GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Contrôles de la gestion du changement et des patchs : Un facteur clé de la réussite pour toute organisation

2ème édition

The Institute of Internal Auditors

Mars 2012

Copyright © 2012 par l'Institute of Internal Auditors, 247 Maitland Ave., Altamonte Springs, Floride, 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 autorisation écrite préalable de 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.

Contenu

Résumé 4

1. Introduction 5

2. Pourquoi se préoccuper de la manière dont son organisation gère les changements ? 11

3. Définir la gestion des changements informatiques 15

4. Quelles questions dois-je poser à propos de la gestion des changements et des patchs ? 26

5. Par quoi les auditeurs internes doivent-ils commencer ? 31

Annexe A : Exemple d'étude de cas pour la gestion des changements 35

Annexe B : Exemple de programme d'audit 37

A propos du CRIPP 40

Résumé

Chaque risque informatique induit un certain niveau de risque opérationnel. C'est pourquoi les responsables d'audit interne (RAI) doivent posséder une connaissance approfondie des problèmes liés à la gestion des changements et des patchs dans les systèmes d'information (SI).

La gestion des changements et des patchs dans les SI peut se définir comme l'ensemble des processus exécutés au sein du département informatique dans le but de gérer les évolutions, les mises à jour, les correctifs incrémentaux, et les patchs appliqués aux systèmes de production, ce qui comprend :

- La maintenance du code applicatif.
- Les montées en version de systèmes (par exemple les applications, les systèmes d'exploitation, et les bases de données).
- Les changements dans l'infrastructure (par exemple les serveurs, le câblage, les routeurs et les pare-feux).

Pour obtenir un environnement informatique productif stable et bien géré, il est nécessaire que la mise en œuvre des changements soit prévisible et reproductible et qu'elle respecte un processus maîtrisé, c'est-à-dire défini, piloté et effectivement appliqué. La séparation des fonctions (par exemple, la séparation des tâches de préparation, de test, d'exécution et d'approbation) et des contrôles réguliers atténueront le risque de fraude et d'erreur dans le processus.

Les auditeurs internes devraient connaître les éléments fondamentaux concourant à la maîtrise du processus de gestion des changements informatiques, à savoir notamment que :

- Seuls les collaborateurs chargés de mettre en œuvre les changements dans les systèmes d'information devraient avoir accès à l'environnement de production ; leur nombre devrait être réduit au minimum (mesure de prévention).
- les processus d'autorisation devraient associer les parties prenantes concernées afin qu'elles évaluent les risques générés par les changements envisagés et définissent les mesures pour les réduire (mesure de prévention).
- Les processus de supervision devraient inciter le management et le personnel informatiques à prendre pleinement conscience de la responsabilité de leurs tâches (mesure de prévention) et à détecter des performances insatisfaisantes (mesure de détection).

Ce guide pratique d'audit des technologies de l'information (GTAG) est conçu pour aider les auditeurs internes à poser les bonnes questions à la DSI afin d'évaluer la capacité de cette direction à gérer les changements, d'évaluer le niveau de risque global du processus et de déterminer si un examen plus détaillé du processus est nécessaire.

Ce guide permettra aux auditeurs internes :

- D'acquérir une connaissance opérationnelle des processus de gestion des changements informatiques.
- De distinguer rapidement les processus efficaces de gestion des changements de ceux qui ne le sont pas.
- De reconnaître rapidement les indicateurs et signaux d'alerte signalant une défaillance des contrôles liés à la gestion des changements dans les environnements informatiques.
- De prendre conscience que l'efficacité de la gestion des changements repose sur la mise en place de contrôles préventifs, détectifs et correctifs qui assurent la séparation des fonctions et la supervision appropriée du management.
- De recommander les meilleures pratiques connues pour remédier aux défaillances, afin de vérifier que les risques sont maîtrisés (et que les contrôles sont bien effectués) et d'accroître l'efficacité et l'efficience.
- De faire passer plus efficacement les recommandations auprès du directeur des systèmes d'information, du directeur général et/ou du directeur financier.

1. Introduction

Ce guide présente la gestion des changements et des patchs informatiques comme un outil de gestion et aborde les questions suivantes :

- Pourquoi la gestion des changements et des patchs informatiques est-elle importante ?
- Comment la gestion des changements et des patchs informatiques permet-elle de mieux contrôler les coûts et les risques liés aux SI ?
- Comment des indicateurs peuvent identifier ce qui fonctionne et ce qui ne fonctionne pas dans le processus de changement ?
- Comment juger du succès ou de l'échec de la gestion des changements et des patchs informatiques ?
- Comment réduire les risques associés aux changements informatiques ?
- Les responsabilités de l'audit interne.

Dans ce GTAG, le terme « Conseil » est utilisé au sens du glossaire des Normes : « Le niveau le plus élevé des organes de gouvernance, responsable du pilotage, et/ou de la surveillance des activités et de la gestion de l'organisation. Habituellement, le Conseil (par exemple, un conseil d'administration, un conseil de surveillance ou un organe délibérant) comprend des administrateurs indépendants. Si une telle instance n'existe pas, le terme « Conseil », utilisé dans les Normes, peut désigner le dirigeant de l'organisation.
Le terme « Conseil » peut renvoyer au comité d'audit auquel l'organe de gouvernance a délégué certaines fonctions ».

1.1 Pourquoi la gestion des changements et des patchs informatiques est-elle importante ?

Des études récentes ont démontré qu'une mauvaise gestion des patchs et des changements informatiques entraînait une augmentation des coûts et des périodes d'indisponibilité du service. Au fil du temps, les activités informatiques dans diverses organisations ont vu des changements occasionner des interruptions majeures et prolongées. Mais par où commencer pour évaluer les coûts liés à des problèmes d'une telle ampleur ?

On peut considérer que les organisations bénéficiant d'une meilleure gestion des changements et des patchs informatiques :

- consacrent moins de temps et d'énergie dans les SI pour des interventions non programmées,
- consacrent davantage d'argent et d'énergie dans les SI pour exécuter de nouvelles tâches et atteindre les objectifs de l'entreprise,
- connaissent moins de périodes d'indisponibilité,
- installent des patchs avec un minimum de perturbations,
- sont plus focalisées sur les améliorations que sur les réparations en urgence.

Si les organisations ont besoin de mesures incitatives supplémentaires, il existe dans plusieurs pays des lois qui requièrent que la direction générale comprenne et avalise les contrôles portant sur le reporting financier, y compris les contrôles informatiques. Sans une gestion efficace des changements informatiques, on voit mal comment le management pourrait répondre aux exigences de la loi et certifier l'intégrité de l'information financière.

1.2 Comment la gestion des changements et des patchs informatiques permet-elle de mieux contrôler les coûts et les risques liés aux SI ?

Chaque risque lié aux SI peut être amplifié par une mauvaise gestion des changements informatiques. À l'inverse, les risques peuvent être contrôlés à l'aide de processus de gestion des changements et des patchs informatiques appropriés et bien conçus. De manière peut-être moins évidente, une gestion appropriée des changements et des patchs

informatiques peut contribuer à réduire les coûts.

Faute des contrôles et de la visibilité appropriés, une organisation risque de consacrer des financements et des efforts à des changements inutiles ou non prioritaires, tout en négligeant des initiatives plus importantes. Des changements mal conçus ou mal évalués sont susceptibles de créer des problèmes qu'il faudra résoudre a posteriori, ou d'entraîner un « retrait » de changements. Des changements informatiques apportés à une seule composante peuvent perturber l'exploitation d'autres composantes. Ces perturbations sont coûteuses en temps et en argent, mais elles peuvent être atténuées grâce à des processus appropriés de gestion des changements et des patchs informatiques.

Au terme du processus, plusieurs facteurs liés à une gestion des changements informatiques inefficiente ou inefficace peuvent pénaliser une organisation de différentes manières :

- Départ de personnel informatique très qualifié, en raison de la frustration suscitée par une qualité médiocre des résultats.
- Systèmes de mauvaise qualité, qui rendent le personnel inefficient et inefficace ou qui provoquent le mécontentement des clients.
- Occasions manquées pour proposer aux clients des produits et services innovants ou plus efficients.

Des processus de gestion des changements informatiques bien conçus et installés avec rigueur peuvent produire les effets inverses. Il est possible de concentrer les efforts informatiques sur les priorités du métier l'entreprise. Le nombre de dépannages en urgence peut être réduit au minimum. On peut s'efforcer de retenir le personnel informatique et de le motiver pour qu'il excelle. Il est possible d'équiper le personnel d'outils qui accroîtront sa productivité. Enfin, les clients peuvent être satisfaits par des systèmes qui répondent à leurs besoins.

1.3 Qu'est-ce qui fonctionne et qu'est-ce qui ne fonctionne pas ?

Pour que la gestion des changements informatiques soit efficace, elle doit procurer à la direction de l'organisation de la visibilité sur les problèmes suivants :

- ce qui a été changé, pourquoi et quand ;
- l'efficience et l'efficacité de l'installation des changements ;
- les problèmes qui sont causés par les changements et leur degré de gravité ;
- le coût des changements ;
- les effets positifs des changements.

Une telle visibilité est possible à travers des mesures et des indicateurs examinés de manière régulière et objective. Ils constituent les compteurs du tableau de bord, nécessaires pour assurer une bonne visibilité au management.
Les changements informatiques sont l'accélérateur, le frein et le volant (et la marche arrière pour le retour à une configuration antérieure) qui permettent de contrôler les SI et ce, par différents moyens :

- une implication précoce et régulière du management et des utilisateurs finaux afin d'adapter les changements informatiques aux besoins de l'entreprise ;
- un processus défini, prévisible et reproductible, avec des résultats définis, prévisibles et reproductibles ;
- la coordination et la communication avec les intervenants affectés par les changements.

1.4 Comment juger du succès ou de l'échec de la gestion des changements et des patchs informatiques ?

Le management, y compris le management informatique, peut se faire une bonne idée du succès ou de l'échec de la gestion des changements et des patchs en étudiant les réponses données aux questions simples qui suivent :

- Le processus de gestion des changements est-il efficace ? La réponse nie-t-elle l'importance des changements informatiques ou la reconnaît-elle en soulignant les progrès en cours ?
- Quels sont les contrôles en place dans le cadre de notre processus de gestion des changements ? Des contrôles sont-ils en place et en cours d'amélioration ou sont-ils simplement évalués et différés jusqu'à ce que les dépannages en urgence se raréfient ?
- Avons-nous observé des bénéfices liés au processus de gestion des changements ? Existe-t-il des bénéfices mesurables ou l'accent est-il mis sur les coûts induits par le processus de gestion des changements informatiques ?
- Qu'en est-il de l'interruption de service due à un changement et qui a touché l'ensemble du site la semaine dernière ? Que s'est-il passé ? À quel point le management est-il informé sur les causes des interruptions de service ? Quel est le niveau de contrôle du management sur la récurrence du problème ?
- Quel processus a été utilisé pour déterminer la cause de l'interruption de service ? S'agit-il d'une démarche improvisée ou méthodique ? Le diagnostic du problème a-t-il permis de déterminer rapidement si c'est un changement qui a provoqué l'interruption de service ? Si oui, quel changement est à l'origine du problème ?
- De quelle manière l'informatique contribue-t-elle au suivi du bon fonctionnement du processus ? Les mesures et les indicateurs sont-ils objectifs et vraiment révélateurs ou sont-ils subjectifs et sujets à caution ?
- Quel est l'objectif de notre processus de gestion des changements ? Est-il axé sur la fiabilité, la disponibilité et l'efficience ou sur d'autres priorités, moins cruciales ? Est-il tout simplement axé sur une priorité ?
- À quel point notre processus de gestion des patchs est-il perturbateur ? La gestion des patchs est-elle intégrée dans un processus de changement et de mise en production défini et reproductible, ou s'inscrit-elle dans une démarche improvisée, informelle et reposant sur l'urgence ?

Les cinq principaux indicateurs d'une mauvaise gestion des changements :

- *Changements non autorisés (plus de zéro est un résultat inacceptable).*
- *Interruptions de service non programmées.*
- *Faible taux de réussite des changements.*
- *Nombre élevé de changements en urgence.*
- *Retards dans le déploiement des projets.*

Voici quelques symptômes et indicateurs de contrôles déficients aisément repérables, qui révèlent des changements informatiques mal maîtrisés :

- Indisponibilité de services ou de fonctions critiques, même pendant un bref laps de temps.
- Indisponibilité non programmée de réseaux ou de systèmes, induisant une interruption de l'exécution de processus critiques, tels que la coordination des plannings avec les fournisseurs ou le traitement des commandes des clients.
- Indisponibilité d'applications critiques, de bases de données ou de serveurs Internet, qui a pour effet d'empêcher les utilisateurs d'exécuter les tâches critiques qu'ils ont à accomplir.
- Publicité négative et interrogation non souhaitée de la part des organes dirigeants.

Au niveau organisationnel, voici quelques indicateurs révélant d'éventuels problèmes systémiques de maîtrise du processus de gestion des changements :

- La DSI consacre la majorité de son temps à l'exploitation et à la maintenance (> 70 %) plutôt qu'à contribuer au développement des activités.
- Des projets et des tâches programmées ne sont pas menés à terme (en raison du nombre élevé de dépannages en urgence et d'interventions non programmées).
- Interventions de nuit du management informatique pour résoudre des problèmes.
- Forte rotation du personnel informatique.
- Relations conflictuelles entre le personnel d'assistance, les développeurs et les clients (internes ou externes), généralement en raison

d'une qualité de service médiocre ou d'un retard dans la livraison d'une fonctionnalité.
- Le management informatique a besoin de beaucoup de temps pour répondre aux audits informatiques et pour mettre en œuvre les recommandations.

Les organisations qui améliorent leurs processus de gestion des changements et des patchs ont besoin de moins en moins d'administrateurs système. Quand la gestion des changements et des patchs dans les SI fonctionne bien, les informaticiens sont plus efficaces et productifs.
Des mesures plus formelles et plus rigoureuses peuvent et doivent être examinées afin d'assurer une visibilité maximale sur l'efficacité de la gestion des changements et des patchs informatiques, telles que :
- Le nombre de changements autorisés par semaine.
- Le nombre de changements installés par semaine.
- Le nombre de changements non autorisés qui contournent le processus de changement.
- Le taux de réussite des changements (pourcentage de changements effectifs qui n'ont pas donné lieu à une interruption de service, à une détérioration du service ou à une charge de travail non programmée).
- Le nombre de changements en urgence (y compris les patchs).
- Le pourcentage de patchs déployés au cours des mises en production programmées de versions de logiciels.
- Le pourcentage de temps consacré à des tâches non programmées.
- Le pourcentage de projets livrés en retard.

1.5 Comment réduire les risques liés aux changements informatiques ?

Ce guide présente les meilleures pratiques de gestion des changements qui permettent de réduire les risques opérationnels et d'accroître l'efficacité et l'efficience des SI. Afin d'améliorer leurs processus de gestion des changements, les organisations peuvent immédiatement appliquer cinq mesures essentielles :
- Faire preuve d'exemplarité *(tone at the top)*, en incitant à adopter une culture de la gestion des changements dans toute l'entreprise, en s'appuyant sur une déclaration du management des SI qui précise que le nombre acceptable de changements non autorisés ne peut être qu'égal à zéro. Des contrôles préventifs et détectifs peuvent ensuite être mis en place afin d'atteindre cet objectif, et de le maintenir durablement, en garantissant que tout changement dans la production peut être rapproché d'ordre de production autorisé.
- Surveiller en permanence le nombre d'interruptions de service non programmées, celui-ci étant un excellent indicateur des changements non autorisés et des défaillances dans la mise en œuvre des changements.
- Réduire le nombre de changements à risque en déterminant clairement et faisant respecter des périodes de gel et des plages de temps ouvertes à la maintenance. Cela a pour effet d'optimiser la stabilité et la productivité pendant les heures de production. Les interruptions de service non programmées constituent de bons indicateurs d'un contournement du processus.
- Utiliser le taux de réussite des changements comme un indicateur clé de la performance en matière de gestion des SI. Les changements non gérés, non pilotés et non contrôlés affichent généralement un taux de réussite inférieur à 70 %. Chaque changement ayant échoué est potentiellement à l'origine de périodes d'indisponibilité, de travail non planifié et réalisé en urgence, d'écarts par rapport aux programmes établis et de risques pour l'entreprise. Une hausse du taux de réussite des changements passe nécessairement par des contrôles préventifs, détectifs et correctifs.
- Utiliser le nombre de tâches non planifiées comme un indicateur de l'efficacité des processus de gestion et de contrôle des changements informatiques. Là où les organisations perfor-

mantes consacrent moins de 5 % de leur temps à des tâches non programmées (et urgentes), la plupart des organisations y consacrent, en moyenne, de 45 à 55 % de leur temps.

1.6 Ce que l'audit interne devrait faire

Ce GTAG traite de la gestion des risques qui constituent une préoccupation croissante des parties prenantes au processus de gouvernance. À l'instar de la sécurité informatique, la gestion des changements informatiques est un processus fondamental qui, s'il n'est pas exécuté correctement, peut nuire à l'entreprise dans son ensemble. C'est pourquoi cet aspect intéresse de nombreux comités d'audit et, par conséquent, la direction générale.

Ce guide propose des outils pour aider les auditeurs internes à obtenir des preuves attestant les affirmations du management informatique (performance, efficacité, efficience) et à en évaluer l'exactitude. Tout comme pour le processus d'audit financier[1], les auditeurs informatiques doivent obtenir des données d'autorisation sous-jacentes (par exemple, des rapports d'autorisation des changements) et des informations de recoupement (par exemple, des rapports de changements dans la production issus des contrôles détectifs, des rapprochements de changements dans la production et de changements autorisés, des interruptions de service, etc.). En agissant ainsi, les auditeurs internes sont en mesure d'émettre une opinion sur les affirmations du management informatique concernant ses processus de gestion des changements et sa capacité à atténuer les risques liés aux informations financières.

Les auditeurs internes peuvent aider le management et le Conseil en :

- appréhendant les objectifs de l'organisation en matière de confidentialité, d'intégrité et de disponibilité du traitement informatique.
- aidant à identifier les risques potentiellement induits par les changements et déterminer si ces derniers correspondent au goût pour le risque et à la tolérance au risque de l'organisation.
- aidant à définir un ensemble de mesures de gestion du risque appropriées.
- recherchant et en encourageant une culture de gestion des changements disciplinée, et en promouvant notamment les bienfaits d'une bonne gestion des changements.
- comprenant les contrôles qui sont cruciaux dans le cadre d'une approche solide de la gestion des changements informatiques.
  - Prévention
    - Autorisations appropriées.
    - Séparation des fonctions.
    - Supervision.
  - Détection
    - Détection des changements non autorisés.
    - Suivi des indicateurs valides et objectifs de la gestion des changements.
  - Correction
    - Revue après installation.
    - Intégration de l'information sur les changements lors des premières étapes du diagnostic des problèmes.
- se tenant informé des principaux processus actuels de gestion des patchs et des changements informatiques et établissant des recommandations en vue de leur adoption par l'organisation.
- démontrant comment le management peut tirer parti d'une meilleure gestion des risques, d'une plus grande efficacité et d'une réduction des coûts.
- aidant le management à identifier des approches pratiques et efficaces de la gestion des changements informatiques.

[1] *Overview of Auditing / O'Reilly et al. - in Montgomery's Auditing: 12e edition. – 1998.*

1.7 La gestion du changement selon les Normes et les lignes directrices de l'IIA

Les lignes directrices suivantes de l'*Institute of Internal Auditors* (IIA) décrivent les rôles et responsabilités des auditeurs internes afférents à la gestion du changement et des patchs au sein de l'organisation :

- Norme 2120 : Management des risques
- MPA 2120-1 : Evaluer la pertinence des processus de management des risques
- Norme 2130 : Contrôle
- MPA 2130-1 : Evaluer la pertinence des processus de contrôle
- MPA 2130.A1-1 : Fiabilité et intégrité de l'information

Les guides pratiques de l'IIA sont également disponibles :

- GTAG 1 : Les contrôles et le risque des systèmes d'information – 2nde édition
- GTAG 3 : Audit continu – répercussions sur l'assurance, le pilotage et l'évaluation des risques
- GTAG 9 : Gestion des identités et des accès
- GTAG 17 : Audit de la gouvernance des systèmes d'information
- Guide pratique : Auditer l'environnement de contrôle
- Guide pratique : Evaluer l'adéquation du management des risques

2. Pourquoi se préoccuper de la manière dont son organisation gère les changements ?

Les auditeurs internes et les professionnels des SI disposent de multiples recommandations au sujet de la gestion des changements et de leur contrôle appliqués à l'exploitation informatique. La publication de référence de l'*Institute of Internal Auditors, Systems Auditability and Control* (1977), a été réactualisée en 1994 et montre bien l'importance de ce sujet pour les managers et les auditeurs internes :

> *La gestion des changements et des problèmes est cruciale si l'on veut obtenir un fonctionnement stable, fiable et correctement maîtrisé. Elle implique un suivi des problèmes, des procédures d'escalade, un examen des problèmes et des changements par le management, une hiérarchisation des ressources, des mises en production maîtrisées et un contrôle des changements applicatifs.*

Cependant, ce n'est que depuis peu que l'on s'attache véritablement à comprendre de quelles pratiques informatiques et de quels environnements dépendent les résultats de l'entreprise. Ces efforts montrent une culture de gestion du changement effective qui fait l'une des différences fondamentales entre les organisations ayant un SI performant et sécurisé et les autres. En d'autres termes, la gestion des changements n'est pas seulement un dispositif de contrôle essentiel mais également une source potentielle de bénéfices pour l'entreprise.

2.1 Les changements sont source de risque : pourquoi faut-il considérer les patchs comme n'importe quel autre changement ?

Les auditeurs sont conscients de l'étroite relation qui existe entre changements et risques. Les actifs informatiques semblent être en constante évolution. Le management des SI doit donc traiter :

- Des changements réguliers (classiquement, les montées de version planifiées concernant les applications, le middleware, les systèmes d'exploitation ou les matériels et les logiciels réseau).
- Les patchs (changements visant à remédier à des codes défectueux ou à d'autres vulnérabilités décelées dans la production).
- Les changements à opérer en urgence pour résoudre des problèmes immédiats à l'origine d'interruptions du service.

Grâce à une gestion efficace des changements informatiques, l'organisation peut passer en toute sécurité d'un état connu et défini à un autre, quelle que soit la motivation du changement.

Les actifs informatiques sont plus faciles à gérer et à contrôler en l'absence de pression pour mettre en œuvre les changements. Ainsi, il peut être bon de définir des plages sans aucun changement : le niveau de service et la disponibilité sont alors à leur maximum, et le département informatique consacre l'essentiel de son temps à des tâches planifiées. Mais que se passe-t-il lorsque des vulnérabilités critiques sont mises en évidence et que des changements deviennent plus urgents ? Que se passe-t-il lorsque nombre de vos fournisseurs déploient régulièrement des patchs pour réparer des failles critiques ? Le nombre de patchs urgents à appliquer et l'absence de procédure ad hoc est un problème critique pour beaucoup d'entreprises.

Dans les organisations peu performantes, le déploiement des patchs se fait au cas par cas, de manière chaotique et urgente. Lorsqu'un patch est proposé pour remédier à une vulnérabilité de sécurité critique, il peut en résulter des perturbations et, souvent, le transfert d'un nombre important de ressources vers ces patchs non prévus, au détriment des tâches initialement planifiées. Pire encore, même le déploiement réussi d'un patch peut poser des problèmes inattendus, comme altérer le fonctionnement des serveurs et de ce fait empêcher la fourniture de services critiques.

Les organisations performantes sont plus enclines à traiter les nouveaux patchs comme des changements prévisibles et planifiés, soumis au processus normal de gestion des changements. Le patch est ajouté à la liste, il est évalué, testé et intégré aux déploiements déjà programmés. Le respect d'un processus bien défini pour l'intégration des changements aboutit à un taux de réussite du changement très supérieur. Il est intéressant de noter que nombre d'organisations performantes appliquent des patchs bien moins fréquemment que les autres, parfois jusqu'à dix voire cent fois moins souvent. Elles considèrent que le risque associé à des vulnérabilités est plus faible que le risque lié à la disponibilité, qui découle des répercussions non anticipées d'un mauvais changement ou d'un changement intervenant en dehors du cycle. A l'inverse, les organisations performantes qui choisissent de déployer un patch constituant un changement prioritaire sont à même de le faire de manière prévisible et reproductible en recourant à un processus efficace de gestion des changements.

Tout au long de ce GTAG, les patchs seront traités comme un type de changement qui relève du processus normal de gestion des changements. Il en découle deux grandes implications : la gestion des patchs est une fonction subordonnée à la gestion des changements, et souvent, un processus efficace de gestion des changements peut permettre de s'assurer que les technologies utilisées pour éviter le « *patch and pray* » (le fait d'appliquer rapidement les correctifs proposés par les différents éditeurs, en espérant qu'ils ne créeront pas d'incident de production ni d'altérations de fonctions) ne feront pas naître de nouveaux problèmes.

2.2 Nous disposons déjà d'un processus de gestion des changements ; en quoi celui-ci est-il différent ?

Pour que le management soit efficace, il faut avant tout que l'organisation ait mis en place un ensemble complet et bien défini de contrôles préventifs, détectifs et correctifs, et qu'elle ait clairement défini la séparation des fonctions. Les contrôles de gestion des changements permettent au management de répondre à de nouveaux besoins (projets de développement, réglementation…) sans avoir à augmenter les moyens. De manière générale, une gestion efficace des changements atténue les risques, réduit les coûts et procure des ressources pour des services additionnels.

À l'inverse, une gestion inefficace des changements constitue un risque considérable. Dans la plupart des organisations, la question n'est pas de savoir s'il existe un processus de gestion des changements mais bien si celui-ci est aussi efficace et efficient que possible, et s'il est utilisé pour l'ensemble des changements apportés aux SI. Lors du déploiement des changements urgents, il est extrêmement difficile de prévenir les erreurs, les irrégularités ainsi que les interruptions non programmées. Les ruptures dans la disponibilité des SI (source d'une médiocre qualité de service et d'une insatisfaction de la clientèle) poussent souvent les organisations à prendre en considération les contrôles et les processus de gestion des changements et à les mettre en œuvre. D'après les recherches, les départements informatiques performants sont constamment en quête de moyens dans le but d'améliorer leurs processus opérationnels, et notamment la gestion des changements. Par l'amélioration des contrôles et de la prévisibilité des changements appliqués aux systèmes et aux réseaux, votre département informatique peut espérer se classer parmi les meilleurs de sa catégorie. Les auditeurs internes sont très bien placés pour aider le management à améliorer ces processus et ces contrôles.

Si la direction des SI n'est pas en mesure de décrire tous les changements et leur niveau d'avancement, il ne peut pas non plus décrire ce qui est actuellement géré ni assurer que les changements se déroulent comme prévu.

S'il est facile d'en parler, la gestion des changements est l'une des disciplines les plus difficiles à

mettre en œuvre. Elle nécessite une collaboration entre une équipe pluridisciplinaire, composée de développeurs d'applications, du personnel d'exploitation informatique, des auditeurs et des membres du personnel chargés des services de bout en bout. Il importe de souligner que chaque groupe a un rôle spécifique à jouer et que ces rôles doivent être définis dans les procédures de gestion des changements.

Les auditeurs internes savent parfaitement établir un diagramme de circulation pour les processus de l'entreprise et évaluer les contrôles. Ils sont les mieux placés pour aider leurs organisations à percevoir les avantages qui découleraient d'une appréhension globale des processus clés.

La direction des SI doit être en mesure, à tout moment, de procéder à des évaluations de tous les changements et d'indiquer leur état d'avancement. La direction des SI devrait publier un calendrier des changements, qui recense aussi bien tous les changements approuvés que les dates de mise en œuvre planifiées. Des processus efficaces de gestion des changements procurent l'information et l'assurance nécessaires pour suivre tous les changements pendant les diverses phases de leur réalisation.

Enfin, l'amélioration de la gestion des changements apportés aux SI dans une organisation a pour objectifs de réduire le risque (qui découle essentiellement d'une incapacité à mener à bien les missions en raison de pannes), diminuer le volume des tâches non planifiées (ce qui libère des ressources déjà limitées) et améliorer la qualité du service pour tous les clients internes et externes.

2.3 Les avantages d'une procédure robuste de gestion des changements

Les demandes de changements découlent du souhait d'obtenir des avantages pour l'entreprise, par exemple une réduction des coûts ou une amélioration des services, ou de la nécessité de résoudre des problèmes. Le processus de gestion des changements vise à étayer et à améliorer le fonctionnement de l'organisation. Il s'agit de faire en sorte que soient utilisées des méthodes et procédures standardisées, qui permettront un traitement efficace et efficient de tous les changements et qui minimiseront l'effet des incidents liés aux changements sur la qualité et la disponibilité des services.

Si l'on veut protéger l'environnement de production, les changements doivent être gérés d'une manière reproductible, définie et prévisible. Il faut veiller à ce que les changements appliqués pour corriger une application, un serveur ou un dispositif réseau n'induisent pas de problème non prévu dans d'autres dispositifs ou applications. Ce point est particulièrement important pour les actifs informatiques (logiciels, matériel, données) qui soutiennent les processus métiers critiques de l'entreprise ou les gisements de données.

De solides processus de gestion des changements peuvent également aider l'organisation à rester conforme aux obligations réglementaires, sans cesse plus nombreuses. La gestion des risques et les étapes d'approbation, par les départements concernés, du processus de changement doivent inclure les activités qui traitent les répercussions potentielles des changements sur la conformité à la réglementation. Ainsi, aux États-Unis, lorsque l'on applique des changements à une technologie qui intervient dans le processus de communication financière, il faut faire attention à continuer de bien respecter la loi Sarbanes-Oxley. De même, en Europe, des changements apportés au traitement d'informations susceptibles de conduire à l'identification de personnes risquent d'enfreindre les directives européennes sur la protection des données à caractère personnel.

Des processus efficaces de gestion des changements doivent être formalisés, ce qui limite les efforts nécessaires pour repérer, valider et certifier les changements apportés au processus de communication financière afin d'assurer la conformité. La section 404 de la loi Sarbanes-Oxley impose au

management de donner son aval et d'évaluer les contrôles portant sur le processus de communication financière, en particulier sur les contrôles des SI. Des changements non contrôlés dans l'environnement de production risquent d'induire des erreurs qui, si elles se propagent ou sont critiques, pourraient être considérées comme des insuffisances significatives qu'il convient de signaler au comité d'audit de l'organisation. Aux États-Unis, les dysfonctionnements graves, ce que les experts comptables appellent des « déficiences importantes » doivent être portés par l'entreprise à la connaissance du grand public, par référencement auprès de la *Securities and Exchange Commission* (SEC). La divulgation de déficiences peut avoir un impact sur la réputation de l'organisation, son cours de Bourse et sa capacité à continuer d'opérer.

Normalement, les déficiences relevées dans le cadre de contrôles informatiques généraux, comme la gestion des changements, doivent être évalués en termes d'effets sur les contrôles applicatifs. Plus précisément, une déficience dans les contrôles généraux des SI est considérée comme une « déficience importante » ou une « faiblesse significative » si elle remplit au moins l'une des conditions suivantes[1] :

- Une lacune dans un contrôle applicatif, causée par, ou en relation avec, une déficience dans les contrôles généraux des SI est considérée comme une déficience importante.
- La propagation et l'importance d'une déficience dans les contrôles généraux des SI amènent à conclure qu'il existe une déficience importante dans l'environnement de contrôle de l'organisation.
- Une déficience dans les contrôles généraux des SI considérée comme importante n'est pas corrigée après un délai raisonnable.

Dans les années précédentes, de nombreuses organisations ont fait état de graves déficiences liées à la gestion des changements dans les contrôles généraux des SI qui portent sur une partie de leur environnement de communication financière. S'il s'avérait que cette déficience n'était pas corrigée sous un an, ces organisations étaient en danger. Les auditeurs internes peuvent aider le management en identifiant ces problèmes et en veillant à ce qu'ils soient résolus en temps utile.

Un modèle communément accepté pour l'évaluation du contrôle interne est *La Nouvelle Pratique du Contrôle Interne (Internal Control - Integrated Framework),* un référentiel édité par le Committee of Sponsoring Organizations of The Treadway Commission (COSO) en 1992. En 2004, ce modèle a été amélioré afin de proposer un cadre de référence largement accepté pour la gestion des risques de l'entreprise. Ce modèle présente des principes clés, des concepts, une terminologie commune relative aux risques et des recommandations claires pour la mise en œuvre. Cette nouvelle publication, intitulée *Le Management des risques de l'entreprise : Cadre de référence, Techniques d'application* [COSO, 2004], décrit quatre catégories d'objectifs pour l'organisation et huit composantes interdépendantes d'une gestion du risque efficace.

Les organisations performantes accueillent généralement bien les contrôles. En effet, un processus efficace de gestion des changements réduit le risque de mauvaises performances, ainsi que le nombre de problèmes soulevés par un expert-comptable extérieur, un organisme de réglementation ou une autorité de contrôle. En conséquence, le conseil d'administration de l'entreprise est davantage satisfait et l'on observe parallèlement un allègement de la pression pesant sur le management de la direction des SI. Enfin, les organisations qui considèrent la gestion des changements comme un catalyseur pour la conduite efficace des affaires enregistrent de meilleurs résultats. Le point essentiel à garder en mémoire est que la gestion des changements est centrée sur les processus avec un axe managérial et humain, et s'appuie sur des contrôles techniques et automatisés.

---

[1] *A Framework for Evaluating Control Exceptions and Deficiencies, version 3 / BDO Seidman LLP, et al.- 2003.*
[développé par les organisations suivantes : BDO Seidman LLP, Crowe Chizek and Company LLC, Deloitte & Touch LLP, Ernst & Young LLP, Grant Thornton LLP, Harbinger PLC, KPMG LLP, McGladrey & Pullen LLP, PricewaterhouseCoopers LLP]

3. Définir la gestion des changements informatiques

Dans la plupart des entreprises, le département informatique a essentiellement deux rôles : 1) faire fonctionner et maintenir les services existants et les engagements, et 2) fournir de nouveaux produits et/ou services pour aider l'entreprise à atteindre ses objectifs. Cette section décrit le champ de la gestion des changements venant étayer ces deux rôles, les caractéristiques respectives d'une gestion des changements efficace et inefficace, la fonction de l'audit dans la gestion des changements et les indicateurs qui peuvent contribuer à la gestion efficace des changements.

3.1 Quelle est la portée de la gestion des changements ?

Ce guide est axé sur la gestion des changements opérationnels dans les SI. Cette gestion commence dès lors que l'on a établi l'applicabilité des montées de version ou des mises à jour d'actifs informatiques (infrastructures, applications) au niveau de la production (via, par exemple, une équipe de développement d'applications ou une équipe de recherche et développement - R&D) et s'achève quand ces actifs sont retirés de l'environnement de production. Elle englobe donc la maintenance des applications et les contrôles des changements en urgence. Les changements qui interviennent au moment de la conception et du développement de logiciels en sont spécifiquement exclus.

Dans ce guide, le terme « gestion des changements » n'inclut pas le processus de gestion des configurations. ITIL (Information Technology Infrastructure Library) définit la gestion de configuration comme consistant à « identifier, vérifier toutes les versions des composantes informatiques (matériels, logiciels, documentation associée) et à en assurer la maintenance ». Cependant, le processus de gestion des changements doit interagir avec celui de la gestion des configurations (et les contrôles qui s'y rapportent) lorsque des changements sont apportés aux configurations.

Sources de changements

À peu près chaque décision dans l'entreprise appelle un changement dans les SI. Voici plusieurs facteurs qui constituent des sources de changements devant être traités et gérés efficacement dans l'environnement informatique :

- L'environnement externe (marché concurrentiel, parties prenantes / actionnaires, évolution des risques).
- L'environnement réglementaire.
- Les buts, objectifs, stratégies, besoins, processus et changements de priorités de l'entreprise.
- Les fournisseurs (nouveaux produits, nouvelles versions, patchs et vulnérabilités).
- Les partenaires et prestataires.
- Les résultats d'un audit, d'une évaluation des risques et d'autres types d'évaluations.
- Les problèmes opérationnels.
- Les variations dans les performances ou les capacités nécessaires.

Portée des changements

Un processus efficace de gestion des changements concerne la totalité des modifications apportées à n'importe quel actif informatique dont dépendent des services de l'entreprise. Parmi les actifs devant faire l'objet d'une gestion des changements, citons :

- Matériel : grands systèmes, serveurs, postes de travail, routeurs, commutateurs et appareils mobiles.
- Logiciel : systèmes d'exploitation et applications.
- Informations, données, structure des données : fichiers et bases de données.
- Contrôles de sécurité : logiciels anti-virus, pare-feux et systèmes détectifs des intrusions / systèmes anti-intrusion (IDS/IPS).
- Processus, politiques et procédures.
- Rôles / responsabilités : autorisation, pouvoir d'action et contrôles d'accès.

Processus de gestion des changements
Le processus de gestion des changements implique généralement :

- D'identifier la nécessité d'un changement.
- De préparer le changement :
  - Détailler par écrit la demande de changement.
  - Présenter par écrit le plan permettant de tester le changement.
  - Prévoir, par écrit, un plan de restauration, pour le cas où les changements ne réussiraient pas.
  - Rédiger une procédure, étape par étape, qui incorpore le changement, le plan de test et le plan de restauration.
  - Soumettre la procédure de changement sous la forme d'une demande de changement.
- D'élaborer une justification et d'obtenir les autorisations nécessaires :
  - Évaluer l'impact, le coût et les avantages associés au changement demandé.
  - Examiner et évaluer les risques et les répercussions associés au changement requis, y compris les implications du point de vue de la réglementation.
- De donner son aval à la demande de changement.
  - Autoriser, rejeter ou solliciter des informations supplémentaires sur la demande de changement.
  - Hiérarchiser la demande de changement par rapport aux autres requêtes en cours.
- De programmer, coordonner et mettre en œuvre le changement.
  - Planifier l'intervention de la personne chargée de déployer le changement et lui assigner la mission.
  - Planifier l'intervention de la personne chargée de tester le changement et lui assigner la mission.
  - Tester le changement dans un environnement de pré-production.
  - Informer du changement toutes les parties prenantes susceptibles d'être concernées.
  - Avaliser le changement en vue de sa mise en œuvre.
  - Mettre en œuvre le changement comme requis.
- De vérifier et d'examiner le changement mis en œuvre (étape critique, le plus souvent négligée).
  - Le changement a-t-il réussi ?
  - La procédure de changement a-t-elle été respectée ?
  - Quel écart observe-t-on entre le changement prévu et celui effectivement mis en œuvre ?
  - Les contrôles internes, les opérations et les impératifs de conformité à la réglementation ont-ils été préservés ?
  - Quels enseignements peut-on en tirer pour améliorer le processus ?
- De revenir à l'état initial si le changement ne réussit pas.
- De clôturer la demande de changement et de communiquer avec les parties concernées.
- D'apporter les changements dont il a été convenu à la procédure de gestion des changements.
- De publier le plan du changement.

Les auditeurs reconnaîtront immédiatement qu'une gestion efficace des changements appelle à la fois des contrôles préventifs, détectifs et correctifs, et que l'indépendance des contrôles est toujours plus cruciale à mesure que l'environnement informatique de production devient plus dynamique et complexe. Au nombre des contrôles préventifs nécessaires figurent la séparation des fonctions, l'autorisation des changements, ainsi que la supervision et la vérification. Cependant, pour surveiller et veiller efficacement à la mise en œuvre du processus, il faut que des contrôles détectifs soient en place pour permettre le suivi des changements dans l'environnement de production, faire le rapprochement avec les changements approuvés et détecter tout écart non autorisé. Une gestion efficace des changements a également un rôle correctif vis-à-vis de la gestion des SI au cours des pannes et des perturbations de service, car elle permet d'exclure en priorité les changements lors de la phase de dépannage, réduisant ainsi le temps de réparation.

3.2 À quoi reconnaît-on une gestion inefficace des changements ?

Comment savoir si le processus de gestion des changements en place dans une organisation est efficace ou non ? Quels comportements ou autres signes constituent des indicateurs utiles de la capacité de l'organisation, ou de son incapacité ?

Une gestion des changements inefficace ou inexistante est révélée par un dysfonctionnement à différents niveaux de l'organisation.

Au niveau du marché :

- Les opportunités manquées. L'entreprise ne parvient pas systématiquement à déployer les nouveaux produits et services programmés, en particulier lorsqu'elle doit, à la suite de changements non gérés, engager des ressources pour des tâches non planifiées. Celles-ci peuvent se traduire par du temps perdu / non budgété, des ressources perdues / non budgétées (personnel, capitaux) et des travaux non budgétés.
- Les projets de développement accusent du retard et dépassent souvent le budget prévu, se traduisant par des produits et services plus coûteux que ceux des concurrents.

Au niveau des clients / consommateurs / parties prenantes :

- Les produits et services n'affichent pas les performances annoncées ou attendues, ou sont défectueux. Il s'ensuit une qualité de produit ou de service faible, non fiable. Si les clients ont la possibilité de changer facilement de fournisseur, ils le feront.

Au niveau de l'organisation :

- Des changements non autorisés, non suivis induisent des risques de fraude.
- Les changements informatiques découlant des besoins de l'entreprise peuvent être mal interprétés et donc se révéler insuffisants ou être appliqués de manière inadéquate.
- Il existe peu de capacité, voire aucune, pour prévoir les répercussions d'un changement sur les processus qui sont en place.
- Étant donné la faible probabilité que les changements soient évalués les uns par rapport aux autres, on observe un manque de hiérarchisation, ce qui conduit soit à ne pas travailler sur ce qu'il faudrait, soit à travailler sur quelque chose de moins important. Les tâches peuvent être effectuées en dehors de la séquence prévue, d'où, éventuellement, la nécessité de revenir sur un travail ou des efforts redondants.
- De nombreux changements correctifs sont effectués sans autorisation, échouent ou sont réalisés en urgence.
- Les systèmes de patchs induisent d'importantes interruptions découlant d'échecs dans les changements, et qui se traduisent par des pannes, des dégradations du service, des tâches non planifiées, ou qui nécessitent de revenir sur un travail. Les relations de travail médiocres ou conflictuelles entre la sécurité et l'exploitation informatiques sont alors exacerbées.
- Un grand nombre de cycles (temps, ressources, capital) sont consacrés à corriger des activités ou des infrastructures en projet non autorisées, ce qui empêche de mener à bien les activités qui ont reçu un feu vert.
- Des ressources sont régulièrement consacrées à des retraitements faisant suite aux conséquences non prévues des changements mal gérés.
- On observe une forte rotation du personnel technique, ainsi que des signes d'épuisement parmi les intervenants clés.

Au niveau de l'infrastructure informatique :

- Un comportement au cas par cas, chaotique et dans l'urgence qui appelle des interventions régulières d'experts techniques; une proportion considérable de temps est consacrée aux situations d'urgence.
- Il y a une incapacité à suivre les changements, à rendre compte de l'avancement des changements et des coûts, et la présence de changements non autorisés.
- Une augmentation des ressources consacrées

à traiter les tâches non planifiées, aux dépens des tâches planifiées. C'est ce que l'on peut décrire comme un faible taux de réussite du changement. Ce taux mesure la quantité de travaux nouveaux qui découlent de la mise en œuvre d'un changement. Un taux élevé signifie que les changements sont appliqués comme prévu et qu'ils n'ont généré aucune tâche supplémentaire. À l'inverse, un taux faible indique qu'un changement a, contre toute attente, généré des tâches supplémentaires non planifiées, qui viennent quelquefois s'ajouter aux travaux nécessaires à la mise en œuvre du changement initial. Un faible taux de réussite peut être à l'origine d'un cercle vicieux qui consomme beaucoup trop de ressources.
- Les interfaces informatiques avec les pairs (R&D, développeurs d'applications, audit, sécurité, exploitation) sont inefficaces, d'où des barrières et des délais injustifiés.
- De nombreux changements non documentés interviennent au fil du temps, entraînant une dérive de la configuration de production, d'où un taux de réussite du changement moins élevé et une plus grande difficulté à déployer des patchs sans échec et un accroissement des tâches non planifiées.

3.3 À quoi reconnaît-on une gestion efficace des changements ?

Comment reconnaître une gestion efficace des changements ? Est-il possible lors d'une visite dans une organisation de déterminer si elle dispose d'un processus efficace de gestion des changements ?

Une gestion efficace des changements apparaît sous la forme d'une capacité mature (prévisible, reproductible, maîtrisée et mesurée) à différents niveaux de l'organisation.

Au niveau du marché :
- L'entreprise est en position pour agir lorsque se présentent de nouvelles opportunités d'affaires qui nécessitent des capacités informatiques supplémentaires ou des montées en version. Chaque opportunité est planifiée et gérée de manière prévisible. Des ressources adéquates peuvent être engagées et l'on sait qu'elles seront suffisantes et qu'elles reposent sur un suivi des performances antérieures.
- Les produits et services reposant sur les SI sont commercialisés comme prévu selon le calendrier défini.

Au niveau des clients / consommateurs / parties prenantes :
- Les produits et services donnent des résultats conformes à la publicité et affichent un niveau de qualité de service et de produit fiable et constant. Les problèmes et plaintes des clients sont traités rapidement. Les clients sont généralement satisfaits et fidèles à l'organisation.
- La demande de ressources destinées au centre d'assistance / service de dépannage est en baisse.
- L'évaluation des risques associés aux changements proposés et la hiérarchisation de mise en œuvre de ces changements sont confiées à des parties prenantes qui ont la capacité de mener à bien ces missions.
- Les participants au processus de changement comprennent les types de changements, leur degré de priorité, ainsi que les niveaux de formalisation et de rigueur requis pour mettre en œuvre chaque changement.
- S'assurer de la conformité aux réglementations demande moins d'efforts, car la gestion du changement fait partie des fondements de l'organisation. Quasiment toutes les réglementations posent des exigences vis-à-vis des SI. Lorsque les contrôles sont bien documentés, la mise en conformité avec une nouvelle loi ou réglementation ne constitue pas un nouveau projet, mais simplement une activité de cartographie.

Au niveau de l'organisation :
- La gestion du changement fait à l'évidence partie de la culture, comme en témoignent une compréhension approfondie, une bonne sen-

sibilisation, une adhésion visible et une capacité à agir.

- On effectue régulièrement des arbitrages efficaces, mettant en regard les coûts et risques associés au changement et les opportunités qui en découlent. Les changements sont programmés et hiérarchisés en conséquence. L'organisation est en mesure de prévoir l'impact du changement sur l'activité.
- Les ressources (temps, efforts, argent, capital) sont utilisées pour mettre en œuvre certains changements, avec aussi peu de gaspillages d'efforts que possible (taux de réussite du changement élevé) ; les ressources sont rarement orientées vers des tâches non planifiées.
- L'organisation peut, en toute confiance, répondre à des questions comme :
  - « Est-ce que je fais ce qu'il faut ? » (capacité à sélectionner et à hiérarchiser) et
  - « Fais-je les choses comme il faut ? » (avec une qualité et des performances acceptables).
- L'efficacité du processus de gestion des changements est mise en évidence par une discipline et une adhésion / un respect rigoureux des règles, une autorité décisionnaire centralisée, ainsi qu'une collaboration et une communication entre les départements.
- Les projets ayant reçu un feu vert sont mis en correspondance avec les ordres de production.
- Les investissements axés sur la sécurité et sur la conformité sont encouragés, car les configurations de production ne dérivent pas vers des états non conformes ou instables. Par conséquent, le coût de la sécurité et de la conformité est bien moindre.
- De plus en plus de temps et de ressources sont consacrés aux questions informatiques stratégiques, car l'organisation maîtrise les aspects tactiques (activité au jour le jour).
- Une gestion efficace des changements constitue un contrôle essentiel du pilotage des SI.

Au niveau de l'infrastructure informatique :

- Les contrôles de la gestion des changements (intégrés dans des processus informatiques bien définis) contribuent à la cohérence et à la prévisibilité, nécessaires pour la réalisation des objectifs de l'entreprise qui dépendent de ces processus. En d'autres termes, le personnel informatique comprend en quoi une gestion efficace des changements permet à l'entreprise d'atteindre ses objectifs.
- Une culture de la gestion des changements est perpétuée à la fois par la hiérarchie et par des contrôles préventifs, détectifs et correctifs qui dissuadent d'effectuer des changements sans qu'ils aient obtenu l'aval de la hiérarchie. Le management indique explicitement qu'il n'est pas envisageable que le nombre de changements non autorisés soit autre que zéro.
- L'organisation affiche un taux de réussite du changement élevé, ce qui se traduit par l'absence de tâches non planifiées, ou tout du moins en quantité minime. S'il n'y a pas d'urgences et que le processus d'intégration des changements est bien défini, le taux de réussite du changement sera bien plus élevé.
- Des contrôles efficaces des changements sont en place, font l'objet de comptes rendus réguliers et sont faciles à auditer. Les contrôles préventifs sont correctement formalisés et déployés systématiquement, et les contrôles détectifs servent à superviser, piloter et opérer des rapprochements avec les ordres de mission. Les contrôles sont propices à un sondage de corroboration par les auditeurs et requièrent peu, voire pas d'informations supplémentaires de la part du responsable des SI.
- Les écarts dans les configurations de production sont détectés rapidement, si bien que leurs coûts et leurs répercussions sont les plus faibles possible.
- L'entreprise fait régulièrement la preuve de son excellence en matière de gestion des changements.
- Des niveaux de service plus élevés (forte disponibilité / disponibilité / temps moyen entre les pannes, faible délai moyen pour détecter les problèmes / incidents, faible délai moyen de réparation) sont observés en présence de processus bien définis qui introduisent des changements programmés et prévisibles.
- Les SI permettent de revenir rapidement à un

état opérationnel connu, fiable et dont on sait qu'il fonctionne, lorsque des problèmes apparaissent après la réalisation d'un nouveau changement ou la mise en place d'une nouvelle configuration.

- Les SI affichent des structures de coûts correspondant à une efficience inhabituelle (ratio d'administration serveurs / systèmes de 100:1 ou plus, alors qu'il est au moins 10 fois moindre dans les organisations peu performantes).
- Les SI sont capables d'identifier et de résoudre rapidement des problèmes opérationnels, y compris des incidents de sécurité.
- Les organisations disposant de processus et contrôles efficaces de gestion des changements traitent les patchs de manière planifiée et prévisible, en leur appliquant la même procédure et la même analyse qu'à tous les autres changements. Des patchs critiques sont ajoutés à la liste des changements envisagés, et ils sont évalués, testés et insérés dans le programme de déploiement déjà établi.
- Les contrôles préventifs et détectifs sont automatisés, ce qui permet une communication plus simple et plus précise aux auditeurs, nécessite moins d'inspections manuelles et font ressembler les sondages de corroboration à de l'archéologie.
- Les organisations les plus efficaces appliquent des patchs moins fréquemment que la moyenne, peut-être dix fois moins souvent, acceptant que le risque d'exposition à une vulnérabilité soit moins important que le risque de non-disponibilité lié aux répercussions non anticipées d'un mauvais changement ou d'un changement hors cycle. Cependant, dans le cas d'une mise à jour critique, les organisations performantes sont à même d'appliquer un patch hors cycle avec un risque minime.

Pour qu'un processus soit efficace, il ne suffit pas que les parties prenantes soient simplement associées à l'évaluation des risques induits par des changements proposés et par leur hiérarchisation. Le manque d'intérêt, d'implication et d'adhésion des collaborateurs est l'un des obstacles auxquels se heurtent les départements informatiques lorsqu'ils tentent de mettre en œuvre un solide processus de gestion des changements. Il faut faire en sorte que les responsables de département participent activement à l'ensemble du processus, depuis l'identification initiale de leurs besoins jusqu'à la vérification de l'acceptation par une majorité d'utilisateurs et à l'agrément des changements à apporter au niveau de la production. Ces points critiques sont davantage susceptibles de poser problème lorsque le rôle du responsable est intégré dans les politiques et procédures correspondantes et que les membres de la direction mettent l'accent qu'il faut sur la nécessité d'être « copropriétaires » du processus, plutôt que de simples observateurs. La communication et la collaboration entre l'informatique et les autres fonctions sont essentielles à l'efficacité des processus.

3.4 Indicateurs de la gestion des changements

Les auditeurs internes doivent déterminer si, pour évaluer l'efficacité du processus et en augmenter la valeur pour l'entreprise, on utilise bien les principaux indicateurs de la gestion des changements. Les indicateurs, énumérés dans le tableau 1, sont utiles pour indiquer la présence d'un processus efficace de gestion des changements.

Tableau 1 : Les indicateurs de la gestion des changements

Indicateurs	Observations
Nombre de changements autorisés par semaine, mesuré dans le journal de gestion des changements autorisés.	En général, des changements plus nombreux sont le signe d'une productivité plus grande, tant que le taux de réussite du changement reste élevé. La tendance (amélioration, recul, situation inchangée) doit être appréhendée dans le contrat de l'activité.
Nombre de changements effectifs par semaine, mesuré par les contrôles détectifs, par exemple grâce à un logiciel de pilotage.	Le nombre de changements effectivement mis en œuvre par semaine ne doit pas dépasser le nombre de changements autorisés.
Nombre de changements non autorisés. Il s'agit de changements qui contournent les processus de changements. On les mesure par soustraction du nombre de changements autorisés au nombre de changements effectifs. En l'absence de contrôles détectifs, il est impossible de mesurer avec fiabilité les changements effectifs. Dans ce cas, on peut prendre, comme indicateur de substitution, le nombre d'interruptions non planifiées.	Plus ce nombre est faible, mieux c'est, mais classiquement, le seul nombre acceptable de changements non autorisés est zéro ; un seul changement « périlleux » peut anéantir toute l'opération ou induire un risque élevé. Un nombre élevé de changements non autorisés est le signe que le « véritable moyen choisi pour procéder à des changements » consiste à contourner le processus de gestion des changements.
Taux de réussite du changement, c'est-à-dire la proportion de changements mis en œuvre avec succès (n'ayant pas entraîné de panne, de dégradation du service ni de tâches non planifiées) par rapport aux changements effectivement réalisés.	Plus ce taux est élevé, mieux c'est. Lorsque les changements ne sont pas gérés ou pas testés correctement, le taux de réussite tourne généralement autour de 70 %. Dans les organisations performantes, non seulement le taux de réussite ressort régulièrement à 99 %, mais les changements ratés entraînent rarement une interruption de service ou des tâches non planifiées.
Nombre de changements urgents (patchs compris), que l'on détermine en dénombrant les changements ayant nécessité un agrément en urgence durant la semaine, en faisant appel au comité d'examen des changements ou au processus de changement urgents.	Généralement, plus ce nombre est faible, mieux c'est. Un nombre élevé de changements urgents est le signe que le « véritable moyen choisi pour procéder à des changements » consiste à recourir à la procédure d'urgence, parce que c'est plus commode ou plus rapide. Les changements urgents affichent généralement un taux de défaillance plus élevé, et génèrent des tâches non planifiées ou nécessitent de revenir sur un travail. Si le nombre de changements urgents augmente, d'autres problèmes de gestion des changements peuvent en être à l'origine.
Proportion de patchs déployés dans le cadre de la diffusion programmée d'une nouvelle version logicielle. Lorsque les patchs sont déployés dans ce cadre, ils n'induisent pas de perturbation de la production et présente un taux de réussite bien supérieur.	En général, plus cette proportion est élevée, mieux c'est. Paradoxalement, les organisations SI performantes affichent généralement le taux de patching le plus faible. Certaines de ces organisations performantes choisissent d'installer des patchs une fois par an, même si elles procédaient à des milliers de changements par semaine. Elles réussissent souvent à atténuer les risques de vulnérabilité sans avoir besoin de procéder à des changements dans les systèmes de production (par exemple en bloquant les vulnérabilités au niveau du pare-feu).

Indicateurs	Observations
Proportion du temps consacré à des tâches non planifiées. Les tâches planifiées correspondent à des projets et travaux autorisés. Les tâches non planifiées incluent les cycles de réparation, de reprise et les changements urgents.	Plus cette proportion est faible, mieux c'est (par exemple 5%, ou moins).
Proportion des projets livrés en retard par rapport à l'échéance prévue même si une mauvaise gestion de projet peut également impacter la mesure.	Typiquement, plus cette proportion est faible, mieux c'est. Quand les organisations passent du temps sur des tâches non planifiées, le temps passé pour des tâches planifiées n'est plus suffisant, comme pour les nouveaux projets et services, ce qui engendre des retards de livraison du projet.

Figure 1 : Les tâches non planifiées, indicateurs d'un processus de gestion efficace des changements

Nombre de changements dans la production X **Pourcentage de changements défaillants ou non autorisés** X **Durée moyenne de reprise** = **Pourcentage de temps consacré à des tâches non planifiées**

Organisation performante	**>1000 changements par semaine**	**< 1%**	**Quelques minutes**	**< 5% du temps**
Moyenne	**Centaines**	**~ 30-50% en moyenne**	**Heures et jours**	**35-45% du temps**

MOYENNE : 35 à 45 % du temps (et des dépenses d'exploitation) consacré à des tâches non planifiées !
IMPACT : Projets en retard, nécessité de revenir sur un travail, problèmes de conformité, écarts non maîtrisés, etc.

Figure 2 : Variables clés influençant les processus de gestion des changements

La figure 1 et la figure 2 présentent les indicateurs d'une gestion efficace des changements et des principaux contrôles qui les améliorent ou les font baisser. Ces indicateurs[1] sont :

- Le nombre de changements appliqués au niveau de la production.
- La proportion de ces changements ayant échoué ou qui ne sont pas autorisés.
- Le délai nécessaire à la restauration après un changement qui a échoué.

Lorsque l'on multiplie ces trois variables, on obtient les tâches non planifiées.

Ce modèle, simplifié à l'extrême, ne prétend pas être mathématiquement exact. Il entend simplement montrer les variables dominantes et les principaux indicateurs d'une gestion efficace des changements informatiques, et donc de SI efficaces :

- C'est lorsqu'une organisation informatique n'applique aucun changement ou se situe dans une période de gel des changements que la disponibilité est la plus grande et que les tâches non planifiées sont les moins nombreuses.
- Lorsqu'une organisation SI ne met pas en œuvre une politique de gestion des changements (contrôles préventifs et détectifs inadéquats), des changements non autorisés et défaillants causent de longues interruptions, qui alourdissent le volume des tâches non planifiées.
- Lorsque les organisations informatiques affichent un ratio tâches non planifiées / tâches planifiées élevé, elles ont moins de temps disponible pour réaliser les travaux qu'elles étaient chargées d'effectuer, par exemple fournir de nouveaux produits et services.

[1] *D'après le benchmark de l'ITPI, qui a étudié 11 organisations SI performantes et enquêté auprès de centaines d'autres.*

Les organisations SI performantes peuvent faire encore mieux que ne le suggère ce modèle. Lorsque les changements sont gérés de manière adéquate, même les changements planifiés échoués conduisent rarement à des pannes, si bien que leur MTTR *(mean time to repear)* est égal à zéro. À l'autre extrémité, les organisations peu performantes sont souvent incapables de mesurer autre chose que les pannes et tâches non planifiées évidentes.

3.5 Intégration de la gestion des patchs dans la gestion des changements

Bien qu'il faille souvent appliquer des patchs logiciels en urgence, dans l'idéal, le déploiement des patchs devrait être intégré à un processus de pré-production, dans lequel les patchs peuvent être correctement testés dans un environnement de simulation. Dans l'idéal, ils seront également déployés lors de la diffusion programmée de la nouvelle version d'un logiciel.

La mise en œuvre d'un patch est souvent risquée, et ce pour plusieurs raisons. Les patchs ont tendance à affecter de nombreuses bibliothèques système critiques, ainsi que d'autres logiciels utilisés par de nombreux programmes d'application. Les patchs constituent généralement des changements de grande ampleur, souvent assortis d'une maigre documentation qui décrit ce qu'ils sont censés changer. Ils représentent des opérations vastes et complexes. Même de petits écarts de configuration peuvent induire des résultats nettement différents. En conséquence, le taux de réussite du changement concernant les patchs est bien inférieur à celui des changements classiques, si bien qu'ils nécessitent des tests plus complets. En l'absence de tests et de planification suffisants apparaît invariablement une attitude qui consiste à appliquer le patch et à prier pour que tout fonctionne bien (« patch and pray »).

Il est souvent fait référence à cette attitude : ni l'application d'un patch, ni le fait de l'éviter ne semble aboutir à l'objectif visé, à savoir créer une plateforme de calcul sécurisée et disponible. Comme indiqué plus haut, les organisations SI performantes appliquent des patchs bien moins fréquemment que les autres, et néanmoins, elles parviennent au niveau de sécurité désiré. Il est faux de supposer qu'en agissant ainsi, elles menacent la sécurité. Au contraire, elles gèrent activement le risque résiduel et, au lieu d'appliquer des patchs, elles déploient des contrôles. Elles créent aussi un programme de déploiement de nouvelles versions qui regroupe les patchs et les montées de version dans le déploiement de nouvelles versions, au lieu d'appliquer les patchs un par un dans chacun des systèmes.

Les risques associés aux changements ne se limitent pas à l'application de patchs et peuvent survenir avec n'importe quelle technologie automatisée de déploiement d'un changement.

Le recours simultané aux technologies de gestion des patchs et de déploiement des changements rend l'environnement informatique de production plus dynamique et plus complexe : le nombre de vecteurs de changements augmente, de même que le nombre de changements susceptibles d'être réalisés. Ces environnements requièrent :

- des contrôles préventifs supplémentaires visant à réduire la probabilité de changements non autorisés et
- des contrôles détectifs indépendants visant à simplifier les fonctions de pilotage, de rapprochement et de *reporting*.

3.6 Principes directeurs : comment décider s'il faut appliquer des changements, quand et comment procéder ?

Les principes qui guident de bonnes décisions de gestion des changements supposent de se poser les questions suivantes :

- Ces changements sont-ils véritablement

nécessaires ? C'est durant les périodes de gel des changements que les organisations SI enregistrent le plus faible volume de tâches non planifiées et d'interventions en urgence. C'est pourquoi tout changement doit justifier, d'une part, les efforts de préparation et de mise en œuvre et, d'autre part, les conséquences (souvent imprévues) qui peuvent s'ensuivre.

- A-t-on défini des périodes de gel des changements, durant lesquelles aucun changement n'est autorisé ? Ces périodes étant non seulement les plus stables, mais aussi les plus productives, il faut impérativement en prévoir et les appliquer.
- Si des changements doivent être effectués, comment s'assurer qu'ils seront couronnés de succès ? Des changements non testés affichent rarement un taux de réussite supérieur à 70%. Les organisations qui veulent que leurs changements soient réussis doivent investir du temps et des ressources pour tester correctement ces changements.
- Lorsque des changements doivent être mis en œuvre, sont-ils programmés par lots ? La variance est source de risque, et on peut la réduire en regroupant plusieurs changements, de sorte qu'ils pourront être testés et appliqués simultanément. Il s'ensuit des périodes plus longues sans changements opérationnels, ainsi que des périodes de mise en œuvre des changements plus courtes et plus productives.
- Les variances sont-elles communiquées régulièrement au responsable des SI ? Les changements dans la production sont-ils comparés aux travaux autorisés ? Les interruptions non planifiées et variances associées aux changements sont-elles documentées et cherche-t-on à y remédier ? Le management et les auditeurs peuvent-ils facilement accéder à des rapports montrant les effets des contrôles préventifs et détectifs ? Lorsque les contrôles continus et de *reporting* fonctionnent correctement, le management informatique a les informations nécessaires pour identifier de façon efficace et efficiente les problèmes et est davantage susceptible de réaliser ses objectifs.

4. Quelles questions dois-je poser à propos de la gestion des changements et des patchs ?

Ce chapitre propose aux auditeurs un ensemble de questions qu'ils peuvent utiliser afin de se faire une idée sur l'efficacité de la gestion des changements. L'objectif est de poser les bonnes questions et de savoir interpréter les réponses habituellement fournies par différents responsables des SI qui peuvent ne pas accorder la même importance à une gestion efficace du changement.

Les archétypes que l'on rencontre le plus fréquemment sont :

- Les responsables des SI qui disposent d'un processus efficace de gestion des changements.
- Les responsables des SI qui disposent d'un processus inefficace de gestion des changements, mais qui cherchent à l'améliorer (selon une approche de résolution des problèmes).
- Les responsables des SI qui disposent d'un processus inefficace de gestion des changements, mais qui ne prévoient rien pour y remédier (déni de la réalité).

Tableau 2 : Questions à poser à propos de la gestion des changements, en fonction du profil

Question à poser au responsable des SI	Responsable des SI dont le processus de gestion des changements est efficace	Responsable des SI adoptant une approche de résolution des problèmes	Responsable des SI en déni potentiel
« La gestion des changements est cruciale. Pensez- vous que votre processus de gestion des changements soit efficace ? »	« Il est irréprochable. Nous sommes même prêts pour une mise en conformité à la section 404 de la loi Sarbanes-Oxley parce que tous les contrôles sont déjà en place. Il nous a fallu produire quelques rapports supplémentaires pour montrer les cartographies des contrôles, mais tout est en ordre. »	« C'est drôle que vous posiez la question, nous sommes justement en train d'y travailler, mais c'est le cas de tous ceux qui doivent se conformer à la section 404 de la loi Sarbanes-Oxley. Nous en saurons plus au fur et à mesure. »	« Notre processus semble fonctionner. Je n'ai rien entendu dire de négatif à son sujet, et notamment de la part de l'audit. Nous ne pouvons pas nous permettre la surcharge d'un processus lourd pour réparer quelque chose qui fonctionne déjà. »
« Combien de changements non autorisés vous paraissent acceptables ? »	« Zéro, et pas un de plus. Le moindre changement non programmé peut réduire à néant tous les efforts, et c'est pourquoi nous opérons quotidiennement des rapprochements concernant les changements. Nous faisons confiance, mais nous vérifions. »	« Eh bien, si vous posez la question comme ça, bien sûr que le seul nombre acceptable de changements non autorisé est zéro. Mais je parie que vous ne trouverez personne qui serait prêt à jouer sa prime trimestrielle là-dessus. Surtout après le dernier trimestre qu'on a eu. »	« Écoutez, nous ne sommes pas payés pour ne pas appliquer de changements. Il faut parfois savoir s'écarter des règles. Ici, c'est comme ça si l'on veut que les choses soient faites. La gestion des changements, c'est la bureaucratie à l'œuvre, et tout ce qu'ils veulent, c'est ralentir les choses. »

Question à poser au responsable des SI	Responsable des SI dont le processus de gestion des changements est efficace	Responsable des SI adoptant une approche de résolution des problèmes	Responsable des SI en déni potentiel
« Décrivez les contrôles dont vous avez besoin dans votre processus de gestion des changements. »	« Il nous faut des contrôles préventifs, détectifs et correctifs, afin que le management puisse disposer d'une vision exacte de la situation. Nous avons défini quelques indicateurs du changement et identifié quelques autres parties prenantes qu'il nous faut intégrer dans le comité de gestion des changements. Nous n'avions pas pensé que la gestion des changements pouvait intéresser les comptables, mais désormais, ils assisteront à nos réunions. »	« Nous avons toute une équipe d'auditeurs internes et de consultants qui travaillent au projet Sarbanes-Oxley. Ils sont en train de concevoir et de mettre sur pied un plan permettant de tester les contrôles spécifiques. Tout ce projet Sarbanes-Oxley a fait apparaître la nécessité d'une surveillance intégrée et d'une vision du changement à l'échelle de l'entreprise. Nous avons aussi décelé quelques processus qui ont besoin d'une meilleure gestion des changements, et on y travaille aussi. »	« Nous en sommes encore à la phase d'analyse. On est tellement pris par toutes les autres tâches urgentes que tout ce à quoi nous avons pu consacrer un peu de temps, ce sont les contrôles imposés par la loi Sarbanes-Oxley. Mais nous savons que c'est important, et nous nous y mettrons dès que nous le pourrons. De plus, actuellement, nous n'avons aucun budget réservé spécialement à ce travail. Mon expérience me fait dire que ce dont nous disposons est probablement suffisant, puisque personne ne m'a spécifiquement fait savoir que le processus actuel était inadéquat. »
« Avons-nous observé des avantages découlant du processus de gestion des changements ? »	« Absolument. De fait, les avantages que nous avons pu observer sont tellement évidents que nous avons créé une culture interne de la gestion des changements. Nous n'avons plus l'impression d'avoir embrassé une carrière de pompier. Nous avons considérablement amélioré nos performances, la disponibilité et le degré de satisfaction, aussi bien de nos clients que du personnel en interne, et de toute la hiérarchie jusqu'au sommet de l'entreprise. »	« Oui, mais nous n'avons pas encore atteint nos objectifs. Nous avons réduit le nombre total de pannes et significativement amélioré notre taux de réussite du changement. Désormais, les changements se déroulent à l'intérieur de la plage définie, même si nous avons encore, à l'occasion, quelques « cowboys » qui ne prennent pas la peine de respecter la procédure. »	« En ce moment, notre rythme d'activité est si effréné que nous n'avons tout simplement pas le temps d'examiner de plus près un processus de gestion des changements lourd et qui ralentit les choses, réduit la productivité et crée un environnement bureaucratique. Je me refuse à réclamer des comptes à chacun concernant le respect du processus de changements, car on leur en demande déjà bien assez. Mais des pannes liées aux changements se produisent occasionnellement, et nous savons que nous ne pouvons pas continuer à laisser le système de gestion des commandes planté. »

GTAG – Quelles questions dois-je poser à propos de la gestion des changements et des patchs ?

Question à poser au responsable des SI	Responsable des SI dont le processus de gestion des changements est efficace	Responsable des SI adoptant une approche de résolution des problèmes	Responsable des SI en déni potentiel
« Vous souvenez-vous de la panne sur tout le site qui s'est produite la semaine dernière à cause d'un changement ? Que s'est-il passé ? »	« Nous avons pu déterminer que le changement qui a causé cette panne de 10 minutes avait été autorisé. Cependant, nous n'avons pas su en anticiper les conséquences en aval sur un système sans lien direct. Mais cela ne se reproduira plus. »	« Nous avons trouvé : un développeur avait procédé à un changement sans suivre le processus dont nous étions convenu. Il n'aurait jamais dû avoir autorité pour donner son accord à des changements sur ce système précis. Nous nous sommes dépêchés de rectifier cela, et ce développeur n'a même plus le droit de se connecter aux serveurs de production. »	« Nous avons constaté que l'un de nos fournisseurs faisait de la maintenance et procédait à des montées en version sur des logiciels. Le problème, c'est qu'ils ont écrasé une bibliothèque de programmes que nous avions personnalisés. Or, ils sont censés garder la trace de nos adaptations : il s'agit donc d'un non-respect de notre contrat de maintenance. »
« Lorsque vous avez travaillé sur cette panne, quel processus avez-vous employé pour trouver ce qui n'a pas fonctionné ? »	« La première chose que nous faisons systématiquement, c'est d'exclure en priorité les changements lors de la phase de dépannage. Nous savions sur-le-champ que la panne n'était pas due à un changement programmé. Ensuite, nous avons vérifié tous les changements urgents au niveau de la production. Nous avons trouvé quatre changements effectués deux minutes avant la panne, puis nous avons trouvé qui les avait réalisés. Ils ont procédé à un retour arrière, et tout a pu repartir en quelques minutes. »	« Nous sentions bien que ce problème ne pouvait pas venir de nos changements autorisés. Nous testons et déployons nos changements uniquement à l'intérieur d'une version spécifique. Nous avons donc commencé à faire des recherches, à regarder les journaux, en remontant à partir de la panne et en examinant tout ce qui s'est passé en dehors de la version. Nous avons finalement trouvé qui avait réalisé le changement en cause, mais pas pourquoi. Je pense que l'administrateur en a tiré tous les enseignements nécessaires ce jour-là. »	« N'ayant pas de processus centralisé, nous avons mobilisé différentes équipes pour qu'elles essaient de trouver ce qui ne fonctionnait pas. Nous avons finalement constitué une équipe de choc. Elle a rapidement conclu que la panne était due à la montée de version du fournisseur, mais il nous a fallu nous réunir avec ce dernier pour déceler que la cause était notre bibliothèque. Ils n'avaient aucun moyen de la restaurer dans son état préalable, si bien qu'il nous a fallu réinstaller l'ensemble du répertoire de logiciels d'origine. »

Question à poser au responsable des SI	Responsable des SI dont le processus de gestion des changements est efficace	Responsable des SI adoptant une approche de résolution des problèmes	Responsable des SI en déni potentiel
« Comment surveillez-vous l'état général du processus ? »	« Par le taux de changements, le taux de réussite du changement, la durée moyenne de reprise (MTTR), la durée moyenne de bon fonctionnement (MTBF), le décompte des changements non autorisés qui contournent le processus. Nous avons également un indicateur de la couverture qui permet de montrer quels pans de l'entreprise ne participent pas au processus. Le nombre de tâches non planifiées constitue un indicateur clé. Nous cherchons toujours à détecter les écarts et à comprendre comment les réduire à la source. »	« Nous mesurons en combien de temps nous pouvons appliquer un changement, ainsi que le délai moyen entre une demande de changement et sa finalisation. Nous allons bientôt aussi mesurer le taux de réussite du changement ainsi que les changements urgents et les changements non planifiés. »	« Nous n'utilisons pas d'indicateurs fantaisistes, même si l'excellence des processus est pour nous une priorité. Je sais que nous avons beaucoup d'urgences à régler, mais il n'y a pas moyen d'y échapper quand on travaille avec certaines de ces personnes. »
« Quel est l'objectif de votre processus de gestion des changements ? »	« Fiabilité, disponibilité et réduction des coûts. Les deux premières doivent augmenter et les coûts baisser. Si l'on se contente de n'optimiser que l'un de ces trois éléments, on ne sera pas dans les clous. »	« Nous voulons faire autant de changements que l'activité le nécessite. Et nous voulons qu'ils soient rapides et précis. »	« Nous voulons que toutes les parties prenantes clés participent à nos réunions sur la gestion des changements, et que tout le monde ait bien conscience de ce qui se passe et pourquoi. Pour nous, tant que nos audits sont favorables, tout va bien. »

Question à poser au responsable des SI	Responsable des SI dont le processus de gestion des changements est efficace	Responsable des SI adoptant une approche de résolution des problèmes	Responsable des SI en déni potentiel
« Votre processus de patch entraîne-t-il des perturbations ? »	« Non, pas du tout. Nous savons bien que la disponibilité est capitale pour les métiers. Il nous faut trouver comment réduire les risques sécurité sans les dangers associés aux changements. En moyenne, nous appliquons un seul lot important de patchs par an. »	« Auparavant, la gestion des patchs induisait beaucoup de perturbations, mais après la grosse panne que nous avons subie il y a six mois, nous sommes revenus sur toutes les certitudes que nous avions à propos des patchs à déployer et du moment le plus adéquat pour les appliquer. Nous y consacrons moins de temps : avant, c'était toutes les semaines, maintenant, c'est tous les mois, et nous envisageons de passer à une fois par trimestre. »	« Étant donné la piètre qualité des logiciels que sortent les fournisseurs, nous continuons de consacrer beaucoup trop de temps à appliquer des patchs. C'est une situation inextricable. Si nous n'appliquons pas de patchs, nos systèmes seront piratés, mais si nous les patchons, nous risquons de crasher nos systèmes de production. Enfin, puisque nous ne pouvons pas nous permettre d'être « descendus en flammes » dans la presse, nous n'avons pas d'autre choix que d'appliquer les patchs. »

4.1 Faire évoluer les capacités de gestion des changements

La gestion des changements est un processus évolutif. Les groupes ne doivent pas se décourager lorsqu'ils commencent à développer leur processus de gestion des changements. Les solutions peuvent consister à changer les gens, les processus ou la technologie. Voici les attitudes classiques vis-à-vis de la gestion des changements :

1. **Oublier le changement :** « Est-ce que le commutateur vient de se réinitialiser ? »
2. **Avoir conscience du changement :** « Qui vient de réinitialiser le commutateur ? »
3. **Annoncer le changement :** « Je réinitialise le commutateur, dites-moi si ça pose un problème. »
4. **Autoriser le changement :** « J'ai besoin de réinitialiser le commutateur. Qui peut m'en donner l'autorisation ? »
5. **Programmer le changement :** « Quand sera la prochaine plage de maintenance ? J'aimerais bien réinitialiser le commutateur à ce moment-là. »
6. **Vérifier le changement :** « En regardant les journaux d'erreurs, je vois que le commutateur a été réinitialisé comme prévu. »
7. **Gérer le changement :** « Programmons la réinitialisation du commutateur sur la semaine 45, comme ça, nous pourrons faire la montée de version et la réinitialisation en même temps. »

5. Par quoi les auditeurs internes doivent-ils commencer ?

D'après le cadre de référence du COSO, c'est le management qui définit les objectifs stratégiques, qui choisit les stratégies et qui assure la diffusion des objectifs dans toute l'entreprise, après les avoir harmonisés. La gestion des risques de l'entreprise est orientée vers la réalisation de ces objectifs, sur quatre axes : stratégie, exploitation, *reporting* et conformité à la législation. Les contrôles préventifs, détectifs et correctifs doivent être conçus et mis en œuvre de façon à permettre un traitement efficace du risque. L'audit peut aider le management informatique à disposer d'une procédure efficace pour gérer les risques liés à la réalisation des objectifs. Au nombre des objectifs de gestion des changements que le management informatique doit définir figurent ceux qui ont trait à la revue et à la validation des demandes de changements, afin que la mise en œuvre des changements soit appropriée et efficiente, ainsi qu'au rétablissement rapide du SI en cas d'échec des changements.

Les contrôles préventifs, détectifs et correctifs doivent être définis d'après les objectifs fixés par la hiérarchie pour la gestion des changements apportés aux SI.

Pour réussir, le management doit répondre aux préoccupations des actionnaires, qui sont représentés par le Conseil. Les objectifs de l'entreprise sont généralement exprimés en termes de chiffre d'affaires / part de marché, de croissance de l'activité / du cours de Bourse, ou de maîtrise du coût des ressources humaines et des opérations. Le plan d'action qui doit permettre d'atteindre ces objectifs devra être formulé et déployé efficacement dans toute l'organisation pour avoir une chance de succès. Le Conseil doit notamment s'assurer que le management a identifié et évalué les risques qui pourraient faire obstacle à la réalisation des objectifs. Des procédures solides devraient être mises en place afin de réduire, de gérer, d'accepter et de transférer les risques efficacement. Les variations par rapport au plan défini constituent un autre risque, qui nécessite une gestion active. Les auditeurs internes sont les yeux et les oreilles du management : ils recherchent les zones de l'environnement de gestion des risques qui doivent être renforcés.

Pour la plupart des entreprises, l'indisponibilité de services ou de fonctions critiques, même pendant une courte période, est l'un des facteurs qui compromet le plus rapidement les avancées dans la réalisation des objectifs clés. Ainsi, une panne inattendue du réseau peut interrompre des processus critiques, tels que la coordination des livraisons avec les fournisseurs et le traitement rapide des commandes de la clientèle. Le dysfonctionnement d'un serveur Internet, d'un serveur d'application, d'une base de données critique peut être tout aussi dommageable. Avec le management, les auditeurs internes doivent s'assurer que ces risques, et les risques connexes, ont été identifiés, et qu'ils sont mesurés et gérés correctement. Mais comment les risques peuvent être gérés si leurs causes n'ont pas été détectées et analysées ?

Au nombre des responsabilités les plus importantes du service informatique figurent la protection de l'environnement de production et le soutien de l'organisation dans la réalisation de ses objectifs. Il incombe aux auditeurs internes de veiller à ce que des processus adéquats de gestion du risque soient en place, y compris au niveau des SI. À cette fin, il ne faut pas sous-estimer l'importance d'un dispositif efficace de gestion du risque, qui doit être régulièrement revu par les auditeurs internes.

5.1 Rôle de l'audit dans la gestion des changements

Les auditeurs internes n'ayant généralement pas le temps d'examiner toutes les facettes des organisations dans lesquelles ils travaillent, ils doivent élaborer leurs programmes d'audit en se fondant sur une évaluation des risques. Pour aider à l'éva-

luation du risque métier dans le cadre informatique, ils devront rassembler des informations préliminaires. Pour déterminer l'ampleur des risques induits par les pratiques de gestion des changements au sein de l'organisation et pour décider de procéder à une revue à un haut niveau ou approfondie, les auditeurs devraient :

- Comprendre les composantes de base de la gestion des changements. Le concept de gestion des changements utilisé ici n'englobe pas l'ensemble du cycle de développement des systèmes, tel que le développement d'applications ou la gestion des configurations. Néanmoins, la gestion des changements doit refléter le cycle de développement des systèmes (et les contrôles qui y sont associés) et en faire partie intégrante. La compréhension du contenu de ce guide procure des connaissances suffisantes pour permettre de poser les questions difficiles concernant l'activité des SI, afin de déterminer le niveau des éventuelles améliorations à apporter à la gestion des changements et aux contrôles (voir le tableau 2, page 26, pour les questions utiles à poser).
- Recourir aux indicateurs de processus de gestion des changements efficace et inefficace pour évaluer l'efficacité relative des processus de gestion des changements au sein de votre organisation. Analyser le processus de gestion des changements et rechercher les éléments clés énumérés dans ce guide. Déterminer comment le management informatique mesure ce processus et si ce dernier répond véritablement aux besoins de l'entreprise.
- Obtenir le tableau de bord du management informatique, afin de mesurer les résultats et l'efficacité du processus. Déterminer si des indicateurs appropriés sont utilisés pour le pilotage et l'amélioration continue (tableau 1, page 21).
- Déterminer si le management informatique a confié la gestion des changements à des intervenants autres que les développeurs de logiciels ou les personnes chargées de préparer les changements. Le management a-t-il sécurisé l'environnement de production, de sorte que les responsables de la mise en place des changements peuvent mener à bien leur mission ?
- Procéder à une brève revue pour déterminer s'il existe des pistes d'audit des changements apportés à l'environnement de production et pour vérifier que les pistes d'audit ne peuvent pas être manipulées ou détruites.
- Dans le cadre des audits de contrôle des changements, rechercher les indicateurs d'efficacité de la gestion des changements. Se concentrer sur les risques pour l'entreprise qui résultent d'une éventuelle incapacité à atteindre les objectifs de contrôle.
- Aider le management à identifier des modèles qui lui permettront de mieux gérer les changements.
- Lorsque l'organisation envisage d'externaliser les fonctions informatiques, vérifier que ses attentes sont clairement définies dans des contrats et accords de niveau de service. Concernant le processus de gestion des changements, il importe de s'assurer de :
  - Qui est responsable, en interne, de la gestion des changements demandés au jour le jour.
  - Comment l'organisation peut déterminer que des changements effectués par le prestataire extérieur sortent du cadre défini.
  - Quels moyens l'organisation dispose pour vérifier que le prestataire extérieur ne lui facture pas des changements non autorisés ou déraisonnables. Comment peut-elle déterminer que de tels changements ont été effectués ?
  - Ce qui empêche le prestataire extérieur de donner son aval à des changements hors des plages de temps définies, ce qui a des répercussions importantes sur l'organisation (applications indisponibles au moment où l'on en a besoin) et sur les coûts (manque à gagner).
  - Qui est chargé de veiller à l'adéquation du calcul, du chiffrage, de la validation, de la planification, du contrôle, de la mise en œuvre et de la revue périodique des changements qui affectent l'informatique.
  - Si le prestataire a pris en compte les répercussions sur l'infrastructure (système et

réseau), ainsi que sur la sécurité informatique.
  - Si l'organisation a identifié qui, parmi ses membres, siège dans les comités de contrôle des changements.
  - Qui veille au respect des accords de niveau de service.
  - Pour les systèmes qui relèvent de la section 404 de la loi Sarbanes-Oxley, ou d'autres dispositions réglementaires, l'accord de niveau de service doit également décrire les pratiques requises, les procédures de validation, le calendrier des tests nécessaires, les actions correctives, les nouveaux tests à réaliser, et d'autres aspects encore.
- Lors de l'analyse et de la rédaction des observations d'audit, présenter toute la valeur ajoutée pour l'entreprise des processus de gestion des changements efficaces, ainsi que les risques découlant de processus inefficaces. Exposer clairement les risques opérationnels, financiers et réglementaires qui ne sont pas correctement gérés, et mettre en relation les constats et les tolérances au risque que le management a définies conformément à ses objectifs. Éviter de se concentrer sur la technologie, sauf dans les cas où certains contrôles des processus de gestion des changements sont automatisés. Rappeler plutôt au management que la gestion des changements s'inscrit dans le cadre d'un processus mettant l'accent sur les aspects managériaux et humains, et qu'il s'accompagne de contrôles techniques et automatisés.

Auteurs et réviseurs

Auteurs
Sajay Sajay Rai, CISSP, CISM
Gregory Wilson, CISSP, CISM, CGEIT
Duy Nguyen

Réviseurs
Philip Chukwuma, CISSP
Steve Hunt, CIA
Steve Jameson, CIA, CCSA, CFSA, CRMA

Réviseurs en français
Hervé Molina
Béatrice Ki-Zerbo, CIA

Annexe A : Exemple d'étude de cas pour la gestion des changements

Les organisations performantes utilisent leurs processus de gestion des changements informatiques pour réduire leurs risques, ainsi que pour accroître leur efficacité et leur efficience. Les effets positifs qui sont associés à un contrôle efficace des changements sont donc significatifs et mesurables. La capacité à le démontrer, plutôt que de se contenter de « faire plaisir aux auditeurs » facilite l'élaboration d'une étude de cas destinée à améliorer ces contrôles. Comme nous l'avons vu dans les sections précédentes, les principaux indicateurs sont le taux de réussite ou d'échec des changements, le délai de rétablissement après des changements échoués et le nombre de tâches non planifiées qui en résulte. Le tableau 3 synthétise les indicateurs d'une gestion inefficace des changements. Le tableau 4 décrit les solutions à mettre en œuvre d'après l'expérience sur le terrain.

Tableau 3 : Problèmes et indicateurs d'une gestion inefficace des changements

Symptômes	Causes sous-jacentes
« Comme de nombreuses grandes organisations recourant à des SI, nous subissions les effets des changements non formalisés. Nous savions quand ces changements survenaient, mais, comme il était difficile d'en faire un suivi, et dans le contexte actuel, axé sur la sécurité, ce n'était pas acceptable. »	Faibles niveaux de service et de disponibilité. Nombre inconnu de changements opérationnels. Taux de changements non contrôlé. Faible taux de réussite du changement (inférieur à 70%). Proportion élevée de tâches non planifiées.
« Dans les scénarios de panne des systèmes de négociation sur le marché obligataire, le service d'assistance était le premier informé. Il faisait remonter l'information jusqu'au management informatique, qui constituait une équipe d'intervention pour procéder aux recherches nécessaires afin de découvrir ce qui s'était passé. »	Si les changements ont échoué, la recherche des causes et la gestion des problèmes représentent plus de 25% de la charge de travail. Un diagnostic inexact aboutit à un faible taux de résolution des problèmes du premier coup (inférieur à 50%).
« On se serait cru au Far West. Les intervenants ne notifiaient pas les changements qu'ils effectuaient, et demandaient encore moins l'autorisation de les réaliser. C'étaient nos statistiques sur la disponibilité qui nous en informaient ! »	En l'absence de contrôles détectifs portant sur les processus de gestion des changements, les performances sont médiocres. En l'absence de contrôles portant sur les changements, les auditeurs ne disposent pas des éléments de preuve de contrôles préventifs et détectifs qui leur auraient permis de confirmer l'efficacité des contrôles.

Tableau 4 : Effets positifs d'une transformation efficace (d'après les résultats effectifs notifiés)

Solution adoptée	Effets positifs
« Nous nous sommes aperçus que les tâches non planifiées étaient le plus souvent dues aux conséquences inattendues de changements. Nous avons donc présenté par écrit la procédure d'autorisation requise pour apporter des changements dans la production et pour consolider les processus. Nous avons également « électrifié la clôture » pour que la procédure de gestion des changements soit respectée. »	Visibilité accrue de la gestion des changements proposés. Les changements opérationnels sont uniquement ceux autorisés par le processus de gestion des changements. Le renforcement du contrôle du taux de changements peut porter le taux de réussite du changement à plus de 95 %, grâce à la visibilité et aux tests.
« Nous avons commencé à instaurer un système imposant réellement à tout le monde de respecter le processus de gestion des changements. Nous avons établi un planning de réunions journalières sur la gestion de la disponibilité, sous la supervision de Kenny, notre vice-président chargé de l'exploitation. Avec l'aide des personnes chargées de la mise en œuvre, Kenny examine tous les changements échoués, et a une discussion avec toute personne qui a contourné la procédure de gestion des changements. Précisons simplement que les changements non autorisés ou sauvages sont, depuis, bien moins fréquents ! »	(Cette entreprise chiffre le coût des pannes à 7 000 USD par minute) Le nombre de changements non autorisés a diminué : on dénombre aujourd'hui « plusieurs changements non autorisées par an », et non plus « plusieurs changements non autorisés par jour ». Étant donné que chaque panne nécessite deux heures de travail pour la reprise de l'activité (estimation prudente), 5 000 heures ont ainsi été économisées sur une base annualisée. Tous les changements sont entièrement formalisés, ce qui permet de commencer par les éliminer comme cause possible d'une panne, et d'exprimer le délai de reprise d'activité non plus en « heures » mais en « minutes ». Pour les 11 pannes survenues au troisième trimestre, on a ainsi pu éviter environ 13 heures d'indisponibilité.
« Nous nous sommes aperçus que les tâches non planifiées étaient le plus souvent dues aux conséquences inattendues de changements. Nous entendions faire mieux respecter nos normes et ne plus passer du temps sur des contrôles détectifs. » « De plus, pour préparer les audits, nous disposions désormais, chaque année, de moins d'une demi-journée par projet, contre, auparavant, quatre semaines ! » « Nous faisions appel à trois équipes différentes pour vérifier la conformité à la législation : une pour la section 404 de la loi Sarbanes-Oxley, une pour la loi Gramm-Leach Billey et une pour la loi *Health Insurance Portability and Accountability*. Lorsque nous avons compris que toutes les trois imposaient une bonne information sur les contrôles relatifs aux changements, nous avons remplacé ces trois équipes par une seule et unique équipe. »	La conformité à la réglementation est aujourd'hui gérée au jour le jour, et non plus dans la précipitation à la dernière minute. Des preuves de l'efficacité des contrôles relatifs aux changements étant produites périodiquement, les auditeurs externes n'ont pas eu à rédiger de lettre de commentaires au management (alors que, l'année précédente, il y avait eu 130 heures de tâches non planifiées et d'honoraires d'audit). La mise en correspondance entre les contrôles des changements et les obligations réglementaires habituelles réduit le nombre d'activités menées en double par différentes équipes. Douze membres du personnel informatique ont été réaffectés dans l'équipe chargée de l'exploitation informatique.
« Outre le fait qu'aucun d'entre nous n'a besoin d'amener son pager à la maison, nous constatons que nous avons davantage de temps à consacrer aux projets planifiés, et que nous n'avons plus besoin de gérer des urgences à tout moment. »	La proportion des tâches non planifiées est tombée de plus de 40 % à 15 %. Le taux de livraison des projets dans les délais est passé de 0 à 60 %. Le directeur des systèmes d'information a chargé le management informatique des grands projets stratégiques pour l'année à venir.

Annexe B : Exemple de programme d'audit

Objectifs de contrôle	Risques	Contrôles	Etapes de travail
Processus de gestion du changement			
Communiquer les objectifs, les besoins, les rôles et les responsabilités.	Erreurs provenant d'une mauvaise compréhension du processus.	Le processus de gestion des changements est défini et communiqué à ceux qui sont impliqués dans le processus, notamment au personnel et aux prestataires de service.	Déterminer si le processus est documenté et l'endroit où il est situé. Déterminer comment les changements apportés au processus sont communiqués. À partir de discussions avec un échantillon des personnes impliquées, évaluer leur compréhension des procédures et des objectifs du processus, ainsi que l'importance de leur rôle dans le processus. Vérifier qu'elles ont accès à la documentation et aux outils nécessaires.
Séparation des tâches			
Déléguer les responsabilités de façon à ce que les erreurs involontaires ou volontaires soient détectées.	Résultats inattendus ou défavorables.	Au minimum, des personnes différentes doivent assumer les responsabilités de l'autorisation des changements et de leur mise en œuvre. Dans l'idéal, la conception et le test des changements seront également effectués par des personnes différentes.	Valider que les changements sont revus et approuvés par un niveau approprié du management. Valider que ceux qui autorisent les changements ne peuvent les mettre en œuvre dans l'environnement de production. Déterminer comment les changements sont testés afin de s'assurer qu'ils fonctionnent comme prévu et ne portent pas atteinte à l'intégrité, la disponibilité ou la confidentialité des données.

GTAG – Annexe B : Exemple de programme d'audit

Objectifs de contrôle	Risques	Contrôles	Etapes de travail
Procédures de gestion du changement			
Veiller à ce qu'un changement réponde aux besoins de l'entreprise.	Résultats inattendus ou défavorables.	Un processus standard et centralisé de traitement de tous les changements existe.	Sélectionner un échantillon des changements et valider le fait que les contrats ont été réalisés, de l'initiation à la mise en œuvre de chaque changement.
Veiller à ce qu'un changement n'affecte pas la disponibilité, l'intégrité et la confidentialité des systèmes et des données.		Tous les changements sont approuvés au niveau approprié du management.	
		Tous les changements sont catégorisés et leur impact est évalué.	
		Tous les changements sont soumis à un test réussi par le personnel informatique et les opérationnels avant d'être mis en production.	
		Tous les changements sont programmés et communiqués aux intéressés avant leur mise en œuvre.	
		Tous les changements relatifs à la production sont associés à un plan de restauration.	
Changements urgents			
Veiller à ce que les besoins de l'entreprise soient satisfaits.	Incapacité à répondre efficacement aux changements urgents devant être réalisés.	Il existe des procédures pour identifier, évaluer et approuver des changements véritablement urgents.	Sélectionner un échantillon de changements urgents et valider qu'ils répondent à la définition d'un changement véritablement urgent, et que les contrôles appropriés ont été exécutés du lancement à la mise en place de chaque changement.
Veiller à ce qu'un changement n'affecte pas la disponibilité, l'intégrité et la confidentialité des systèmes et des données.	Résultats inattendus ou défavorables.	Une revue après la mise en place est réalisée afin de valider que les procédures d'urgence ont été convenablement suivies, et de déterminer l'impact du changement.	

Objectifs de contrôle	Risques	Contrôles	Etapes de travail
Surveillance et *reporting*			
Veiller à ce que le processus fonctionne comme prévu et à sa bonne compréhension par ceux qui sont concernés et impactés.	Problèmes inconnus.	Les indicateurs sont recueillis, analysés et communiqués au management et à ceux impliqués dans le processus	Identifier les indicateurs existants, la façon dont ils sont calculés et qui les calcule. Identifier à qui ils sont communiqués. Déterminer si les indicateurs sont appropriés, complets et exacts. Les indicateurs communs recueillis dans le cadre du processus de gestion des changements comprennent : • Le nombre total de changements sur une période donnée. • Les changements couronnés de succès. • Les changements qui ont échoué. • La réussite ou l'échec des plans de reprise. • Les changements qui ont dévié du processus de gestion des changements. • Le pourcentage de changements urgents. • Le nombre d'interventions de service non programmées sur une période donnée. • Le pourcentage d'interventions non programmées par rapport à l'ensemble des travaux réalisés par le personnel informatique.

A propos du CRIPP

Eléments	Définition
Les dispositions obligatoires. Le respect de ces éléments est exigé et la ligne directrice est élaborée selon le processus requis qui inclut une consultation publique. La conformité aux principes mis en exergue dans les lignes directrices obligatoires est indispensable pour la pratique professionnelle de l'audit interne. Les trois composantes des dispositions obligatoires sont la définition de l'audit interne, le Code de Déontologie et les Normes internationales pour la pratique professionnelle de l'audit interne (Normes).	
Définition	La Définition de l'Audit Interne établit l'objectif fondamental, la nature et le champ d'application de l'audit interne.
Code de déontologie	Le Code de déontologie établit les principes et attentes régissant le comportement des individus et des organisations dans la conduite de l'audit interne. Il décrit les règles minimales de conduite ainsi que des comportements attendus plutôt que des activités spécifiques.
Normes internationales pour la pratique professionnelle de l'audit interne (Normes)	Les Normes sont des principes qui fournissent un cadre pour la réalisation des missions et la promotion de l'audit interne. Elles se composent de Normes de qualification, de Normes de fonctionnement et de Normes de mises en œuvre. Les Normes sont des exigences obligatoires constituées : · de déclarations sur les exigences fondamentales pour la pratique professionnelle de l'audit interne et pour l'évaluation de sa performance. Elles sont internationales et applicables au niveau du service et au niveau individuel. · d'interprétations clarifiant les termes ou les concepts utilisés dans les déclarations. Il est nécessaire de considérer le texte dans sa totalité (c'est-à-dire les déclarations et les interprétations) afin de comprendre et d'appliquer correctement les Normes. Les termes spécifiques utilisés dans les Normes sont explicités dans le Glossaire.

Eléments	Définition
Les dispositions fortement recommandées. La conformité à ces lignes directrices, approuvées par l'IIA, est fortement recommandée. Elles proposent des pratiques pour la mise en œuvre effective de la définition de l'audit interne, du Code de Déontologie de l'IIA et des Normes internationales pour la pratique professionnelle de l'audit interne (Normes). Les trois composantes des dispositions fortement recommandées sont les prises de position, les modalités pratiques d'application (MPA) et les guides pratiques.	
Prises de position	Les Prises de Position aident l'ensemble des parties prenantes, y compris celles qui ne sont pas des professionnels de l'audit interne, à comprendre les principaux enjeux en matière de gouvernance, de risque ou de contrôle. Elles précisent également le rôle et les responsabilités de l'audit interne.
Modalités pratiques d'application (MPA)	Les Modalités Pratiques d'Application fournissent une approche et une méthodologie mais ne précisent pas les processus et les procédures détaillées. Ce sont des lignes directrices qui aident les auditeurs internes dans l'application du Code de déontologie et des Normes ainsi que la promotion des meilleures pratiques. Ces pratiques concernent notamment : • des problématiques internationales, nationales ou spécifiques à certains secteurs d'activité ; • des missions d'audit spécifiques ; • des questions légales ou réglementaires.
Guides pratiques	Les guides pratiques sont des lignes directrices détaillées pour la conduite des activités d'audit interne. Ce sont des processus et des procédures détaillés tels que des outils, des techniques, des programmes, des approches séquentielles (par exemple, des modèles de livrables).

Ce GTAG est un guide pratique du CRIPP.

GTAG®

A PROPOS DE L'INSTITUTE OF INTERNAL AUDITORS

Fondé en 1941, The Institute of Internal Auditors (IIA) est une organisation professionnelle internationale dont le siège mondial se situe à Altamonte Springs, en Floride, aux États-Unis. L'Institute of Internal Auditors est la voix mondiale, une autorité reconnue, un leader incontesté et le principal défenseur de la profession d'auditeur interne. C'est également un acteur de premier plan pour la formation des auditeurs internes. Il est représenté en France par l'IFACI.

A PROPOS DES GUIDES PRATIQUES

Les guides pratiques détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Les guides pratiques s'inscrivent dans le Cadre de référence international des pratiques professionnelles de l'audit interne de l'Institute of Internal Auditors. Ces guides pratiques relèvent de la catégorie des dispositions fortement recommandées. La conformité à ces guides pratiques n'est donc pas obligatoire, mais fortement recommandée. Ces guides ont été officiellement révisés et approuvés par l'IIA.
Le Global Technologies Audit Guide (GTAG) est un type de guide pratique qui aborde, dans un langage courant, une question d'actualité liée à la gestion, au contrôle ou à la sécurité des technologies de l'information.
Pour de plus amples informations sur les documents de référence proposés par l'Institute, vous pouvez consulter notre site Web, www.theiia.org.guidance ou www.ifaci.com.

AVERTISSEMENT

L'Institute of Internal Auditors publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et doit uniquement servir de guide. L'Institute of Internal Auditors vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'Institute dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

COPYRIGHT

Le copyright de ce guide pratique est détenu par l'Institute of Internal Auditors et par l'IFACI pour sa version française. Pour l'autorisation de reproduction, prière de contacter l'Institute of Internal Auditors à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com.

The Institute of Internal Auditors
247 Maitland Avenue, Altamonte Springs
Florida 32701, États-Unis
Téléphone : +1 407 937 1100
Télécopie : 1 407 937 1101
Site Web : www.theiia.org
Courrier électronique : guidance@theiia.org

IFACI
98bis, Boulevard Haussmann
75008 PARIS, France
Téléphone : 01 40 08 48 00
Fax : 01 40 08 48 20
Site Web : www.ifaci.com
Courrier électronique : recherche@ifaci.com

The Institute of Internal Auditors

ifaci
institut français de l'audit et du contrôle internes