infrastructure Informatique, Sanofi-Aventis.

Ce guide propose aussi une liste de questions utiles lors de l'examen d'un projet SI.

Votre avis nous intéresse ! Pour attribuer une note à ce guide ou formuler des commentaires, veuillez vous rendre sur :

www.theiia.org/guidance/technology/gtag12