GTAG®

GUIDE PRATIQUE D'AUDIT DES TECHNOLOGIES DE L'INFORMATION

Audit des contrôles applicatifs

The Institute of Internal Auditors

Guide pratique d'audit des technologies de l'information (GTAG) 8: Audit des contrôles applicatifs

Auteurs

Christine Bellino, Jefferson Wells

Steve Hunt, Enterprise Controls Consulting LP

Juillet 2007

Copyright © 2007 par l'Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201, États-Unis. Tous droits réservés. 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 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, aucuns résultats juridiques ou comptables. En cas de problèmes juridiques ou comptables, il convient de recourir à l'assistance de professionnels.

GTAG – Table des matières

1. Résumé 1
2. Introduction 2
   - Définition des contrôles applicatifs 2
   - Contrôles applicatifs et contrôles généraux informatiques 2
   - Environnements TI complexes et non complexes 3
   - Avantages des contrôles applicatifs 3
   - Rôle des auditeurs internes 5
3. Évaluation des risques 7
   - Évaluer les risques 7
   - Contrôle des applications : approche de l'évaluation des risques 8
4. Étendue des revues au titre des contrôles applicatifs 9
   - Méthode du processus d'entreprise 9
   - Méthode de l'application unique 9
   - Contrôles d'accès 9
5. Approches de la revue des contrôles applicatifs et autres considerations 10
   - Planification 10
   - Besoin de ressources d'audit spécialisées 10
   - Méthode du processus d'entreprise 10
   - Techniques de documentation 12
   - Tests 13
   - Techniques d'audit assistées par ordinateur 13
6. Annexes 18
   - Annexe A: Contrôles applicatifs courants et propositions de tests 18
   - Annexe B: Exemple de plan d'audit 21
7. Glossaire 26
8. Bibliographie 27
9. Les auteurs 28

Ces dernières années, les organisations du monde entier ont dépensé des milliards pour moderniser leurs systèmes d'applications ou en installer de nouveaux, et ce pour différentes raisons : objectifs tactiques (mise en conformité « an 2000 », par exemple) ou activités stratégiques (utilisation de la technologie comme facteur de différenciation de l'entreprise sur le marché). Une application ou un système d'applications est un logiciel qui permet d'exécuter des tâches en recourant directement aux capacités de l'ordinateur. Selon le *GTAG 4* publié par l'IIA (The Institute of Internal Auditors), ces systèmes peuvent se classer en deux catégories : applications transactionnelles et applications de support.

Les applications transactionnelles traitent les données à l'échelle de l'organisation :

- Elles enregistrent la valeur des transactions de l'entreprise en termes de débits et de crédits.
- Elles servent à archiver les données financières, opérationnelles et réglementaires.
- Elles permettent diverses formes de communication financière et managériale, notamment le traitement des commandes, des factures clients, des factures fournisseurs et des écritures de journaux.

SAP R/3, PeopleSoft et Oracle Financials, qu'on qualifie souvent de progiciels de gestion intégrés (ERP – enterprise resource planning), ainsi que d'innombrables logiciels non-ERP, sont des exemples de systèmes de traitement des transactions. Ils fonctionnent sur la base d'une logique programmée et, dans de nombreux cas, en complément des tables configurables qui stockent les règles uniques de l'organisation pour l'exploitation et le traitement.

Les applications de support sont, quant à elles, des logiciels spécialisés qui facilitent les activités de l'organisation : programmes de messagerie électronique, logiciels de télécopie, d'imagerie documentaire et de conception. Cependant, ces applications ne gèrent généralement pas les transactions.[1]

Tout comme n'importe quelle technologie supportant les processus d'entreprise, les applications transactionnelles et de support peuvent engendrer des risques pour l'organisation. Ceux-ci proviennent de la nature même de la technologie et des équipements, de la gestion et de l'utilisation du système. Avec les systèmes de traitement transactionnel, les risques qui ne font pas l'objet de mesures de correction appropriées peuvent compromettre l'intégrité, l'exhaustivité, la rapidité d'exécution et la disponibilité des données financières ou opérationnelles. De plus, quelle que soit l'application utilisée, les processus eux-mêmes présentent un risque inhérent. C'est pourquoi nombre d'organisations associent des contrôles automatisés et manuels pour gérer ces risques dans les applications transactionnelles et de support. L'efficacité de la gestion du risque dépend toutefois directement des éléments suivants :

- L' appétence pour le risque ou la tolérance au risque de l'organisation.
- La rigueur de l'évaluation du risque lié à l'application.
- Les processus concernés.
- L'efficacité des contrôles généraux informatiques (CGTI).
- La conception et l'étendue actuelle de l'efficacité opérationnelle des activités de contrôle.

L'une des approches les plus efficientes et présentant le meilleur rapport coût-efficacité utilisées par les organisations pour gérer ces risques consiste à recourir à des contrôles intrinsèques ou intégrés (par exemple, une triple concordance des factures fournisseurs) dans les applications transactionnelles ou de support ainsi qu'à des contrôles configurables (par exemple, les tolérances relatives aux factures fournisseurs). Ces contrôles, généralement qualifiés de contrôles applicatifs, concernent l'étendue des différents processus ou systèmes d'applications, dont l'édition des données, la séparation des fonctions, la balance des totaux de contrôle, la journalisation des transactions et les rapports d'erreurs.[2]

Les responsables de l'audit interne et leurs équipes doivent par ailleurs impérativement comprendre la différence entre les contrôles applicatifs et les contrôles généraux informatiques (CGTI). Ces derniers s'appliquent à l'ensemble des composants, processus et données des systèmes de l'organisation,[3] tandis que les contrôles applicatifs sont spécifiques à un programme ou à un ensemble de programmes (système) qui soutient un processus d'entreprise donné. La section de ce chapitre consacrée aux contrôles applicatifs et aux contrôles généraux informatiques reviendra plus en détail sur ces deux types de contrôles.

En raison de l'importance des contrôles applicatifs pour les stratégies de gestion des risques, les responsables de l'audit interne et leurs équipes doivent élaborer et réaliser périodiquement des audits de ces contrôles afin de vérifier qu'ils sont bien conçus et fonctionnent correctement. Le présent guide a donc pour objectif de donner aux responsables de l'audit interne des informations sur les aspects suivants :

1. Définition et avantages des contrôles applicatifs.
2. Rôle des auditeurs internes.
3. Exécution d'une évaluation des risques.
4. Délimitation de l'étendue de la revue des contrôles applicatifs.
5. Approches de la revue des applications et autres considérations.

Nous présentons en outre dans ce guide une liste des contrôles applicatifs courants et un exemple de plan d'audit.

1 *GTAG 4 : Management de l'audit des systèmes d'information*, p. 5.

2 *GTAG 1 : Les contrôles des technologies de l'information*, p. 3.

3 *GTAG 1 : Les contrôles des technologies de l'information*, p. 3.

Définition des contrôles applicatifs

Les contrôles applicatifs portent sur l'étendue des différents systèmes d'applications ou processus d'entreprise, dont les éditions de données, la séparation des fonctions, la balance des totaux de contrôle, la journalisation des transactions et les rapports d'erreurs. Leur objectif est de veiller à ce que :

- Les données d'entrée soient exactes, complètes, autorisées et correctes.
- Les données soient traitées conformément aux objectifs et dans un délai acceptable.
- Les données stockées soient exactes et complètes.
- Les données de sortie soient exactes et complètes.
- Un enregistrement du processus soit conservé ; il permet de suivre la progression des données depuis leur entrée jusqu'à leur stockage et à leur sortie éventuelle.[4]

Plusieurs types de contrôles applicatifs existent :

- **Les contrôles des données en entrée** – Ces contrôles servent principalement à vérifier l'intégrité des données entrées dans une application, que les données aient été entrées directement par le personnel de l'entreprise, à distance par un partenaire commercial ou via une application ou interface Web. La vérification de la saisie des données intègre la vérification que les limites spécifiées ne sont pas dépassées.
- **Les contrôles sur le traitement** – Ces contrôles constituent un moyen automatisé de faire en sorte que le traitement soit complet, exact et autorisé.
- **Les contrôles des données en sortie** – Ces contrôles portent sur ce qu'il advient des données et doivent rapprocher les résultats en sortie avec le résultat escompté, en confrontant les données de sortie aux données entrées.
- **Les contrôles d'intégrité** – Ces contrôles surveillent les données en cours de traitement et les données stockées afin de veiller à ce qu'elles restent cohérentes et correctes.
- **La piste de contrôle de gestion** – La trace des opérations réalisées, souvent appelée piste d'audit, permet à l'encadrement d'identifier les transactions et les événements enregistrés en suivant les transactions depuis leur entrée jusqu'à leur sortie et en sens inverse. Ces contrôles permettent également de vérifier l'efficacité des autres contrôles et de repérer les erreurs au plus près possible de leur source.[5]

Les contrôles applicatifs se répartissent en contrôles préventifs et contrôles de détection. Même si ces deux catégories se retrouvent dans une même application reposant sur une logique programmée ou configurable, les contrôles préventifs préviennent, comme leur nom l'indique, la survenue d'une erreur au sein d'une application. C'est par exemple le rôle d'une routine de validation des données en entrée, qui vérifie que les données entrées sont cohérentes avec la logique du programme qui leur est associé et n'autorise la sauvegarde que des données correctes. Les données incorrectes ou invalides sont quant à elles rejetées au moment de la saisie.

Les contrôles de détection détectent, comme leur nom l'indique également, les erreurs sur la base d'une logique de programme prédéfinie. Ainsi, un contrôle de détection peut mettre au jour un écart favorable ou défavorable entre le prix figurant sur la facture du fournisseur et celui du bon de commande.

Les contrôles applicatifs, en particulier ceux de détection, servent également à faciliter les contrôles manuels. Les données ou les résultats d'un contrôle de détection peuvent permettre d'alimenter un contrôle de surveillance. Ainsi, le contrôle de détection décrit au paragraphe précédent peut mettre en évidence toute variation du prix d'achat grâce à un programme qui énumère ces exceptions dans un rapport. L'examen par la direction de ces exceptions peut alors être considéré comme un contrôle de surveillance.

Contrôles applicatifs et contrôles généraux informatiques

Il est important que les responsables de l'audit interne et leurs équipes comprennent les relations et les différences entre les contrôles applicatifs et les contrôles généraux informatiques (CGTI). À défaut, la revue des contrôles applicatifs risque de ne pas être correctement délimitée, ce qui aura une incidence sur la qualité et l'étendue de l'audit.

Les contrôles généraux informatiques s'appliquent à tous les composants, processus et données des systèmes d'une organisation, ou d'un environnement de systèmes.[6] Ils ont pour objectif de veiller au développement et à la mise en œuvre appropriés des applications, à l'intégrité des fichiers de programmes et de données, ainsi que des opérations informatiques.[7] Les CGTI les plus courants sont les suivants :

- Contrôles d'accès logique à l'infrastructure, aux applications et aux données.
- Contrôles du cycle de développement des système d'applications informatisées.
- Contrôles sur la gestion des changements dans les programmes.
- Contrôles de sécurité physique sur le centre de traitement informatique.
- Contrôles de sauvegarde et de restauration des systèmes et des données.
- Contrôles de l'exploitation.

4, 5 *GTAG 1: Les contrôles des technologies de l'information*, p. 8.

6 *GTAG 1: Les contrôles des technologies de l'information*, p. 3

7 ISACA, IS Auditing Guideline — Application Systems Review, Document G14, p. 3.

Étant donné que les contrôles applicatifs concernent les transactions et les données relatives à chaque système d'applications informatisées, ils sont spécifiques à chaque application. Leur objectif est de veiller à l'exhaustivité et à l'exactitude des données enregistrées, ainsi qu'à la validité de chaque entrée enregistrée après traitement par le programme.[8] Autrement dit, ces contrôles sont spécifiques à une application donnée, contrairement aux CGTI. Ils servent généralement à :

- Déterminer si le traitement des bons de commande tient compte des plafonds de crédit des clients.
- Veiller à ce que les biens et les services soient toujours achetés sur la base d'un bon de commande validé.
- Veiller à la séparation des fonctions en regard des responsabilités définies.
- Vérifier que les marchandises reçues sont comptabilisées à la réception.
- Veiller à ce que l'amortissement des immobilisations corporelles soit rigoureusement enregistré dans l'exercice approprié.
- Déterminer s'il existe un triple rapprochement entre le bon de commande, le bordereau de réception et la facture fournisseur.

En outre, il importe que les responsables de l'audit interne examinent à quel point la direction peut se fier aux contrôles applicatifs pour gérer les risques. Ce niveau de confiance dépend directement de la conception et de l'efficacité des CGTI. En d'autres termes, si ces contrôles ne sont pas mis en œuvre, ou ne fonctionnent pas correctement, l'organisation ne pourra pas s'y fier pour gérer les risques. Ainsi, si les CGTI qui portent sur les changements dans les programmes ne sont pas efficaces, des modifications non autorisées, non approuvées et non testées peuvent être introduites dans l'environnement de production, ce qui risque de compromettre l'intégrité globale des contrôles applicatifs.

Environnements TI complexes et non complexes

La sophistication (ou la complexité) de l'environnement informatique d'une organisation exerce une incidence directe sur l'exposition globale aux risques et les stratégies de gestion afférentes. Les organisations qui sont dotées d'une infrastructure informatique complexe présentent les caractéristiques suivantes :

- Les applications, bases de données et systèmes existants subissent des changements fréquents.
- Elles développent en interne le code source des logiciels critiques.
- Elles adaptent les progiciels de série à leurs besoins.
- Elles déployent en production des applications pré-packagées, des changements et des programmes.[9]

Les organisations dont l'environnement informatique est peu complexe présentent, elles, les caractéristiques suivantes :

- Elles modifient peu l'environnement informatique existant.
- Elles peuvent mettre en place, en cours d'exercice, une application financière pré-packagée sans apporter de changements significatifs.
- Elles n'utilisent que des options configurables par les utilisateurs qui ne modifient pas significativement le fonctionnement de l'application.
- Elles n'ont pas de projets de développement informatique.[10]

Comme le soulignent ces différences, il existe une corrélation directe entre la complexité des applications transactionnelles et de gestion, et la disponibilité, l'utilisation et la confiance accordée aux contrôles applicatifs intrinsèques et configurables. En d'autres termes, une infrastructure informatique peu complexe ne présentera certainement pas autant de contrôles applicatifs intrinsèques ou configurables pour la gestion des risques. Le degré de complexité des applications transactionnelles et de gestion conditionnera donc la délimitation, la mise en œuvre, le degré d'effort et les connaissances nécessaires pour réaliser un examen des contrôles applicatifs, ainsi que le niveau de l'activité de conseil que pourront apporter les auditeurs internes.

Avantages des contrôles applicatifs

Le recours aux contrôles applicatifs peut être utile sur plusieurs plans. Nous allons en décrire les principaux.

Fiabilité

Les contrôles applicatifs sont plus fiables que les contrôles manuels si l'on évalue le potentiel d'erreurs de contrôle dues à l'intervention humaine. Une fois qu'un contrôle applicatif est mis en place, et que les changements apportés à l'application, à la base de données ou à la technologie sont minimes, l'organisation peut s'appuyer sur ce contrôle jusqu'à ce qu'un changement soit introduit.

En outre, un contrôle applicatif continuera d'être efficace si les CGTI qui ont un impact direct sur sa nature programmatique, fonctionnent également avec efficacité. Cela se vérifie en particulier pour les contrôles relatifs aux changements apportés aux programmes et à la séparation des fonctions des administrateurs informatiques.

8 ISACA, IS Auditing Guideline — Application Systems Review, Document G14, p. 3.
9 The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's), *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, Vol. III, p. 61.
10 COSO's, *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, Vol. III, p. 56.

En conséquence, l'auditeur pourra se contenter de tester le contrôle une seule fois, et non plusieurs, pendant la période de tests.

Analyse comparative (benchmarking)

Selon l'annexe B de la norme n° 5 du Public Company Accounting Oversight Board (PCAOB) des États-Unis, portant sur l'audit du contrôle interne de la communication financière intégré à un audit des états financiers, on peut utiliser l'analyse comparative des contrôles applicatifs, car ces contrôles ne subissent généralement pas de défaillances dues à l'erreur humaine. Si les contrôles généraux qui servent à encadrer les changements apportés aux programmes, l'accès aux programmes et la réalisation des opérations informatiques sont efficaces et régulièrement testés, l'auditeur peut en conclure que le contrôle de l'application est efficace sans avoir à réitérer le test du contrôle de l'année précédente. C'est particulièrement vrai si l'auditeur vérifie que les contrôles applicatifs n'ont pas changé depuis le dernier test qu'il a effectué.[11]

En outre, la nature et la quantité des preuves que l'auditeur doit obtenir pour vérifier que le contrôle n'a pas changé peuvent varier en fonction des circonstances, telle que la solidité des contrôles des changements dans les programmes de l'organisation.[12] En conséquence, lorsqu'il recourt à l'analyse comparative pour un contrôle donné, l'auditeur doit tenir compte de l'action des fichiers, tables, données et paramètres connexes sur la fonctionnalité des contrôles applicatifs. Ainsi, une application qui calcule les intérêts créditeurs peut tout à fait être tributaire du maintien de l'intégrité de la grille de taux utilisée par le calcul automatisé.[13]

L'auditeur doit considérer le bien-fondé de l'utilisation de l'analyse comparative pour un contrôle automatisé, en tenant compte de la fréquence à laquelle l'application est modifiée. Par conséquent, plus les changements de programmes sont fréquents, moins cette stratégie est pertinente. En outre, l'auditeur doit évaluer la fiabilité de l'information relative aux changements apportés au système. Ainsi, s'il y a peu ou pas d'informations ou de rapports vérifiables concernant les changements apportés à l'application, à la base de données ou à la technologie sous-jacente, l'analyse comparative se justifie moins pour le contrôle de l'application.

Cependant, l'analyse comparative est particulièrement efficace lorsque les entreprises utilisent des progiciels de série qui n'autorisent pas de développement ou de modification des codes sources. Dans ces cas, l'organisation ne doit pas s'arrêter au seul changement de code. En effet, dans une application complexe, comme un logiciel SAP ou Oracle Financials, il est possible de modifier, de désactiver ou d'activer un contrôle facilement et sans changement de code.

Enfin, les changements de paramètres et de configuration exercent un impact significatif sur la plupart des contrôles applicatifs. Ainsi, il est facile de manipuler les niveaux de tolérance pour désactiver les contrôles concernés, tandis que les contrôles sur les autorisations d'achats peuvent être manipulés lorsque leur stratégie d'autorisation est modifiée, et là encore, sans qu'il soit nécessaire de changer le code.

Les organisations doivent évaluer chaque contrôle applicatif afin de déterminer jusqu'où l'analyse comparative peut être efficace. Une fois que la référence n'est plus efficace, il importe de rétablir la base de comparaison en testant à nouveau le contrôle. Les auditeurs doivent se poser les questions suivantes lorsqu'ils déterminent si un contrôle applicatif donné fonctionne toujours efficacement et tel qu'il a été étalonné à l'origine :

- Le niveau de risques associé au processus de gestion et le contrôle applicatif ont-ils été modifiés depuis l'origine ? (i.e. le processus de gestion engendre-t-il des risques substantiellement plus importants qu'au départ, en termes de conformité aux règles de communication financière, de paramètres opérationnels et de respect de la réglementation ?)
- Les contrôles généraux informatiques sont-ils efficaces, notamment les contrôles portant sur l'accès logique, la gestion des changements, le développement ou l'acquisition de systèmes et les opérations machine ?
- L'auditeur peut-il comprendre pleinement les effets éventuels des changements sur les applications, les bases de données ou la technologie qui contiennent les contrôles applicatifs ?
- Des changements ont-ils été introduits dans le processus de gestion tributaire du contrôle applicatif, qui pourraient avoir une incidence sur la conception ou l'efficacité du contrôle ?

Économies de temps et réduction de coûts

Les contrôles applicatifs prennent généralement moins de temps à être réalisés que les contrôles manuels. En effet, la taille des échantillons de ces derniers dépend de la fréquence des contrôles (journalière, hebdomadaire, mensuelle, trimestrielle, annuelle), contrairement à celle des contrôles applicatifs (ces derniers fonctionnent efficacement ou non). En outre, les contrôles applicatifs sont généralement testés une seule fois, tant que les contrôles généraux informatiques sont efficaces. En conséquence, tous ensemble, ces facteurs peuvent réduire considérablement le nombre d'heures nécessaires pour évaluer le contrôle d'une application, par rapport à un contrôle manuel.

11, 12 PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraphe B29.

13 PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraphes B29 - 30.

Rôle des auditeurs internes

Savoir

Aujourd'hui, les organisations utilisent davantage les contrôles applicatifs que par le passé pour gérer les risques, en raison de l'efficience naturelle, du bon rapport coût-efficacité et de la fiabilité de ces contrôles. Par tradition, tous les contrôles informatiques étaient testés par un auditeur informaticien expérimenté, tandis que les contrôles liés aux données financières, aux paramètres opérationnels ou au respect de la réglementation l'étaient par un auditeur non spécialisé dans les systèmes d'information. Même si la demande d'auditeurs spécialisés dans l'informatique s'est substantiellement accrue ces dernières années, et si cette tendance devrait se poursuivre, tous les auditeurs internes doivent être capables d'évaluer, de manière exhaustive, tous les contrôles de processus d'entreprise.

De plus, selon l'ouvrage *Normes internationales pour la pratique de l'audit interne (Normes)*, publié par l'IIA, et en particulier les Normes 1220 et 1210.A3, « les auditeurs internes doivent apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent »,[14] et « posséder une bonne connaissance des principaux risques et contrôles liés aux technologies de l'information et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés. Toutefois, chaque auditeur interne n'est pas censé posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique ».[15] Autrement dit, chaque auditeur interne doit connaître les risques et les contrôles liés à l'informatique, et être à même de déterminer si les contrôles applicatifs mis en œuvre sont conçus et fonctionnent correctement pour gérer les risques financiers, opérationnels et liés au respect de la réglementation.

Conseils ou assurance

Parallèlement aux services d'assurance traditionnels, la fonction d'audit interne peut, par ses missions de conseil, apporter de la valeur à une organisation. Ces missions peuvent revêtir diverses formes et porter sur n'importe quel domaine ou fonction. Ainsi, il peut s'agir d'aider le personnel de l'organisation à concevoir des contrôles pendant la mise en œuvre, ou la modernisation, des applications transactionnelles ou de support.

Malheureusement, nombre d'auditeurs internes n'aident pas la direction à comprendre l'évolution des risques lorsque l'organisation introduit une nouvelle application transactionnelle ou de support, ou procède à une mise à niveau majeure. Dans la grande majorité des cas, cette attitude n'est pas due à un manque de volonté ou d'attention, mais au fait que les auditeurs internes ne sont pas au courant des activités de développement des systèmes, ou que la direction ne souhaite pas les y associer.

Qu'elle qu'en soit la raison, le responsable de l'audit interne doit veiller à ce que les auditeurs internes soient informés de ces activités, et mettre en avant les qualités, les connaissances et le savoir-faire des auditeurs internes lorsqu'il s'agit de procurer à l'organisation des services de gestion des risques. Il importe par ailleurs que les auditeurs internes participent au développement des systèmes, afin qu'ils contribuent à la gestion du risque que présente l'application, et qu'ils s'assurent que des contrôles intrinsèques et configurables fonctionnent efficacement, avant la mise en service de l'application en question. À défaut, il reviendra nettement plus cher a posteriori, de mener un examen,, de déceler les faiblesses et d'installer des contrôles. Les paragraphes ci-dessous présentent des exemples de la façon dont les auditeurs internes peuvent créer de la valeur lors des activités de développement de systèmes, en donnant des conseils sur les contrôles applicatifs.

Évaluation indépendante des risques

À chaque fois qu'une application transactionnelle ou de support, nouvelle ou considérablement améliorée, est mise en œuvre, deux choses peuvent se produire. Premièrement, nombre des contrôles automatisés ou manuels qui étaient en place pour gérer les risques dans l'ancien environnement, devront être remplacés par de nouveaux contrôles. Deuxièmement, le profil de risque de l'application peut changer ; autrement dit, la nouvelle application comportera de nouveaux risques intrinsèques (par exemple, du fait de sa configuration) et les risques ne peuvent pas être atténués au sein de l'application elle-même, ce qui nécessite d'utiliser des contrôles manuels. Par conséquent, s'ils n'en sont pas à l'origine, les auditeurs internes peuvent au moins contribuer aux efforts de l'organisation pour comprendre comment les risques vont évoluer avec l'arrivée de la nouvelle application. Les auditeurs internes sont en effet compétents pour fournir ce niveau de service et se trouvent dans une position unique en raison de leur indépendance par rapport à la direction.

Pour que les auditeurs puissent procurer ce service, ainsi que les autres énumérés ci-dessous, ils doivent posséder une connaissance suffisante de l'application en cours de développement. Le nombre et la catégorie d'auditeurs qui ont besoin de ce type de connaissances dépend de l'application en cours de développement, de l'ampleur de son impact sur les processus de l'entreprise, de la taille de l'organisation et du nombre d'entités ou de domaines vérifiables, une fois que l'application aura été pleinement déployée dans toute l'organisation. Les responsables de l'audit interne ont à leur disposition plusieurs stratégies différentes pour faire en sorte que leur niveau de connaissance soit suffisant, et notamment recourir à des manuels, des cours en ligne, des séances de formation et des consultants extérieurs.

14 Norme 1220 de l'IIA : Conscience professionnelle.

15 Norme 1210.A3 de l'IIA.

Conception des contrôles

Lors de l'introduction d'un nouveau système ou de la modernisation significative d'un système existant, les auditeurs internes peuvent apporter un autre service de valeur en élargissant leur évaluation des risques de façon indépendante. Plus précisément, ils peuvent aider la direction à concevoir les contrôles destinés à limiter les risques identifiés pendant l'évaluation des risques. Les auditeurs internes assignés à cette tâche doivent faire partie intégrante de l'équipe de mise en œuvre. Par conséquent, les tâches, le temps requis et le nombre d'auditeurs internes nécessaires pour concevoir les contrôles applicatifs doivent être intégrés au plan du projet global.

Il est important que les responsables de l'audit interne désignent le bon nombre d'auditeurs, mais aussi des auditeurs qui possèdent les compétences et le savoir-faire nécessaires pour mener à bien leur mission. Les auditeurs sont souvent affectés à plein temps sur le projet, dans ce cas, les responsables de l'audit interne doivent décharger le personnel retenu pour ce projet de ses tâches habituelles et les confier à d'autres auditeurs internes. Les auditeurs affectés au projet pourront ainsi s'y consacrer pleinement. De plus, les auditeurs internes qui travaillent sur le projet doivent rendre compte au chef de projet pendant le cycle d'introduction du système.

Lorsque les auditeurs ont pour mission d'aider la direction à concevoir des contrôles applicatifs, les responsables de l'audit interne doivent noter que l'indépendance et l'objectivité peuvent être altérées si des missions d'assurance sont réalisées dans l'année qui suit une mission de conseil. De plus, il convient de prendre des mesures visant à minimiser les effets de cette altération : affecter différents auditeurs à chacune des missions, s'assurer de l'indépendance de l'encadrement et de la supervision des auditeurs, définir des responsabilités distinctes concernant les résultats du projet et déceler une altération éventuelle des capacités de l'auditeur. Enfin, il est de la responsabilité de la direction d'accepter et de mettre en œuvre les recommandations.[16] En d'autres termes, si un auditeur interne participe à la conception des contrôles liés à une application transactionnelle ou de support, il ne doit pas participer à l'évaluation de l'efficacité opérationnelle de ces contrôles au cours des 12 mois qui suivent l'achèvement de la mission de conseil.

Formation

Les auditeurs internes ne se contentent pas de contrôler les applications, ils peuvent aussi sensibiliser l'encadrement aux aspects suivants :

- Évolution de l'exposition aux risques ésultant de l'introduction de la nouvelle application.
- Faiblesses connues des contrôles intrinsèques des applications en cours de développement.
- Solutions envisageables pour réduire les faiblesses identifiées.
- Différents services que les auditeurs peuvent apporter à la direction lors du développement de systèmes.

Test des contrôles

Que l'équipe chargée de la mise en œuvre ait conçu et déployé ces contrôles en fonction de l'évaluation des risques, voire sans procéder à une telle évaluation, les auditeurs internes peuvent se révéler utiles en effectuant une évaluation indépendante des contrôles applicatifs. Ce test déterminera si les contrôles sont bien conçus, et fonctionneront efficacement une fois l'application en service. Si certains contrôles ne sont pas bien conçus, ou ne sont pas susceptibles de fonctionner correctement, les auditeurs doivent en avertir la direction et lui formuler des recommandations pour éviter la survenance, lorsque l'application sera pleinement déployée, de risques non pris en compte.

Examen des contrôles applicatifs

En fonction de leur importance pour l'environnement général de contrôle, il est nécessaire de procéder à un examen régulier des contrôles, pour les applications transactionnelles et de support. La fréquence, l'étendue et la profondeur de ces examens varient en fonction du type d'application, et de son impact sur la communication financière, le respect de la réglementation et les paramètres opérationnels, ainsi que sur la confiance que place l'organisation dans les contrôles présents dans l'application, pour la maîtrise des risques.

16 Norme 1130.C1 de l'IIA

Évaluer les risques

Lorsqu'il élabore le plan d'évaluation des risques, l'auditeur doit utiliser des techniques spécifiques pour identifier les vulnérabilités critiques liées à la communication financière de l'entreprise, ainsi que les impératifs opérationnels et de conformité aux règles. Ces techniques portent sur :

- La nature, le calendrier et l'étendue de la revue.
- Les fonctions critiques de l'entreprise tributaires des contrôles applicatifs.
- Le temps et les ressources qui seront consacrés à cet examen.

De plus, les auditeurs doivent se poser quatre questions essentielles lorsqu'ils déterminent la portée requise par la revue :

1. Quels sont les principaux risques qui doivent être évalués et gérés pour l'organisation, en fonction des principales préoccupations du comité d'audit,et sachant qu'il faut aussi tenir compte de l'opinion de la direction ?
2. Quels sont les processus de l'entreprise qui sont exposés à ces risques ?
3. Quels sont les systèmes utilisés pour mettre en œuvre ces processus ?
4. Où sont mis en œuvre les processus ?

Lors de l'identification des risques, les auditeurs peuvent juger utile de recourir à une approche descendante *(top-down)* afin de déterminer les applications à inclure dans l'examen des contrôles, ainsi que les tests à effectuer. Par exemple, la figure 1 présente une méthode efficace pour identifier les risques liés à la communication financière et déterminer l'étendue de la revue. Veuillez noter que cette illustration ne constitue pas l'unique manière d'effectuer toutes les évaluations des risques.

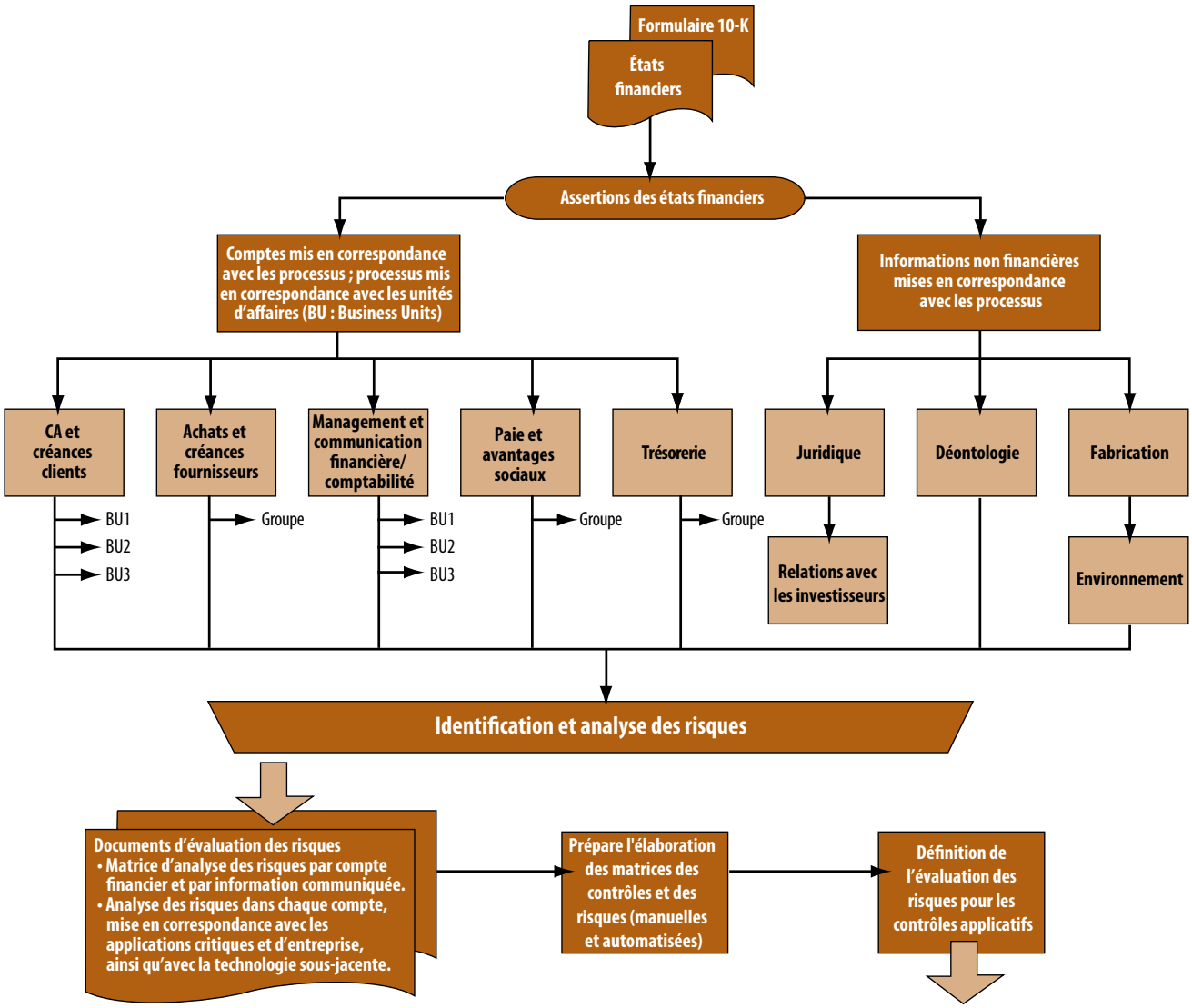


Figure 1. Analyse des risques liés à la communication financière.

Contrôle des applications : approche de l'évaluation des risques

Pour ajouter de la valeur aux activités d'évaluation des risques liés aux contrôles applicatifs dans l'organisation, les auditeurs internes :

- définissent l'univers des applications, des bases de données et de la technologie utilisée qui recourent aux contrôles applicatifs, et synthétisent le risque et les contrôles à l'aide des matrices des risques et des contrôles décrites lors du processus d'évaluation des risques,
- définissent les facteurs de risque associés à chaque contrôle applicatif, à savoir :
  - Les contrôles primaires des applications (c.-à-d. essentiels).
  - L'efficacité de la conception des contrôles applicatifs.
  - Des applications ou des bases de données pré-packagées ou développées. Applications pré-packagées ou développées non configurées, par opposition aux applications maison ou achetées fortement configurées.
  - Si l'application supporte plus d'un processus d'entreprise critique ?
  - La classification des données traitées par l'application (par ex. financières, privées ou confidentielles).
  - La fréquence des changements apportés aux applications ou aux bases de données.
  - La complexité des changements (changements dans les tables ou dans les codes source des programmes).
  - L'impact financier des contrôles applicatifs.
  - L'efficacité des contrôles généraux informatiques intégrés dans l'application (par ex., gestion du changement, sécurité logique et contrôles opérationnels).
  - L'historique de l'audit des contrôles.
- pèsent tous les facteurs de risque de manière à déterminer quels sont ceux qui doivent être davantage pondérés que les autres.
- déterminent l'échelle qui convient au classement de chaque risque lié aux contrôles applicatifs, en envisageant des échelles qualitatives et quantitatives, telles que :
  - Risque de contrôle faible, moyen ou élevé.
  - Échelles numériques reposant sur des informations qualitatives (par ex., 1 = risque à faible impact, 5 = risque à fort impact ; 1 = contrôle poussé et 5 = contrôle insuffisant).
  - Échelles numériques reposant sur des informations quantitatives (par ex., 1 = < 50 000 dollars et 5 = > 1 000 000 dollars)
- effectuent l'évaluation des risques et classent toutes les catégories de risque.
- évaluent les résultats de l'évaluation des risques.
- élaborent un plan de revue des risques fondé sur cette évaluation et sur le classement des catégories de risque.

La figure 2 montre un exemple d'évaluation des risques liés aux contrôles applicatifs recourant à une échelle de classement qualitative (1 = risque ou impact faible et 5 = risque ou impact fort). On calcule les scores composites de chaque application en multipliant chaque facteur de risque par sa pondération dans l'application et additionnant les totaux. Par exemple, on a obtenu le score composite de 375 sur la première ligne en multipliant le chiffre correspondant au facteur de risque par le score spécifique à l'application [(20 x 5) + (10 x 1) + (10 x 5) +…]. Pour cet exemple, l'auditeur peut décider que la revue des contrôles applicatifs inclura toutes les applications affichant un score supérieur ou égal à 200.

Pondération des facteurs de risque									
	20	10	10	10	10	10	15	15	
Application	L'application contient des contrôles primaires	Efficacité de la conception des contrôles applicatifs	Pré-packagées ou développées	L'application supporte plus d'un processus critique	Fréquence des changements	Complexité des changements	Impact financier	Efficacité des contrôles généraux informatiques	Score composite
APPA	5	1	5	5	3	3	5	2	375
APPB	1	1	2	1	1	1	4	2	170
APPC	5	2	2	1	5	5	5	2	245
APPD	5	3	5	1	5	5	5	2	395
APPE	5	1	1	1	1	1	3	2	225

Figure 2. Exemple d'une évaluation des risques liés aux contrôles applicatifs.

Voici deux méthodes permettant de déterminer l'étendue de la revue de contrôles applicatifs. Les auditeurs internes ne doivent pas oublier que l'étendue, la profondeur, l'approche et la fréquence de la revue dépendent des résultats de l'évaluation des risques et de la disponibilité des ressources d'audit interne. Quelle que soit la méthode choisie pour déterminer l'étendue de la revue, cette dernière doit englober une évaluation des contrôles sur les entrées, le traitement et les sorties de données.

Méthode du processus d'entreprise

La méthode du processus d'entreprise (*business process*) est une approche de revue descendante (*top-down*), utilisée lorsqu'on veut évaluer les contrôles applicatifs présents dans tous les systèmes qui supportent un processus donné. Au cours des dernières années, cette méthode a gagné en importance au point de devenir la plus courante et la plus largement employée. Cette popularité s'explique principalement par une augmentation de l'utilisation des applications transactionnelles ERP, et par le recul des applications « best of breed » autonomes (« meilleure du genre »).

Lorsqu'ils utilisent la méthode du processus d'entreprise dans un univers non-ERP, les auditeurs internes doivent intégrer dans l'étendue de la revue toutes les applications utilisées par l'entreprise qui participent au processus analysé, car il s'agit en général de systèmes autonomes. En d'autres termes, l'auditeur doit y inclure les applications distinctes qui forment les différentes composantes du cycle du processus d'entreprise. Il peut alors identifier les interfaces entrantes et sortantes au sein des applications analysées, et achever de déterminer l'étendue de la revue.

Le recours à la méthode du processus d'entreprise afin de définir l'étendue de la revue des contrôles applicatifs diffère dans le cas d'applications intégrées, comme dans un système ERP, car les processus sont alors communs à de multiples modules. Prenons le cas du processus allant de la demande d'achat au paiement des fournisseurs (procure-to-pay). Dans un environnement ERP, ce processus englobe généralement les modules ou les sous-applications achat, gestion des stocks, grand livre général et créances fournisseurs au sein du système ERP. Il importe donc de bien comprendre les modules qui composent le processus d'entreprise, ainsi que la manière dont les données sont gérées et circulent d'un module à l'autre.

Méthode de l'application unique

L'auditeur utilise la méthode de l'application unique lorsqu'il veut examiner les contrôles applicatifs au sein d'une seule application, ou d'un seul module, au lieu de s'intéresser à l'ensemble du processus d'entreprise. Comme nous l'avons expliqué précédemment, il s'agit de la méthode la plus efficace pour déterminer l'étendue de la revue dans un environnement non-ERP, ou non intégré, car l'auditeur peut plus facilement isoler l'application (c'est-à-dire inclure l'application dans la revue). En d'autres termes, l'auditeur peut identifier les données entrantes et sortantes, car ces données et les règles de traitement afférentes sont contenues dans une seule application, et cette dernière est la seule à les utiliser.

Cependant, dans un environnement ERP ou intégré, la mise en œuvre de cette méthode n'est pas souhaitable. Bien qu'il puisse paraître relativement facile d'isoler le module d'un système ERP ou d'un système transactionnel intégré, cette tâche peut en réalité se révéler assez difficile. En effet, il peut arriver que de multiples données entrent et sortent d'un module, et il serait vain de s'efforcer de les identifier. L'emploi de l'approche par module risque donc d'aboutir à un examen inadéquat, tandis que la méthode du processus d'entreprise se prête davantage à un tel environnement.

Contrôles d'accès

Quelle que soit la méthode choisie pour déterminer l'étendue des contrôles applicatifs, il convient de procéder à un examen périodique des contrôles d'accès logiques aux modules ou aux applications. Dans la plupart des cas, les droits d'accès utilisateurs et administrateurs (lire, écrire et supprimer) sont conçus sur la base des outils et de la plateforme de sécurité inhérents à l'application. Les stratégies utilisées pour définir quels droits d'accès logique attribuer aux utilisateurs peuvent être dictées par le besoin pour les utilisateurs d'accéder aux informations (« *need-to-know* »), ou au contraire par la nécessité d'y soustraire certains utilisateurs (« *need-to-withhold* »). Quoi qu'il en soit, les droits d'accès doivent être accordés sur la base de la fonction et des responsabilités de l'utilisateur.

La façon dont les droits d'accès sont créés varie d'une solution à l'autre. Dans certains cas, les droits d'accès logiques sont accordés sur la base d'un code de transaction, d'un pseudonyme ou d'un numéro de compte. D'autres solutions, telles que SAP R/3, recourent à des protocoles de sécurité plus complexes, orientés objet. Lorsqu'on examine les contrôles d'accès logique d'une application, il importe aussi d'examiner les contrôles de sécurité généraux de l'application, à savoir :

- La longueur du nom ou de l'identification de l'utilisateur.
- La longueur du mot de passe.
- Les combinaisons de caractères du mot de passe.
- L'ancienneté du mot de passe (les utilisateurs doivent en changer tous les 90 jours, par exemple).
- Le renouvellement du mot de passe (les utilisateurs ne peuvent utiliser aucun de leurs cinq mots de passe précédents).
- Le verrouillage du compte utilisateur après un certain nombre de tentatives infructueuses pour ouvrir une session.
- La déconnexion automatique (l'application ferme automatiquement la session si l'utilisateur n'a pas interagi avec l'application au bout de 15 minutes).

Les applications de la dernière génération comportent souvent des paramètres que l'encadrement peut configurer, tels que ceux évoqués ci-dessus. Dans certains cas, il arrive toutefois que l'encadrement oublie d'activer le(s) paramètre(s), ou que les réglages utilisés pour chaque paramètre ne correspondent pas aux meilleures pratiques. Ainsi, il est possible de régler le paramètre de l'ancienneté du mot de passe de manière à imposer un changement de mot de passe tous les 90 jours. De plus, les auditeurs doivent périodiquement examiner les droits d'accès administrateur en environnement de développement et de test.

Une fois que l'étendue de la revue est définie, il s'agit de déterminer comment cet examen sera exécuté. Outre la méthodologie standard d'audit retenue, voici quelques recommandations qui peuvent aider l'auditeur à exécuter un examen des contrôles applicatifs correctement délimité.

Planification

Après avoir évalué les risques et déterminé l'étendue de la revue des contrôles applicatifs, les auditeurs doivent élaborer un plan d'examen détaillé et le communiquer. La première étape consiste à définir un plan de travail énumérant les composantes suivantes :

- Toutes les procédures d'examen à mettre en œuvre.
- Tous les outils et les techniques informatiques utilisés et leur mode d'utilisation.
- La taille des échantillons, le cas échéant.
- La sélection des points à examiner.
- Le calendrier de la revue.

Lors de l'élaboration de ce plan de travail, il convient d'inclure toutes les ressources d'audit interne nécessaires dès la planification. C'est également le moment d'identifier les spécialistes des technologies de l'information, et de les associer au processus de planification.

Une fois le plan de travail achevé, l'auditeur interne doit élaborer un programme d'examen détaillé (cf. annexe B page 21, pour un exemple de plan d'audit.) Lors de l'élaboration du programme d'examen, il convient d'organiser une réunion avec la direction afin d'évoquer les points suivants :

- Les préoccupations de la direction concernant les risques.
- Les problèmes déjà mentionnés.
- L'évaluation des risques et des contrôles par les auditeurs internes.
- Un résumé de la méthodologie d'examen,
- L'étendue de la revue.
- La façon dont les problèmes seront communiqués,
- Les dirigeants/cadres qui feront partie de l'équipe d'examen.
- Toute information nécessaire au préalable (rapports, par ex.).
- La durée de la revue.

Outre le résumé de la phase d'évaluation des risques, cette réunion répond à un objectif important : obtenir le soutien de la direction. Bien que les discussions doivent se tenir au début de la phase de planification, il convient de continuer d'évoquer les principaux processus, les risques et les contrôles tout au long de la revue, afin de veiller à ce que la direction soit d'accord avec l'étendue de la revue.

Il convient d'informer la direction de toute préoccupation connue, et spécifiquement de tout problème identifié pendant la phase d'évaluation des risques ou de planification, même si l'existence de ces problèmes n'est pas corroborée par des preuves. Des discussions doivent permettre de confirmer que la direction est d'accord avec tous les risques identifiés et les contrôles corespondants. L'équipe sera alors en mesure de la convaincre de décider immédiatement d'actions correctives et d'inciter toute l'entreprise à adopter un comportement tenant compte des risques. À cette fin, les auditeurs peuvent envoyer aux dirigeants un courrier leur annonçant la revue. Ce courrier doit mentionner :

- la date prévue pour le début de la revue.
- le calendrier de la revue.
- les principales activités examinées.

Besoin de ressources d'audit spécialisées

L'auditeur interne doit évaluer l'étendue de la revue et déterminer si la présence d'un auditeur informaticien est requise pour une partie des travaux. Le fait d'adjoindre à l'équipe un auditeur spécialisé dans les technologies de l'information ne dispense toutefois pas l'auditeur d'évaluer la qualité des contrôles informatiques. L'auditeur informaticien sera simplement chargé d'évaluer le recours aux technologies de l'information dans l'organisation, afin de vérifier l'intégrité des données, ainsi que l'exactitude, l'exhaustivité et l'autorisation des transactions. Les auditeurs informaticiens peuvent aussi s'intéresser au nombre de transactions traitées par l'application. Des outils spéciaux peuvent se révéler nécessaires pour évaluer l'efficacité des contrôles applicatifs, et établir un rapport. Les informations recueillies par les auditeurs informaticiens, associées au savoir de l'auditeur interne, permettront de déterminer si des ressources spécialisées sont nécessaires.

Il convient par exemple de disposer de ressources spécialisées lors de l'examen de la séparation des fonctions incompatibles pendant l'installation d'une application Oracle eBusiness Suite dans une grande entreprise industrielle. La complexité des rôles et des fonctions contenus au sein de l'application et des bases de données, nécessite de recourir à un personnel connaissant bien les possibilités de configuration de l'application Oracle. Du personnel supplémentaire sachant comment explorer des données depuis les bases de données et l'application Oracle peut aussi se révéler nécessaire. De plus, il se peut que l'équipe en charge de la revue ait besoin d'un spécialiste connaissant parfaitement un outil d'audit informatique précis, afin de faciliter l'extraction et l'analyse des données.

Méthode du processus d'entreprise

Le chapitre précédent expliquait que la méthode du processus d'entreprise est la plus utilisée lorsqu'on veut déterminer l'étendue de la revue des contrôles applicatifs. Aujourd'hui, beaucoup d'applications transactionnelles sont intégrées dans un système ERP. Dans la mesure où les transactions qui circulent dans ces systèmes ERP peuvent concerner plusieurs modules tout au long de leur cycle de vie, le meilleur moyen de mener à bien la revue consiste à opter pour une approche par processus d'entreprise ou par cycle (c'est-à-dire d'identifier

les transactions qui créent, modifient, ou effacent des données au sein d'un processus et, au minimum, de vérifier les contrôles applicatifs d'entrée, de traitement et de sortie). Le mieux est de décomposer le processus à l'aide du modèle à quatre niveaux présenté à la figure 3 :

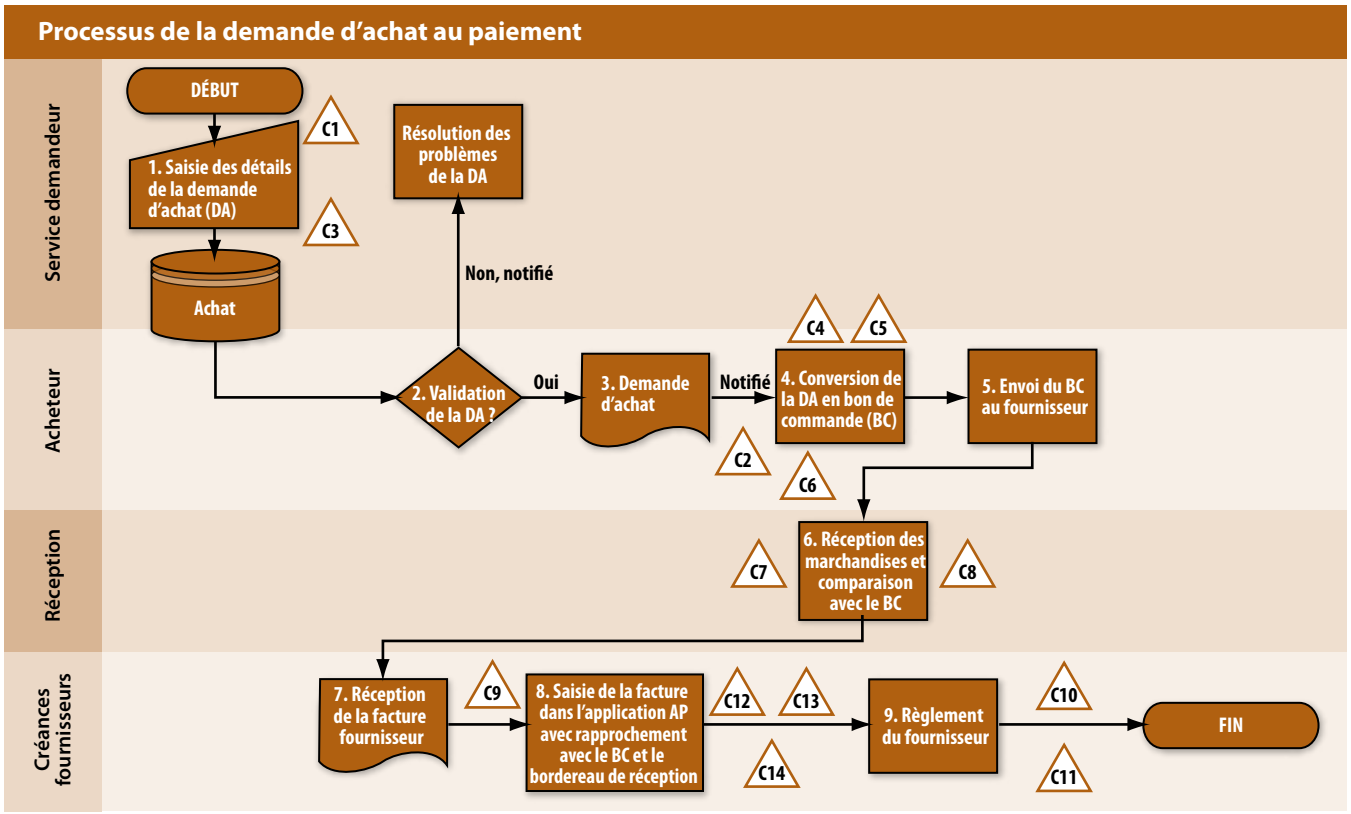
- Méga processus (niveau 1) : ce niveau correspond à l'intégralité du processus, de bout en bout, par exemple de la demande d'achat au paiement.
- Processus majeur (niveau 2) : ce niveau correspond aux principaux composants du processus de bout-en-bout, tels que l'achat, la réception et le paiement des marchandises.
- Processus mineur, ou sous-processus (niveau 3) : ce niveau correspond aux composants mineurs, ou sous-processus, de chacun des processus majeurs, tels que la demande et l'élaboration du bon de commande.
- Activité (niveau 4) : ce dernier niveau correspond aux transactions du système qui aboutissent à la création, à la modification ou à l'effacement de données pour chacun des composants mineurs ou sous-processus.

Il est essentiel d'adopter un point de vue centré sur l'entreprise si l'on veut que la revue soit exhaustive et utile à l'organisation. À partir de là, la revue peut être menée à bien dans le cadre d'une simple mission ou d'un examen intégré.

Méga-processus (niveau 1) : de la demande d'achat au paiement

Processus majeur (niveau 2)	Sous-processus (niveau 3)	Activité (niveau 4)
Achat	Traitement de la demande	Créer, modifier et supprimer
	Traitement du bon de commande	Créer, modifier, supprimer, valider et émettre
Réception	Traitement de la réception des marchandises	Créer, modifier et supprimer
	Traitement du retour des marchandises	Créer, modifier et supprimer
Créances fournisseurs	Gestion des fournisseurs	Créer, modifier et supprimer
	Traitement des factures	Créer, modifier et supprimer
	Traitement des notes de crédit	Créer, modifier et supprimer
	Règlements en cours	Créer, modifier et supprimer
	Règlements annulés	Créer, modifier et supprimer

Figure 3. Décomposition d'un processus d'entreprise.



△ Les triangles représentent chaque contrôle dans le processus. Le numéro de chaque contrôle le relie aux activités représentées dans la Matrice des risques et des contrôles.

Figure 4. Diagramme de flux d'un processus de la demande d'achat au paiement.

Techniques de documentation

Outre les normes relatives à la documentation que respectent les auditeurs internes, voici quelques suggestions concernant la documentation de chaque contrôle des applications.

Diagrammes de flux

Les diagrammes de flux constituent l'une des techniques les plus efficaces utilisées pour présenter la circulation des transactions, et les applications qui leur sont associées, ainsi que les contrôles manuels effectués dans un processus de bout-en-bout. La figure 4 présente un exemple de diagramme de flux pour un processus « de la demande d'achat au paiement ». Étant donné qu'il est difficile de faire apparaitre la description des contrôles sur le diagramme, il est recommandé de numéroter les contrôles et d'en reporter le numéro sur le diagramme. Les descriptions et les informations annexes seront détaillées dans un document distinct, reprenant chaque contrôle dans l'ordre, comme la matrice des risques et des contrôles (figure 6, pages 14–17). Cependant, les diagrammes de flux ne sont pas toujours pratiques, et une description narrative des processus se révèle parfois plus adaptée. C'est notamment le cas lorsqu'un auditeur consigne par écrit les domaines, ou un travail effectué dans l'environnement informatique. Il est fréquent que les tâches exécutées lors des contrôles applicatifs informatisés, ainsi que des applications connexes ne s'enchaînent pas de manière aussi linéaire que dans les processus tels que celui « de la demande d'achat au paiement ».

Description narrative des processus

La description narrative constitue une autre technique permettant d'établir la documentation sur les flux des transactions induits par les processus d'entreprise, ainsi que sur les applications qui y sont associées, comme le montre la figure 5. Le mieux est de se servir de ces descriptions comme d'un outil de documentation pour des processus et des environnements informatiques relativement peu complexes. En effet, plus le processus est complexe, plus il est difficile de rédiger une description narrative qui en reflète correctement et fidèlement la vraie nature. Dans le cas des processus relativement complexes, l'auditeur doit élaborer un diagramme de flux accompagné d'une description narrative correspondante dans lesquels les contrôles sont numérotés. Les auditeurs doivent également élaborer un document distinct, tel qu'une matrice des risques et des contrôles.

Description narrative	Processus « de la demande d'achat au paiement »
Contact(s) essentiel(s)	
Principaux éléments	C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, and C14.

Figure 5. Matrice des risques et des contrôles.

Voici un exemple de description narrative appliquée au processus « de la demande d'achat au paiement ».

1) Achat

a) Demande d'achat

i) Lorsque des salariés ont besoin d'acheter des biens ou des services, ils créent une demande d'achat dans l'application achat (**Contrôle C1**). L'acheteur vérifie ensuite si cette demande est correcte, complète et précise. Il s'attache notamment, sans que cette liste soit exhaustive, aux mentions du fournisseur, des articles, de la quantité et du code du compte. S'il ne constate aucune erreur, il valide la demande d'achat. Si l'acheteur rejette la demande pour quelque raison que ce soit, le service demandeur sera informé. Enfin, si les problèmes posés par la demande d'achat initiale sont résolus, l'acheteur valide la demande.

ii) Toutes les demandes d'achat font l'objet d'un examen mensuel destiné à détecter toute demande non autorisée, ainsi que les commandes en quantités excessives (**Contrôles C2 et C3**).

b) Traitement du bon de commande

i) Une fois que l'acheteur a validé la demande d'achat, il établit un bon de commande référençant la demande dans l'application achat (**Contrôle C4**). L'acheteur envoie ensuite une copie du bon de commande au fournisseur.

ii) Tous les bons de commande font l'objet d'un examen mensuel destiné à détecter tout achat non autorisé, ainsi que les commandes en quantités excessives (**Contrôles C5 et C6**).

2) Réception

a) Toutes les marchandises sont réceptionnées sur le quai d'expédition et de réception. Un salarié de l'entrepôt examine le bordereau de marchandises, prend note du numéro du bon de commande et compte les articles effectivement reçus. Il entre ensuite dans l'application achat et saisit le nombre des articles reçus en face du numéro de bon de commande correspondant.

b) Chaque mois, l'employé du service comptabilité compétent examine et effectue une vérification du compte stocks du grand livre général afin de déterminer si des marchandises ont été reçues, mais pas facturées par le fournisseur (**Contrôle C7**).

c) Chaque mois, l'acheteur du service achats compétent examine la liste de tous les bons de commandes posant probléme (**Contrôle C8**).

3) Créances fournisseurs

a) Le service créances fournisseurs reçoit chaque jour les factures émises par les différents fournisseurs. Ces factures sont triées et assignées à un agent du service, en fonction de l'identité du fournisseur. Chaque agent doit horodater la facture à la date de réception par le service créances fournisseurs. Il compare ensuite les quantités

et les prix mentionnés sur la facture et ceux indiqués sur le bon de commande et le bordereau de réception, puis saisit la facture dans l'application créances fournisseurs (**Contrôles C9 et C14**).

b) L'application créances fournisseurs génère automatiquement les demandes de règlement sur la base des modalités de paiement définies par le fournisseur, et tous les mercredis, des chèques sont établis pour le règlement des créances fournisseurs (**Contrôles C10, C12 et C13**).

c) En fin de mois, le responsable des créances fournisseurs compare le total du poste créances fournisseurs du grand livre auxiliaire, au total de contrôle du grand livre général. Toutes les différences sont ensuite consignées puis corrigées (**Contrôle C11**).

Les matrices de risques et de contrôles doivent contenir toutes les informations pertinentes relatives à un processus d'entreprise donné. De plus, chacune des activités de contrôle doit être numérotée ; c'est ce numéro qui sera reporté dans les diagrammes de flux ou les descriptions narratives. Voici les informations importantes qui doivent figurer dans la matrice :

- Les risques identifiés.
- Les objectifs de contrôle.
- Les activités de contrôle.
- Les attributs des contrôles tels que le type de contrôle (par ex., automatisé ou manuel) et la fréquence (quotidienne, hebdomadaire, mensuelle, trimestrielle, annuelle, etc.).
- Les informations relatives aux tests.

Tests

L'auditeur doit déterminer si les contrôles applicatifs fonctionnent, ou si des utilisateurs imaginatifs, ou les dirigeants, parviennent à les contourner. Il convient de procéder à des tests de corroboration de l'efficacité des contrôles, plutôt que d'examiner la description des contrôles. Les auditeurs doivent également déterminer l'efficacité des contrôles généraux informatiques, et se demander si l'équipe d'audit a besoin d'examiner les journaux de contrôle des changements générés par l'application, les journaux de sécurité et les journaux d'administration.

L'auditeur peut tester les contrôles applicatifs en utilisant plusieurs méthodes, suivant le type de contrôle. Selon la nature, le calendrier et l'étendue des tests, il est possible de tester un contrôle ou un rapport spécifique par :

- L'inspection des configurations du système.
- L'inspection des tests d'acceptation utilisateur, s'ils ont été effectués durant l'année en cours.
- L'inspection ou une nouvelle exécution des rapprochements avec les pièces à l'appui.
- Une nouvelle exécution des activités de contrôle à l'aide des données système.
- L'inspection des listes d'accès utilisateur.
- Une nouvelle exécution des activités de contrôle dans un environnement de test (à l'aide des mêmes procédures programmées que pour la production), avec des scripts de test solides.

Un test de configuration peut par exemple consister à examiner les paramètres de triple concordance du système testé, en retraçant une transaction. Il peut aussi consister à consulter le code de programmation du processus de production des rapports de l'application, afin de vérifier que la logique est appropriée. De plus, l'auditeur doit répéter l'éxecution de la requête afin de comparer le nouveau rapport à celui produit initialement.

L'auditeur peut vérifier les contrôles d'édition pour les principaux champs, en stratifiant ou en classant les transactions en fonction des valeurs de champs. En outre, si l'on recourt à un logiciel d'audit, il est facile de recalculer et de vérifier les calculs effectués par le système. Par exemple, si le système utilise les champs de la quantité et du prix unitaire pour calculer le coût total, l'auditeur peut recourir à un logiciel d'audit afin de procéder au même calcul et identifier toute transaction pour laquelle ses calculs donnent des résultats différents de ceux de l'application.

Enfin, les auditeurs peuvent procéder à des contrôles de vraisemblance afin d'examiner les fourchettes de valeurs possibles pour les principaux champs. Par exemple, en calculant l'âge actuel en fonction de la date inscrite dans le champ date de naissance, les auditeurs peuvent déterminer les âges, et prendre note des valeurs négatives et des valeurs supérieures à 100 qui sortent des fourchettes attendues.

Techniques d'audit assistées par ordinateur

Les techniques d'audit assistées par ordinateur (CAATs) recourent aux applications informatiques, telles que ACL, IDEA, VIRSA, SAS, SQL, Excel, Crystal Reports, Business Objects, Access, et Word pour automatiser et faciliter le processus d'audit. Elles permettent d'instaurer la couverture requise pour un examen des contrôles d'une application, en particulier lorsque des milliers, voire des millions, de transactions sont effectuées durant une période de test. Dans de telles situations, il serait impossible d'obtenir des informations pertinentes sous un format permettant un examen, sans recours à un outil automatique. Puisqu'avec les CATTS, on peut analyser de gros volumes de données, un audit bien pensé s'appuyant sur ces techniques peut procéder à un examen complet de toutes les transactions afin d'y déceler les anomalies (par exemple les fournisseurs ou les transactions saisis en double), ou un ensemble de problèmes de contrôle prédéterminés (par exemple des conflits liés à la séparation des fonctions).

Matrice des risques et des contrôles : de la demande d'achat au paiement

	PROCESSUS D'ENTREPRISE ET OBJECTIFS DE CONTRÔLE	RISQUES		ACTIVITÉS DE CONTRÔLE	COMPOSANTS COSO					ATTRIBUTS DU CONTRÔLE				CLASSIFICATION DU CONTRÔLE						VÉRIFICATION		
Numéro	Objectifs de contrôle	Risques	Impact/ probabilité	Activités de contrôle	EC	ER	AC	I/C	S	C (O/N)	Man/Auto	Prév./détect.	Fréquence	Réel	Enregistré	Evalué	Rapide	Classifié	Diffusé	Résultats des tests	Efficacité op. (O/N)	Notes
	Majeur : Achats																					
	Sous-processus : Traitement des demandes d'achat																					
	Activité : Créer																					
C1	Les contrôles donnent une assurance raisonnable que les demandes d'achat sont établies complètement et exactement, par du personnel habilité.	En raison d'une séparation insuffisante des fonctions, un utilisateur peut créer, valider (c-à-d émettre), assigner et transformer une demande d'achat, ce qui se traduit par l'attribution indue de commandes à des fournisseurs, des trop-perçus et des niveaux de stocks excessifs.	E	Les contrôles sont conçus de telle manière que l'accès n'est accordé qu'aux individus qui sont fondés à établir des demandes d'achat du fait de leur activité.			X				A	P	Permanent	X	X	X		X	X			
C2	Les contrôles donnent une assurance raisonnable que les demandes d'achat sont établies complètement et exactement, par du personnel habilité.	En raison d'une séparation insuffisante des fonctions, un utilisateur peut créer, valider (c-à-d émettre), assigner et transformer une demande d'achat, ce qui se traduit par l'attribution indue de commandes à des fournisseurs, des trop-perçus et des niveaux de stocks excessifs.	E	Les demandes d'achat sont examinées sur une base mensuelle, ce qui permet de détecter toute demande non autorisée.			X	X	X		M	D	Mensuel	X	X	X		X	X			
C1	Les contrôles donnent une assurance raisonnable que les demandes d'achat sont établies complètement et exactement, par du personnel habilité.	Les demandes d'achats non autorisées ou mentionnant des volumes excessifs peuvent aboutir à des prix défavorables, à des stocks excessifs et au retour des produits inutiles.	M	Les contrôles sont conçus de telle manière que l'accès n'est accordé qu'aux individus qui sont fondés à établir des demandes d'achat du fait de leur activité.			X				A	P	Permanent	X	X	X		X	X			
C3	Les contrôles donnent une assurance raisonnable que les demandes d'achat sont établies complètement et exactement, par du personnel habilité.	Les demandes d'achats non autorisées ou mentionnant des volumes excessifs peuvent aboutir à des prix défavorables, à des stocks excessifs et au retour des produits inutiles.	M	Les demandes d'achat sont examinées sur une base mensuelle, ce qui permet de détecter tout volume de commande excessif.			X	X	X		M	D	Mensuel	X	X	X			X			

Liste des acronymes utilisés dans ce tableau

Éléments du COSO
1. EC : environnement de contrôle
2. ER : évaluation des risques
3. AC : activités de contrôle
4. I/C : information et communication
5. S : surveillance

Attributs du contrôle
6. C : contrôle clé
7. Man/aut : manuel ou automatique
8. Prév/détec. : prévention ou détection

Figure 6. Matrice des risques et des contrôles pour un processus « de la demande d'achat au paiement »

Matrice des risques et des contrôles : de la demande d'achat au paiement

	PROCESSUS D'ENTREPRISE ET OBJECTIFS DE CONTRÔLE	RISQUES		ACTIVITÉS DE CONTRÔLE	COMPOSANTS COSO					ATTRIBUTS DU CONTRÔLE				CLASSIFICATION DU CONTRÔLE						VÉRIFICATION		
Numéro	Objectifs de contrôle	Risques	Impact/ probabilité	Activités de contrôle	EC	ER	AC	I/C	S	C (O/N)	Man/Auto	Prév./détect.	Fréquence	Réel	Enregistré	Evalué	Rapide	Classifié	Diffusé	Résultats des tests	Efficacité op. (O/N)	Notes
	Majeur : Achats																					
	Sous-processus : Traitement des demandes d'achat																					
	Activité : Créer																					
C4	Les contrôles donnent une assurance raisonnable que les bons de commande sont établis complètement et exactement, par du personnel habilité.	En raison d'une séparation insuffisante des fonctions, un utilisateur peut créer, valider (c-à-d émettre), assigner et transformer un bon de commande, ce qui se traduit par des commandes indues à des fournisseurs, des trop-perçus et des niveaux de stocks excessifs.	E	Les contrôles sont conçus de telle manière que l'accès n'est accordé qu'aux individus qui sont fondés à établir des bons de commande du fait de leur activité.			X				A	P	Permanent	X	X	X		X	X			
C5	Les contrôles donnent une assurance raisonnable que les bons de commande sont établis complètement et exactement, par du personnel habilité.	En raison d'une séparation insuffisante des fonctions, un utilisateur peut créer, valider (c-à-d émettre), assigner et transformer un bon de commande, ce qui se traduit par des commandes indues aux fournisseurs, des trop-perçus et des niveaux de stocks excessifs.	E	Les bons de commande sont examinés sur une base mensuelle, ce qui permet de détecter tout bon de commande non autorisé.			X	X	X		M	D	Mensuel	X	X	X		X	X			
C6	Les contrôles donnent une assurance raisonnable que les bons de commande sont établis complètement et exactement, par du personnel habilité.	Les bons de commande non autorisés ou mentionnant des volumes excessifs peuvent aboutir à des prix défavorables, à des stocks excessifs et au retour des produits inutiles.	M	Les bons de commande sont examinés sur une base mensuelle, ce qui permet de détecter tout volume de commande excessif.			X	X	X		M	D	Mensuel	X	X	X		X	X			

Liste des acronymes utilisés dans ce tableau

Éléments du COSO

1. EC : environnement de contrôle
2. ER : évaluation des risques
3. AC : activités de contrôle
4. I/C : information et communication
5. S : surveillance

Attributs du contrôle

6. C : contrôle clé
7. Man/aut : manuel ou automatique
8. Prév/détec. : prévention ou détection

Figure 6. Suite.

Matrice des risques et des contrôles : de la demande d'achat au paiement

	PROCESSUS D'ENTREPRISE ET OBJECTIFS DE CONTRÔLE	RISQUES		ACTIVITÉS DE CONTRÔLE	COMPOSANTS COSO					ATTRIBUTS DU CONTRÔLE				CLASSIFICATION DU CONTRÔLE						VÉRIFICATION		
Numéro	Objectifs de contrôle	Risques	Impact/ probabilité	Activités de contrôle	EC	ER	AC	I/C	S	C (O/N)	Man/Auto	Prév./détect.	Fréquence	Réel	Enregistré	Evalué	Rapide	Classifié	Diffusé	Résultats des tests	Efficacité op. (O/N)	Notes
	Majeur : Achats																					
	Sous-processus : Traitement des demandes d'achat																					
	Activité : Créer																					
C7	Les contrôles donnent une assurance raisonnable que les réceptions de marchandises sont traitées complètement, exactement et rapidement, par du personnel habilité.	Associer une réception de marchandises à un bon de commande incorrect ou à un poste incorrect fausse l'évaluation du stock et du compte marchandises reçues/non facturées, ce qui retarde le traitement des factures et le paiement.	E	Le rapprochement du compte marchandises reçues/non facturées est effectué sur une base mensuelle.			X	X	X		M	D	Mensuel	X	X	X		X	X			
C8	Les contrôles donnent une assurance raisonnable que les réceptions de marchandises sont traitées complètement, exactement et rapidement, par du personnel habilité.	Les marchandises reçues ne sont pas enregistrées correctement.	M	Les rapports signalant des bons de commande problématiques sont examinés sur une base mensuelle.			X	X	X		M	D	Mensuel	X	X		X	X				
	Majeur : Achats																					
	Sous-processus : Traitement des demandes d'achat																					
	Activité : Créer																					
C9	Les contrôles donnent une assurance raisonnable que les factures sont établies complètement, exactement et rapidement, par du personnel habilité.	Une facture qui devrait être payée après rapprochement avec un bon de commande est réglée sans référence au bon de commande, ce qui peut entraîner un paiement inacceptable pour du matériel ou des services (c-à-d. des écarts de prix inacceptables et défavorables).	M	La sécurité des applications est telle que l'accès aux transactions d'entrée de factures non accompagnées d'un bon de commande est aussi limité que possible.			X				A	P	Permanent	X	X	X		X	X			
C10	Les contrôles donnent une assurance raisonnable que les factures sont traitées, complètement, exactement et rapidement, par du personnel habilité.	Des montants de factures inexacts sont enregistrés, ce qui entraîne des paiements incorrects aux fournisseurs.	E	Les chèques sont rapprochés des pièces justificatives (facture, demande de règlement par chèque ou remboursement de frais) en fonction d'une limite en valeur.			X	X			M	P	Selon les besoins	X	X	X			X			
C11	Les contrôles donnent une assurance raisonnable que les factures sont traitées complètement, exactement et rapidement, par du personnel habilité.	La saisie des factures fournisseurs dans le grand livre auxiliaire n'est pas reportée dans le grand livre général.	F	Le total du grand livre auxiliaire des créances fournisseurs est comparé au solde du grand livre en fin de mois via un rapport chronologique. Toutes les différences observées doivent être corrigées.			X	X	X		M	D	Mensuel	X	X	X			X			

Liste des acronymes utilisés dans ce tableau

Éléments du COSO
1. EC : environnement de contrôle
2. ER : évaluation des risques
3. AC : activités de contrôle
4. I/C : information et communication
5. S : surveillance

Attributs du contrôle
6. C : contrôle clé
7. Man/aut : manuel ou automatique
8. Prév/détec. : prévention ou détection

Figure 6. Suite.

Matrice des risques et des contrôles : de la demande d'achat au paiement

	PROCESSUS D'ENTREPRISE ET OBJECTIFS DE CONTRÔLE	RISQUES		ACTIVITÉS DE CONTRÔLE	COMPOSANTS COSO					ATTRIBUTS DU CONTRÔLE				CLASSIFICATION DU CONTRÔLE						VÉRIFICATION		
Numéro	Objectifs de contrôle	Risques	Impact/ probabilité	Activités de contrôle	EC	ER	AC	I/C	S	C (O/N)	Man/Auto	Prév./détect.	Fréquence	Réel	Enregistré	Evalué	Rapide	Classifié	Diffusé	Résultats des tests	Efficacité op. (O/N)	Notes
	Majeur : Achats																					
	Sous-processus : Traitement des demandes d'achat																					
	Activité : Créer																					
C12	Les contrôles donnent une assurance raisonnable que le règlement des fournisseurs est effectué complètement, exactement, par du personnel habilité.	Les décaissements enregistrés diffèrent des montants payés.	F	L'application créances fournisseurs établit les chèques ou procède aux paiements électroniques automatiquement, sur la base de la valeur des factures validées, en fonction des modalités de règlement des fournisseurs et du système.			X				A	P	Permanent	X	X	X	X	X	X			
C13	Les contrôles donnent une assurance raisonnable que le règlement des fournisseurs est effectué complètement, exactement, par du personnel habilité.	Les décaissements effectués ne sont pas enregistrés.	E	L'accès est réservé au personnel autorisé à établir des chèques.			X				A	P	Permanent	X	X	X			X			
C14	Les contrôles donnent une assurance raisonnable que le règlement des fournisseurs est effectué, complètement, exactement, par du personnel habilité.	Des décaissements fictifs sont enregistrés.	M	L'application créances fournisseurs procède à une triple concordance entre le numéro de bon de commande, le bordereau de réception et la facture lors du traitement des factures.			X	X			A	P	Permanent		X			X	X			

Liste des acronymes utilisés dans cœ tableau

Éléments du COSO

1. EC : environnement de contrôle
2. ER : évaluation des risques
3. AC : activités de contrôle
4. I/C : information et communication
5. S : surveillance

Attributs du contrôle

6. C : contrôle clé
7. Man/aut : manuel ou automatique
8. Prév/détec. : prévention ou détection

Figure 6. Suite.

Annexe A: Contrôles applicatifs courants et propositions de tests

Les paragraphes qui suivent décrivent les contrôles applicatifs communs avec les tests proposés pour chaque contrôle. Le tableau a été communiqué par le groupe AXA.[17]

Contrôles des entrées

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

Contrôles des entrées et des accès

Ces contrôles permettent de vérifier que toutes les données d'entrée sont exactes, complètes et autorisées.

Domaine	Contrôle	Tests possibles
Vérification et validation des données	• Contrôles de vraisemblance sur les valeurs financières. • Contrôles des formats et des champs requis, écrans d'entrée standardisés. • Contrôles de séquence (p. ex. éléments manquants), contrôle des limites et chiffres clés. • Contre-vérification (certaines politiques ne sont valides qu'avec certains codes de table premium). • Validations (p. ex. table en mémoire et menu déroulant des éléments valides).	• Tester des échantillons pour chaque scénario. • Observer les tentatives d'entrer des données incorrectes. • Déterminer qui peut passer outre les contrôles. • S'ils sont gérés par tables, déterminer qui peut altérer les modifications et les niveaux de tolérance.
Autorisation et agrément automatisés et contournement (*override*)	• Des droits d'autorisation (p. ex. pour les dépenses, le paiement des créances ou les crédits au-delà d'un certain seuil) sont accordés à des utilisateurs sur la base de leurs rôles et de leur besoin d'utiliser l'application. • Le pouvoir de passer outre (p. ex. l'autorisation de créances d'un montant inhabituellement élevé) est réservé à certains utilisateurs, sur la base de leurs rôles et de leur besoin d'utiliser l'application.	• Procéder à des tests sur la base des droits d'accès des utilisateurs. • Vérifier les privilèges d'accès pour chaque fonction ou transaction sensible. • Examiner les droits d'accès qui établissent et modifient des limites configurables d'agrément ou d'autorisation.
Séparation automatisée des fonctions et des droits d'accès	• Les individus qui décident qui sont les fournisseurs agréés ne peuvent pas engager de transactions d'achat. • Les individus qui ont accès au traitement des créances ne doivent pas être en mesure de définir ou d'amender une politique.	• Procéder à des tests sur la base des droits d'accès des utilisateurs. • Examiner les droits d'accès qui établissent et modifient des rôles configurables ou des structures de menu.
Éléments en attente	• Les superviseurs vérifient tous les jours ou une fois par semaine les rapports chronologiques faisant apparaître des nouveaux éléments des politiques dont le traitement est incomplet. • Les fichiers en attente pour lesquels les informations disponibles sont insuffisantes pour permettre un traitement de la transaction.	• Examiner le résultat du classement chronologique et la preuve des procédures d'examen par les superviseurs. • Cheminer dans un échantillon vers et depuis le rapport chronologique ou le fichier en attente.

Contrôles de la transmission des fichiers et des données

Ces contrôles permettent de vérifier que les fichiers et les transactions transmis en interne ou à l'extérieur par voie électronique ont été envoyés par une source identifiée et traités exactement et complètement.

Domaine	Contrôle	Tests possibles
Contrôles des transmissions des fichiers	• Contrôle de l'exhaustivité et de la validité du contenu, y compris la date et l'heure, la taille des données, le volume des enregistrements et l'authentification de la source.	• Observer les rapports de transmission et d'erreur. • Observer les paramètres de validité et d'exhaustivité et les réglages. • Examiner les droits d'accès à la définition et à la modification des paramètres configurables pour le transfert de fichiers.
Contrôles des transmissions des données	• Application de certains contrôles des entrées afin de valider les données reçues (p. ex. principaux champs, vraisemblance, etc.).	• Tester des échantillons pour chaque scénario • Observer les tentatives d'entrer des données incorrectes. • Déterminer qui peut passer outre les contrôles. • S'ils sont gérés par tables, déterminer qui peut modifier les éditions et les niveaux de tolérance.

17 Tiré de *Common Application Controls and Suggested Testing* du Groupe AXA.

Contrôles du traitement

Ces contrôles sont conçus pour apporter une assurance raisonnable que le traitement des données s'est déroulé comme prévu, sans omission ni double décompte. Les contrôles du traitement sont en grande partie les mêmes que les contrôles des entrées, particulièrement pour les systèmes de traitement en ligne, ou en temps réel, mais sont appliqués pendant les phases de traitement. Ces contrôles sont les totaux intermédiaires, les rapports des totaux de contrôle, les contrôles des fichiers et des opérateurs, tels que les labels externes et internes, les journaux système des opérations informatiques et les tests de vraisemblance.

Contrôles du traitement

Ces contrôles permettent de vérifier que les données d'entrée valides ont été traitées exactement et complètement

Domaine	Contrôle	Tests possibles
Identification et validation automatique des fichiers	• Les fichiers à traiter existent et sont complets.	• Examiner le processus de validation et le fonctionnement du test.
Fonctionnalité automatique et calculs	• Calculs spécifiques effectués sur une ou plusieurs entrées et éléments de données stockés qui produisent d'autres éléments de données. • Utilisation des tables de données existantes (p. ex. fichiers maîtres ou données de référence telles que les barèmes).	• Comparer les valeurs d'entrée et de sortie pour tous les scénarios par cheminement et re-exécution. • Examiner les contrôles de la maintenance des tables et déterminer qui peut modifier les éditions et les niveaux de tolérance.
Pistes d'audit et contournements/ *overrides*	• Suivi automatisé des changements apportés aux données, attribuant le changement à un utilisateur précis. • Suivi automatisé et mise en évidence des contournements des procédures normales.	• Examiner les rapports et les preuves des vérifications. • Examiner les droits de contourner les procédures normales.
Extraction, filtrage et communication des données	• La vraisemblance et l'exhaustivité des sorties des routines d'extraction sont contrôlées. • Allocation automatisée des transactions (p. ex. à des fins de réassurance, d'autres processus actuariels ou l'allocation des fonds). • Évaluation des données utilisées pour procéder aux estimations à des fins de communication financière.	• Examiner la conception de la routine d'extraction par rapport aux fichiers de données utilisés. • Examiner l'évaluation par les superviseurs du résultat de la routine d'extraction pour vérifier qu'un examen régulier est effectué et s'il existe des problèmes. • Examiner le bien-fondé d'un échantillon d'allocations. • Examiner le processus d'évaluation de l'exhaustivité et de la validité des données extraites.
Équilibre à l'interface	• Vérification automatique des données reçues depuis les systèmes en amont (p. ex. données sur les paies, les créances, etc.) par les entrepôts de données ou les grands livres. • Vérification automatique de la correspondance entre les soldes des deux systèmes. En cas de non correspondance, un rapport d'exception est généré et utilisé.	• Inspecter les rapports d'erreur à l'interface. • Inspecter les paramètres et les réglages de la validité et de l'exhaustivité. • Examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les interfaces. • Examiner les preuves des rapports de correspondance, des vérifications et du traitement des fichiers contenant des erreurs.
Fonctionnalité automatique et classement chronologique	• Extraits de fichiers des listes de débiteurs afin de procurer à la direction des données sur les transactions par ordre chronologique.	• Tester des échantillons de transactions sur ces listes afin de valider le bien-fondé du processus de classement chronologique.
Contrôles des doublons	• Comparaison de chaque transaction aux transactions précédemment enregistrées afin de mettre les champs en correspondance. • Comparaison de chaque fichier avec les dates, heures, tailles, etc. attendus.	• Examiner les droits d'accès au réglage et à la modification des paramètres configurables sur les transactions ou les fichiers dupliqués. • Examiner le processus de manipulation des fichiers ou des transactions rejetés.

Contrôles des sorties

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

Contrôles des sorties

Ces contrôles permettent de vérifier que les données de sortie sont complètes, exactes et diffusées à qui de droit.

Domaine	Contrôle	Tests possibles
Report dans le grand livre général	• Tous les reports des transactions individuelles et synthétisées dans le grand livre.	• Remonter jusqu'au grand livre général un échantillon de transactions synthétisées d'entrée et du grand livre auxiliaire.
Report dans le grand livre auxiliaire	• Tous les reports de transactions réussis dans le grand livre auxiliaire.	• Remonter jusqu'au grand livre auxiliaire un échantillon de transactions d'entrée.

Contrôles des fichiers maîtres et des données de référence

Ces contrôles permettent de vérifier l'intégrité et l'exactitude des fichiers maîtres et des données permanentes

Domaine	Contrôle	Tests possibles
Autorisation des mises à jour	• Droits d'accès aux mises à jour attribués aux utilisateurs seniors sur la base de leurs rôles et de leur besoin d'utiliser l'application	• Examiner les droits d'accès au réglage et à la modification des fichiers maîtres et des données de référence.

Annexe B: Exemple de plan d'audit

Les auditeurs internes doivent élaborer et archiver un plan pour chaque mission d'audit. Ce plan doit mentionner les objectifs, l'étendue, les ressources et le programme de travail. Les objectifs permettent à l'auditeur de déterminer si les contrôles applicatifs sont bien conçus et fonctionnent efficacement, afin de gérer les risques afférant à la communication financière, au respect de la réglementation et aux paramètres opérationnels. Les contrôles applicatifs ont pour objectifs de vérifier que (cf. page 2 du présent guide) :

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

Voici les étapes permettant d'atteindre les objectifs ci-dessus :

- Étape 1. Réaliser une évaluation des risques (cf. page 7 du présent guide).
- Étape 2. Définir l'étendue de la revue (cf. page 9 du présent guide).
- Étape 3. Élaborer et communiquer le plan détaillé de la revue (cf. page 10 du présent guide).
- Étape 4. Déterminer quelles sont les ressources spécialisées nécessaires (cf. page 10 du présent guide).
- Étape 5. Déterminer si des techniques d'audit informatique seront nécessaires (cf. page 13 du présent guide).
- Étape 6. Conduire l'audit (cf. l'exemple de programme d'audit ci-dessous). Veuillez noter que cet exemple n'a pas pour intention de couvrir tous les tests applicables à votre organisation.

Exemple de plan d'audit

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

Objectif du contrôle	Contrôles	Activités liées à la revue
Objectif 1 : Les données d'entrée sont exactes, complètes, autorisées et correctes.		
	Les contrôles portant sur les données d'entrée sont conçus et fonctionnent efficacement de manière à veiller à ce que toutes les transactions aient été autorisées et validées avant la saisie des données.	Se procurer les procédures de saisie des données, comprendre le processus d'autorisation et de validation, déterminer s'il existe un processus d'examen et de validation et s'il a été communiqué aux utilisateurs chargés d'obtenir les autorisations correspondantes. Vérifier que le propriétaire de l'application ou du processus veille à ce que toutes les données soient autorisées avant leur saisie. Cette assurance peut passer par la répartition des rôles et des responsabilités selon les fonctions de chaque poste. Se procurer une copie des niveaux d'autorisation et déterminer si quelqu'un a été chargé de vérifier que les autorisations correspondantes sont toujours respectées.

Exemple de plan d'audit

Objectif du contrôle	Contrôles	Activités liées à la revue
	Les contrôles portant sur les données d'entrée sont conçus et fonctionnent efficacement de manière à veiller à ce que toutes les transactions saisies seront traitées correctement et intégralement.	Se procurer les procédures de saisie des données et vérifier que les individus responsables de la saisie des données ont été formés à l'élaboration, à la saisie et au contrôle des données d'entrée. Déterminer si les routines d'édition sont intégrées dans l'application qui vérifie puis rejette les informations entrées qui ne satisfont pas à certains critères : dates incorrectes, caractères incorrects, longueurs de champ non valides, données manquantes et entrées/numéros de transactions en double (la liste n'est pas exhaustive). Vérifier l'existence et le fonctionnement de contrôles manuels pour éviter les saisies en double. Les contrôles manuels peuvent comporter la pré-numérotation des documents source et l'apposition de la mention « entré » après saisie. Vérifier que les données ajoutées proviennent d'une source acceptable et soit rapprochées de cette source à l'aide de totaux de contrôle, de nombres d'enregistrements et d'autres techniques, comme les rapports de sources indépendantes. Déterminer si la séparation des fonctions est suffisante pour éviter que les utilisateurs saisissent et autorisent des transactions. Vérifier que la séparation des fonctions soit suffisante entre les individus qui saisissent les données et ceux qui sont chargés du rapprochement et de la vérification de l'exactitude et de l'exhaustivité des données de sortie. Vérifier que des contrôles sont en place pour éviter les changements non autorisés des programmes-systèmes, comme les calculs et les tables.
	Les contrôles portant sur les données d'entrée sont conçus et fonctionnent efficacement pour veiller à ce que toutes les transactions rejetées aient été identifiées et retraitées correctement et intégralement.	Se procurer les procédures de saisie des données pour le traitement des transactions rejetées et la correction ultérieure des erreurs et vérifier que le personnel responsable de la correction des erreurs et de la ressaisie des données a reçu la formation adéquate. Vérifier qu'un mécanisme est en place permettant d'avertir le propriétaire du processus que des transactions ont été rejetées ou que des erreurs se sont produites. Vérifier que les éléments rejetés sont retraités correctement et dans les délais, conformément aux procédures, et que les erreurs ont été corrigées avant la ressaisie dans le système.

Exemple de plan d'audit

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

Exemple de plan d'audit		
Objectif du contrôle	**Contrôles**	**Activités liées à la revue**
Objectif 3 : Les données stockées sont exactes et complètes.		
	Les contrôles d'accès logique sont conçus et fonctionnent efficacement pour prévenir l'accès, la modification ou la divulgation non autorisés de données système.	Se procurer la configuration et les procédures d'utilisation des mots de passe et vérifier la présence de critères obligatoires concernant les mots de passe, le renouvellement des mots de passe, le verrouillage du compte et la réutilisation des mots de passe. Vérifier que les dispositions décrites ci-dessus sont bien appliquées aux applications examinées. Vérifier que des contrôle d'accès à distance sont conçus et fonctionnent efficacement. Vérifier que les utilisateurs ne peuvent exécuter que des fonctions spécifiques, conformément aux responsabilités inhérentes à leur poste (accès fondé sur les rôles). Vérifier que des numéros d'identification utilisateur uniques ont été attribués à tous les utilisateurs, y compris les utilisateurs privilégiés, et que les comptes utilisateurs et administrateurs ne sont pas partagés. Vérifier que la création et la modification des comptes utilisateurs sont dûment autorisées avant d'accorder ou de modifier l'accès. (Les utilisateurs sont les utilisateurs privilégiés, les salariés, les sous-traitants, les fournisseurs et les intérimaires.) Vérifier que l'accès est supprimé immédiatement après la fin du contrat de travail. Vérifier que le propriétaire de l'application veille à ce qu'un examen semestriel des comptes utilisateurs et système est effectué pour confirmer que l'accès aux données financières, applications et systèmes opérationnels critiques est correct et à jour.
	Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce que la sauvegarde des données soit rigoureuse, complète et rapide.	Vérifier que la création et la modification des comptes utilisateurs sont dûment autorisées avant d'accorder ou de modifier l'accès. (Les utilisateurs sont les utilisateurs privilégiés, les salariés, les sous-traitants, les fournisseurs et les intérimaires.) Vérifier que l'accès est supprimé immédiatement après la fin du contrat de travail. Vérifier que le propriétaire de l'application veille à ce qu'une revue semestrielle des comptes utilisateurs et système est effectuée pour confirmer que l'accès aux données financières, applications et systèmes opérationnels critiques est correct et à jour.
	Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce que les données soient physiquement stockées dans un lieu sécurisé, hors-site et à environnement contrôlé.	Vérifier que des mécanismes sont en place pour stocker des données hors-site dans un lieu sécurisé et à environnement contrôlé.

Exemple de plan d'audit

Objectif du contrôle	Contrôles	Activités liées à la revue
Objectif 4 : Les données de sortie sont exactes et complètes.		
	Les contrôles sur les sorties sont conçus et fonctionnent efficacement pour veiller à ce que tous les résultats issus des transactions soient complets et précis.	Se procurer les procédures de sortie des données, comprendre le processus d'examen et vérifier que les individus responsables de la saisie sont formés à l'analyse et à la vérification des sorties de données. S'assurer que les données de sortie sont examinées ou rapprochées avec les documents source pour en vérifier l'exhaustivité et l'exactitude, y compris en vérifiant les totaux de contrôle.
	Les contrôles sur les sorties sont conçus et fonctionnent efficacement pour veiller à ce que tous résultats issus des transactions soient diffusés au personnel approprié et que les informations sensibles et confidentielles soie nt protégées durant leur diffusion.	Examiner les procédures existantes sur les sorties de données et déterminer si elles précisent quel personnel les reçoit et comment ces données sont protégées lors de leur diffusion.
	Les contrôles sur les sorties de données sont conçus et fonctionnent efficacement pour veiller à ce qu'un rapport de sortie soit créé au moment indiqué et couvre la période indiquée.	Vérifier qu'un rapport de sortie a été créé et que la date et l'heure du rapport correspondent bien au moment indiqué. Vérifier que le rapport couvre la période indiquée par un rapprochement avec les documents source pour cette période.
Objectif 5 : Les processus d'entrée, de stockage et de sortie des données sont archivés.		
	Les contrôles sont conçus et fonctionnent efficacement pour veiller à ce qu'une piste d'audit soit générée et actualisée pour toutes les données relatives aux transactions.	Vérifier l'existence de pistes et journaux d'audit qui confirment que tous les dossiers ont été traités et permettent de suivre la transaction de la saisie des données à leur stockage et à leur sortie. Vérifier l'existence de rapports d'audit qui retracent l'identification et le retraitement des transactions rejetées. Ces rapports doivent contenir une description claire de la transaction rejetée, de la date et de l'heure indiquées.

Glossaire

Contrôles applicatifs : Chaque application a ses propres contrôles, qui portent sur les transactions et les données relatives à chaque système d'applications informatisées. Les contrôles ont pour objectif de veiller à l'exhaustivité et à l'exactitude des données enregistrées, ainsi qu'à la validité des entrées effectuées dans le cadre des traitements automatisés. Exemples de contrôles applicatifs : validation des données d'entrée, concordance des totaux de contrôle et chiffrement des données transmises.

Contrôles des données d'entrée : le contrôle des données en entrée portent sur l'exactitude, l'exhaustivité et l'actualisation des données, pendant leur conversion, après leur saisie sur un ordinateur, ou dans une application. La saisie des données dans une application informatique peut être manuelle et en ligne, ou automatisée et par lots.

Contrôles des données de sortie : les contrôles des données en sortie portent sur l'intégrité des informations de sortie, ainsi qu'à la diffusion conforme et rapide des données produites. Celles-ci peuvent se présenter sur un support physique, comme les fichiers servant de données d'entrée dans d'autres systèmes, ou être consultées en ligne.

Contrôles du traitement des données : Les contrôles du traitement des données veillent à l'exactitude, l'exhaustivité et l'actualisation des données pendant leur traitement par lot ou en temps réel.

Contrôles généraux informatiques (CGTI) : ces contrôles s'appliquent à tous les composants, processus et données système d'une organisation, ou d'un environnement TI donnés. Ils ont pour objectif de veiller au bon développement et à la bonne mise en œuvre des applications, ainsi qu'à l'intégrité des programmes, fichiers de données et opérations informatiques.

Voici les plus courants :

- Contrôles d'accès logique sur l'infrastructure, les applications et les données.
- Contrôles sur le cycle de développement des systèmes.
- Contrôles de la gestion des changements dans les programmes.
- Contrôles sur la sécurité physique du centre de données
- Contrôles sur la sauvegarde et la récupération du système et des données.
- Contrôles des opérations machine.

Risque : possibilité que se produise un événement qui aura un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité.[18]

Séparation des fonctions : contrôles qui préviennent le risque d'erreurs et d'irrégularités en assignant à des individus distincts la responsabilité d'engager des transactions, de les enregistrer et de superviser les actifs. La séparation des fonctions est couramment utilisée dans les organisations dont le personnel est nombreux, afin qu'aucun individu ne soit en mesure de commettre une fraude sans que cela soit détecté.

Systèmes ou progiciels de gestion intégré (ERP) : L'ERP recouvre la planification et la gestion des ressources dans une entreprise, ainsi que l'utilisation d'un logiciel qui gère l'ensemble des processus de l'entreprise. Il intègre à ce titre les achats, les stocks, les effectifs, le service après-vente, l'expédition, la gestion financière et d'autres aspects de l'activité. Ce système s'appuie généralement sur une base de données commune, des modules intégrés et des outils d'analyse de l'activité.[19]

18 Tiré de le glossaire du l'International Professional Practices Framework de l'IIA.

19 Tiré de Certified Information Systems Auditor Glossary de l'ISACA.

Bibliographie

- GTAG 4 : *Management de l'audit des systèmes d'information*.
- GTAG 1 : *Les contrôles des technologies de l'information*.
- ISACA, IS Auditing Guideline — Application Systems Review, Document G14.
- COSO's *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*.
- PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraphes B29 - 30.
- Norme 1220 de l'IIA : Conscience professionnelle.
- Norme 1210.A3 de l'IIA.
- Norme 1130.C1 de l'IIA
- Groupe AXA, *Common Application Controls and Suggested Testing*.
- ISACA: Certified Information Systems Auditor Glossary.
- Professional Practices Framework de l'IIA.

Christine Bellino, CPA, CITP
Christine Bellino est directeur de la gestion du risque technologique au bureau de Denver de Jefferson Wells. Elle est membre de l'Advanced Technology Committee de l'IIA. Elle est également membre de l'équipe principale du *Guide to the Assessment of IT General Controls Scope based on Risk (GAIT)* de cette organisation. Elle s'occupe actuellement de la gestion de processus d'entreprise multiples et de la revue des contrôles généraux informatiques pour les petites, moyennes et grandes organisations.

Elle possède plus de 25 ans d'expérience dans la gestion du risque financier, opérationnel et technologique. Elle a co-présidé la Task Force du COSO qui a rédigé et récemment publié l'ouvrage *Internal Control Over Financial Reporting – Guidance for Smaller Public Companies*.

Steve Hunt, CIA, CISA, CBM
Steve Hunt est directeur des solutions d'entreprise chez Enterprise Controls Consulting (ECC). Il est membre de l'Advanced Technology Committee de l'IIA, de l'ISACA et de l'Association of Professionals in Business Management. Chez ECC, il travaille avec les entreprises du Fortune 1 000 de taille moyenne opérant sur des marchés restreints dans divers secteurs. Il dirige l'exécution des missions de gestion des risques financiers, opérationnels et informatique.

Il dispose de plus de 20 ans d'expérience dans différents secteurs : comptabilité, audit interne et conseil en management. Il a notamment réalisé des audits détaillés de la conformité avec la loi Sarbanes-Oxley et d'autres missions d'audit interne et externe, et participé à des projets de réingénierie des processus et des initiatives de développement de l'entreprise. Il possède également plusieurs années d'expérience en configuration des applications SAP R/3 et des contrôles de la sécurité des applications et des processus opérationnels. Il a donné des conférences dans plusieurs universités et organisations aux États-Unis.

Réviseurs
L'IIA tient à remercier les personnes et organismes suivants pour leurs précieux commentaires :

- IT Auditing Speciality Group, The IIA – Norvège.
- Les comités techniques de l'IIA – Royaume-Uni et Irlande.
- Helge Aam, Deloitte – Norvège.
- Ken Askelson, JCPenney Co. Inc. – États-Unis.
- Rune Berggren, IBM – Norvège.
- Shirley Bernal, AXA Equitable Life Insurance Co. – États-Unis.
- Lily Bi, The IIA.
- Claude Cargou, AXA – France.
- Maria Castellanos, AXA Equitable Life Insurance Co. – États-Unis.
- Nelson Gibbs, Deloitte & Touche, LLP.
- Steven Markus, AXA Equitable Life Insurance Co. – États-Unis.
- Peter B. Millar, ACL Services Ltd. – Canada.
- Stig J. Sunde, OAG – Norvège.
- Jay R. Taylor, General Motors Corp. – États-Unis.
- Karine Wegrzynowicz, Lafarge Amérique du Nord.
- Hajime Yoshitake, Nihon Unisys, Ltd. – Japon.
- Jim Zemaites, AXA Equitable Life Insurance Co. – États-Unis.
- Joe Zhou, GM Audit Services – Chine.

GTAG®

Audit des contrôles applicatifs

Les contrôles applicatifs portent sur les processus d'entreprise ou les systèmes d'applications (édition de données, séparation des fonctions d'entreprise, balance des totaux de contrôle, journalisation des transactions ou rapports d'erreurs). L'efficacité des contrôles applicatifs garantira à votre organisation l'intégrité, l'exactitude, la confidentialité et l'exhaustivité de ses données et systèmes. Le présent guide renseigne les responsables de l'audit interne sur ce qu'est un contrôle applicatif, ses relations avec les contrôles généraux, l'étendue d'une revue des contrôles applicatifs fondé sur les risques, les étapes d'une telle revue, énumère les principaux contrôles d'application, et enfin propose un exemple de plan d'audit.

Pour attribuer une note à ce guide ou formuler des commentaires, veuillez vous rendre sur www.theiia.org/GTAG.

À propos des guides pratiques d'audit des technologies de l'informaiton ?

Élaboré par l'Institute of Internal Auditors (IIA), chaque guide est rédigé dans des termes simples et traite d'un thème d'actualité qui a trait à la gestion, au contrôle et à la sécurité des TI. Cette série de guides constitue un précieux outil pour les responsables de l'audit interne, qui peuvent ainsi s'informer sur les différents risques induits par la technologie et sur les pratiques recommandées.

Guide 1: *Les contrôles des systèmes d'information*

Guide 2: *Contrôles de la gestion du changement et des patchs : un facteur clé de la réussite pour toute organisation*

Guide 3: *Audit continu : répercussions sur l'assurance, le pilotage et l'évaluation des risques*

Guide 4: *Management de l'audit des systèmes d'information*

Guide 5: *Le management et l'audit des risques atteinte à la vie priveé*

Guide 6: *Gérer et auditer les vulnérabilités des technologies de l'information*

Guide 7: *L'infogérance*

Consultez le site Web de l'IIA consacré à la technologie : www.theiia.org/technology.

ISBN 978-0-89413-613-9

The Institute of Internal Auditors

www.theiia.org