AUDIT

L'audit du contrôle interne de la fonction informatique dans les PME

Par Fabien CLEUET,
Auditeur CISA
(Certified Information Systems Auditor),
Vice-président de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées (CNEJITA)

Dans la majorité des cas, les commissaires aux comptes interviennent sur des dossiers de PME sans disposer de collaborateurs auditeurs certifiés en informatique de type CISA, CISSP [1] et autres. Il est toutefois possible d'évaluer la fonction informatique par des contrôles limités en nombres et en technicité pour un premier niveau de compréhension et de mesure du risque. La démarche proposée se base sur un document Word téléchargeable, facilitant la collecte des informations et les contrôles [2].

Analyser le système d'information de l'entreprise permet de connaître l'origine des informations en amont de la comptabilité et donc une partie des risques. L'objectif n'est ni de se limiter à vérifier les extincteurs, ni de suggérer des mesures de sécurité excessives et inadéquates, mais de démontrer une valeur ajoutée qui ne se limite pas à la certification des comptes.

Sans être auditeur informatique certifié, il est possible de mener certaines investigations et de faire une évaluation générale du contrôle interne de la fonction informatique. Il n'y a pas plus de raison de craindre d'aller voir l'informaticien de l'entreprise [3] que l'actuaire d'une compagnie d'assurance. Dans les deux cas, le sujet n'est pas facile et le langage abscons. Il est fréquent d'entendre *« je ne sais pas évaluer l'informatique »*. C'est la même situation lorsque l'on veut comprendre comment est calculée la provision mathématique d'une compagnie d'assurance. Il faut faire l'effort d'y aller et accepter de ne pas tout comprendre tout de suite. Nous souhaitons ici donner les raisons et les outils qui vont aider à dépasser cette crainte.

Résumé

L'auditeur financier rencontre des difficultés dans la prise en compte de l'environnement informatique de l'entreprise. L'article présente des supports de travail et met en évidence les enjeux et les zones de risque pour améliorer la pratique des auditeurs.

L'approche :

La RGI (Revue Générale Informatique) permet d'évaluer le contrôle interne de la fonction informatique au moyen de supports utilisés depuis longtemps dans le contexte du commissariat aux comptes en PME.

Tout audit a besoin d'un point de référence. Pour la mission d'un CAC en PME, il n'est pas envisageable d'utiliser les référentiels tels ITIL ou COBIT [4], du fait de leur complexité et de leur complétude.

Préparer l'intervention

Anticiper par une demande de document

La direction de l'entreprise donne les coordonnées de l'interlocuteur en charge de l'informatique [5]. Lors de la prise de contact, il convient de :

- parler de prise de connaissance et non d'audit, en prévoyant 4 heures environ, suffisant pour faire le tour d'un environnement simple d'une PME ;
- demander les documents, s'ils existent (ce n'est pas toujours le cas en PME) :
  - schéma d'architecture physique (ou réseau) ;
  - schéma d'architecture applicative ;
  - procédure de sauvegarde des serveurs ;
  - charte des utilisateurs.

Impliquer le management en évaluant le besoin de sécurité

Toutes les entreprises n'ont pas les mêmes exigences de sécurité. Il est essentiel de commencer par déterminer ce besoin qui conditionne tout le reste. Pour cela, il faut dialoguer avec les directeurs concernés qui connaissent la réponse et qu'il est nécessaire d'associer à cette réflexion.

■ Exigence de disponibilité

La question est :
« Demain le SI est ravagé :
a : comment travaillez-vous en mode dégradé ?
b : au terme de combien de jours la situation devient-elle très critique, voire vitale ? »
Assurément, seules les applications opérationnelles sont généralement concernées, car sauf exception [6], la paie et la comptabilité ne sauraient être considérées comme vitales.

Cycle	Application // serveurs	Exigence (J)	Obs.
Vente	PGI XYZ => sys025 (site Dijon)	2 jours	Att : données sensibles = Tarif

*1. Certified Information System Auditor et Certified Information Systems Security Professional sont des certifications de compétences organisées par l'*Information Systems Audit and Control Association

2. Document téléchargeable sur http://rgipourtous.diathese.fr

3. L'informaticien peut aussi être un prestataire externe.

4. ITIL et COBIT sont deux grands référentiels de bonnes pratiques des activités informatiques.

5. C'est éventuellement l'intégrateur du progiciel installé.

6. La question est légitime pour un cabinet d'expertise qui pourrait se retrouver durant plusieurs jours avec des collaborateurs oisifs, car sans possibilité d'accès aux données des clients.

Au cas présent, cela signifie qu'en tenant compte des niveaux de service internes et externes et des pertes potentielles de CA, on accepte une interruption du PGI[7] sur 2 jours, mais jamais au-delà. C'est un niveau très élevé qui impose une organisation de la sécurité, des coûts, des tests, bref des contraintes non nécessairement identifiées.

Dans le cas d'un délai court (<=4j) il convient d'inciter les acteurs-métiers à réfléchir à des modes de fonctionnement dégradés permettant de réduire cette exigence. La question pour l'auditeur est ensuite de savoir si l'on s'est donné les moyens de faire ce que l'on a dit en termes d'exigence….et si le management a la lucidité de reconnaître que le compte n'y est pas.

L'hébergement de serveur (*cloud*) apporte ici une sécurité importante si un dispositif de bascule entre *datacenter* est prévu. Outre le fait que ce n'est pas toujours le cas, l'externalisation présente par ailleurs d'autres difficultés de disponibilité réseau et de maîtrise organisationnelle et contractuelle qui méritent à eux seuls un développement spécifique.

■ Exigence de confidentialité des données

Ici encore, il importe de poser la question suivante :
« Quelles sont les données vraiment sensibles et pour lesquelles on est prêt à investir en protection ? »
Cette exigence relève en général de l'activité et non de la réglementation (R&D, Brevet, secret de fabrication ou tarifaires….etc).

Conséquences

C'est sur la base des bonnes pratiques (les divers référentiels proposés) et de ces exigences qu'il est alors possible d'apprécier la situation en étant crédible. Il est souvent utile de laisser quelques jours aux interlocuteurs pour affiner leur réflexion et donc revenir sur le sujet. Cette réflexion est à la fois le point de départ et la crédibilité de la RGI. C'est en fonction du besoin que seront écoutés le constat et les recommandations qui seront faites.

Besoin de sécurité =
exigence de disponibilité +
exigence de confidentialité

Être conscient de ses atouts

L'auditeur n'est pas un spécialiste informatique, mais a une vision globale de l'objectif de sécurité à atteindre. L'informaticien de l'entreprise peut (va) utiliser des termes techniques qui ne doivent pas déconcerter. Il ne faut pas craindre le vocabulaire informatique, ni les informaticiens, c'est un milieu où les techniques et le vocabulaire évoluent suffisamment pour que l'on accepte celui qui questionne *« c'est quoi ? Comment ça marche ? »*. Pour faire une RGI, il n'est pas requis d'être un technicien informatique[8].

La réflexion visant à fixer le besoin de sécurité permet d'en comprendre le sens et d'en connaître le détail. Dans 80% des cas, l'informaticien ne dispose pas de ces éléments. Il faut donc se positionner en pilote qui questionne et attend d'être convaincu, plutôt qu'en inspecteur d'octets en quête de savoirs.

***Exemple** : Le DG estime après réflexion que le site Web a une exigence de disponibilité de 5 jours :*

- *Quelles sont les ressources matérielles et logiciels concernées ?*
- *En combien de temps réinstaller et republier le site en cas de sinistre ? Quelle documentation ? Quels tests ? Qui sait faire ? Comment assurer au management que l'on sait le faire en 5 jours ?*[9]

Utiliser les documents supports

Le support de RGI[10] téléchargeable est imparfait mais adaptable. Il permet de balayer les points-clés en fonction des exigences exprimées. Il est décomposé comme suit :

- Cartographie des applications et des interfaces
- Description de l'équipe informatique et des serveurs
- Besoin de sécurité – exigence de disponibilité
- Questionnaire de RGI :
  - Sécurité physique
  - Sécurité logique et poste de travail
  - Condition d'exploitation (option si nécessaire)
  - Procédure de sauvegarde
  - Méthodologie de développement (option si nécessaire)
  - Contraintes légales
  - Pilotage de la DSI (option si nécessaire)

Le support de RGI passe en revue des thèmes de contrôle en face desquels l'auditeur indique les forces et les faiblesses qu'il constate (colonnes séparées pour faciliter la synthèse). L'enjeu, les investigations et les interlocuteurs concernés sont explicités dans un mémento de contrôle[11].

Cartographie (schéma et tableau)

Cet exercice consiste à établir un schéma des applications en mettant en évidence les flux d'échange de données pour en comprendre la nature et donc l'alimentation de la comptabilité.

Ici, la situation est simple, mais dans tous les cas, un tel schéma permet de comprendre visuellement quelle application est à l'origine de quelles informations et transactions. C'est dire l'enjeu. Dans la pratique, le recueil de ces informations et leur schématisation prend 15 minutes hors évaluation du risque des interfaces. Si le client a transmis un schéma d'architecture applicative, cela sera encore plus rapide.

A ce niveau, l'auditeur dispose d'une évaluation du niveau de sécurité attendu et d'une vision panoramique du système d'information. Le moment est venu d'approfondir la RGI.

RGI : la sécurité physique

La sécurité physique assure la disponibilité des données et des traitements

7. Progiciel de Gestion Intégrée.

8. Pour ceux qui veulent "réviser", les cours de préparation de l'UE5 du DSCG sont disponibles sur la page de téléchargement http://rgipourtous.diathese.fr
Le module 2 reprend le contrôle interne de la fonction informatique, le module 5, la gestion de projet.

9. Soyez assuré que pour une telle question vous serez pris au sérieux.

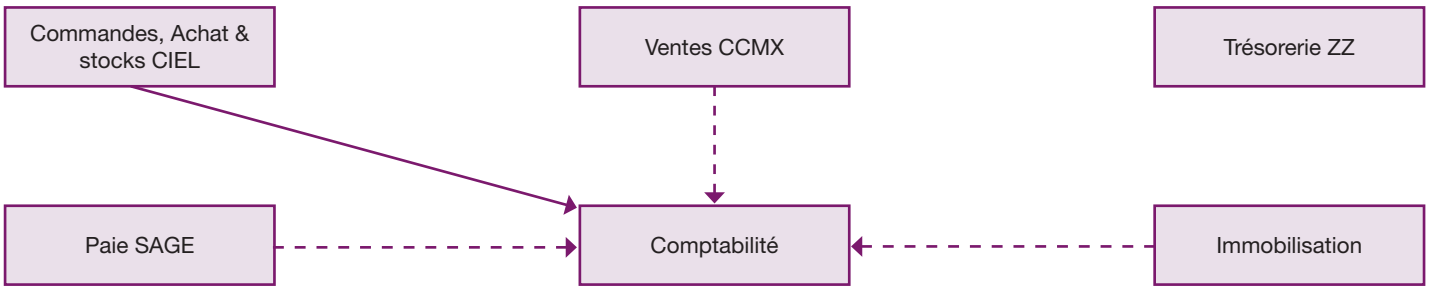
10. Téléchargeable sur http://www.diathese.fr/rgi-pour-tous

11. Ce support de RGI contient des éléments qui relèvent plus de la moyenne que de la petite entreprise. Ils permettent donc une évolution en « montée de gamme » et maintiennent la cohérence avec le mémento proposé en téléchargement. Ces domaines de contrôle supposent une relative complexité informatique. Ils seront donc sans objet dans la majorité des cas et non traités ici.

Abstract

The financial auditor encounters issues regarding the company's computing environment. The article introduces working papers and highlights the stakes and areas of risk in order to improve auditor's best practices.

AUDIT



Liaison exp : Paie⇨comptabilité	Type : M/S/A *	Fréquence (M,H,Q) **	Nature des contrôles (manuels ou automatisés)	Risque (I/M/F)***
Ciel => Compta	A	Q	Ctrl bouclage mensuel (formalisé et archivé)	F
Ventes => compta	S	Q	Att manipulation de fichiers non contrôlée. Bouclage annuel	M
Paie => compta	S	M	Bouclage livre paie // journal paie	F
IMMO => compta	S	A	Bouclage état 2054-2055// journal amort	F

* M = interface manuelle ; S = semi-automatique c'est-à-dire intervention d'un utilisateur ; A = automatique aucune intervention.
** Annuel, Mensuel, Hebdomadaire, Quotidien.
*** Important, Moyen, Faible.

au travers des serveurs et du réseau (internes et externes). Cela recouvre donc l'ensemble des ressources informatiques utilisées dans les processus opérationnels (acheter, produire, livrer) et fonctionnels (gérer). Sauf exception, la PME ne requiert pas un niveau de sécurité élevé. C'est donc uniquement en cas d'exigence de disponibilité inférieure à 5 jours que l'on va s'intéresser à un plan de back-up. *A contrario*, si le matériel est standard et qu'il existe des compétences internes ou externes, il sera raisonnablement possible de remettre en état un système similaire dans un délai de 5 jours. Dans tous les cas de figure, il faut s'intéresser au contexte de fonctionnement des équipements centraux. Les équipements informatiques sont d'autant plus à protéger par des actions de réduction de risque que les mesures de réduction d'impact sont faibles pour une exigence élevée.

Cela signifie que pour un délai de disponibilité attendu de 4 jours, il convient de combiner deux types d'actions :
• **Réduction de risque** : contrôle d'accès aux locaux (badge, accueil filtrant, zonage, portes imposant badgage), sécurité des locaux informatiques (ressources centrales dans un local bunkerisé ou dans un datacenter sécurisé), prévention électrique (onduleur, redresseur, batteries), niveau des contrats d'assurance, etc.
• **Réduction d'impact** : réplication des données (voire des serveurs) en externe, sauvegardes redondantes et très contrôlées, plan de back-up (documenté, testé), surveillance incendie et extinction 100% automatique, etc.

Remarques :

• S'agissant de la sécurité physique, il faut tenir compte des effets de bord entre disponibilité des applications et confidentialité des données. Ainsi, lorsque l'on peut voler le serveur central d'une PME, les deux exigences sont concernées.

• Il y a aussi des effets de bord entre sécurité logique et physique : la mise en œuvre d'un plan de back-up suppose un dispositif de sauvegarde sans faille.

• Pour beaucoup de PME qui ont peu de dépendance vis-à-vis de leur SI, il est possible de ne pas considérer comme "défaillant" une absence de sécurité autour d'un serveur classique pour des données non sensibles, mais bien sauvegardées.

• Les mesures de réduction de risque liées à la sécurité physique ne sont pas nécessairement onéreuses et relèvent souvent du bon sens. Ainsi, centraliser les équipements et les arrivées réseau dans une pièce centrale (sans fenêtre) protégée de murs solides est souvent possible. Y ajouter une porte de haute sécurité ne constitue pas une forte dépense. Il en va de même pour l'hygiène et les onduleurs-batterie (100 à 150€ par machine). Une telle organisation des locaux limite notoirement le risque de vol et de malveillance, tout en facilitant la surveillance incendie.

• Pour la réduction d'impact, seule l'extinction automatique constitue un budget significatif.

• Se garder de l'idée reçue selon laquelle la sécurité physique est réservée aux banques, cette remarque dissimule souvent négligence dans l'évaluation du besoin de sécurité et inconséquence quant à sa couverture.

• La prévention du risque est un acte de management, lorsqu'elle résulte d'un choix éclairé ; ce qui n'est pas toujours le cas.

Le support de RGI permet de passer en revue les points-clé de contrôle pour lesquels l'auditeur va évaluer si le contrôle interne est adéquat au besoin de sécurité qui a été fixé avec le management. Les 20 points-clés sont regroupés selon :
• l'infrastructure physique qualité des locaux au regard des vols, intrusions, inondations ;
• protection – extinction incendie ;
• protection électrique ;
• climatisation (normalement sans objet sauf si le local est fortement exposé au soleil) ;
• contrôle d'accès ;
• hygiène des locaux ;
• contrats de maintenance des équipements centraux (serveurs notamment) et réseau (si dépendance externe) ;
• plan de back-up.

RGI : la sécurité logique

Il n'est pas possible de tout évoquer ici, mais plutôt revenir sur les zones de risque les plus fortes ou les thèmes le nécessitant.

Sur bien des points, la sécurité logique est le moyen d'action du contrôle interne

Illustration du support de RGI

Ref.	Point de contrôle	Forces	Faiblesses
	Historique de l'informatique de la société		
1	**Sécurité physique**		
1.1	**Infrastructures physiques**		
	Qualité des murs et fenêtres		
	Risque étanchéité / inondation		
	Détection intrusion (alarme, gardiennage)		
	Organisation des locaux informatiques & télécom		

de l'entreprise, c'est dire son importance pour le commissaire aux comptes. La sécurité logique recouvre plusieurs axes :

- Eviter les intrusions => antivirus, antispam, mise à jour des logiciels, firewall.
- Prévenir une défaillance matérielle ou logicielle => sauvegarde.
- Surveiller l'accès à des données ou transactions critiques => contrôles ponctuels.
- Limiter les accès aux données et traitements en fonction des responsabilités et donc des droits des utilisateurs => gestion des accès (user), mots de passe, habilitation.
- Maintenir la sensibilité des acteurs sur le sujet => charte informatique.

L'organisation de la sécurité est souvent absente. Si les trois premiers objectifs sont maintenant entrés dans les usages, leur mise en œuvre pratique (en PME) est plutôt médiocre, notamment pour les deux premiers axes, voire défaillante pour le troisième. Le contrôle d'accès aux données et traitements est le tendon d'Achille du contrôle interne. La grande majorité des PME ne s'y intéresse pas, comme si la dématérialisation n'avait pas encore eu lieu.

En admettant le principe de séparation des fonctions, n'importe qui ne doit pas pouvoir :

- initier un virement bancaire sur un nouveau RIB,
- accéder à tout document du réseau, y compris ceux de la DG,
- purger la comptabilité de l'exercice,
- modifier les conditions tarifaires d'un client…etc.

On doit donc facilement admettre le caractère impérieux des points suivants :

- la délivrance, la modification et la révocation des droits sont nécessairement organisées, surveillées et formalisées => procédure d'habilitation,
- l'accès aux données et traitements est fonction des responsabilités de chacun, pour préserver le secret des affaires et prévenir la fraude => organisation des accès, groupe d'utilisateurs,
- les accès reposent sur un mécanisme d'identification (code utilisateur public) et d'authentification (mot de passe secret). C'est le maillon essentiel qui requiert en conséquence des règles et une surveillance. Parmi ces règles, un mot de passe complexe de 8 caractères minimum dont le changement est imposé mensuellement.

La sensibilisation des utilisateurs par une charte informatique est particulièrement peu mise en place. Ce n'est pas faute de modèle de document [12], mais plus vraisemblablement parce que de nombreuses organisations n'ont toujours pas compris certains fondamentaux : la sécurité globale repose sur le niveau du maillon le plus faible. Un seul utilisateur qui désactive un antivirus mal configuré, qui ouvre n'importe quelle pièce jointe venant d'un inconnu, qui laisse sa session ouverte durant le déjeuner, qui écrit son mot de passe "toto2015" sur un post-it et qui dispose de droit d'accès important… et c'est la sécurité de toute l'organisa-

12 .Google référence 677 000 résultats pour "modèle de charte informatique".

13. Test de relecture assuré par le logiciel de gestion des sauvegardes.

14. C'est maintenant facile et bon marché grâce aux débits internet, au cloud, à la chute des prix du stockage.

15. Operating System ou système d'exploitation tels Windows, Linux, Mac OS.

16. Selon la technologie utilisée ; DAT, DDS , DLT et SDLT.

Bref focus sur les sauvegardes

Elles ont pour objectifs de pallier un dysfonctionnement ou une indisponibilité matérielle ou logicielle. Elles sont quotidiennes et automatiques, ce qui les différencie des archives. Il est indispensable de contrôler systématiquement [13] leur bon fonctionnement et de disposer d'exemplaire à distance [14]. Elles ne servent pas qu'en cas de bris ou de vol de machine, mais aussi lorsqu'un traitement a dysfonctionné et pollué des données. Cette situation explique pourquoi il ne faut pas se limiter à des sauvegardes quotidiennes sans utilité, pour revenir sur des traitements qui ne le sont pas. C'est le sens du tableau décrivant l'organisation des sauvegardes figurant dans le support de RGI.

Cycle	***Contenu*** *(OS [15], data, appli,….)*	***Nbr Jeux***	***Stockage*** *(lieu, accès, conditions température, …)*
Quotidienne			
Hébdo.			

Autres points en bref :

- *Chaque session de sauvegarde doit faire l'objet d'un contrôle de relecture, chaque support doit être réutilisable par principe (c'est loin d'être le cas) ;*
- *Tous les supports de bande de sauvegarde n'ont pas la même durée de vie et cycle de réutilisation [16] => comment surveille-t-on les supports ?*

AUDIT

tion qui est mise à mal. Ici encore, il faut penser et organiser de manière globale pour ensuite agir en local. Un tel comportement des acteurs ne peut pas être obtenu par la seule coercition. Il est donc particulièrement important d'informer l'ensemble des utilisateurs de leurs droits, de leurs devoirs et responsabilités. Enfin, des mesures de contrôles et des sanctions sont à prévoir. Mettre en place des règles, les expliquer et les diffuser et plus impérieux que le contrôle mécanique de leur application. Tel est l'enjeu de la charte des utilisateurs et des actions de sensibilisation.

RGI : contraintes réglementaires

Nous ne ferons ici qu'un focus sur deux points significatifs pour le commissaire aux comptes (sanctions pénales possibles) et pour le client, en termes d'image de marque ou de pénalités financières. Les atouts du commissaire aux comptes sont ici essentiels. Qui mieux que lui pour apprécier des aspects de droit (fiscal notamment) liés au SI de la PME ? C'est un domaine où il doit faire connaître sa valeur ajoutée, d'autant qu'aucun acteur interne ne prend en charge ce sujet.

■ Loi informatique et liberté

Si l'entreprise traite en BtoC [17], le risque d'atteinte à l'image de marque est significatif, il convient donc d'être vigilant. Le support de RGI permet de vérifier la déclaration des principaux fichiers. Il faut par ailleurs contrôler les points suivants :

- existence d'une démarche régulière de recensement des fichiers "oubliés", à commencer par celui des visiteurs s'il est informatisé ;
- complétude des formulaires de collecte de données (papier ou non), au regard des mentions légales obligatoires (art 32) :
  - finalité et destinataire du traitement ;
  - existence d'un droit d'accès et coordonnée de la personne concernée ;
  - possibilité d'opposition à la collecte ;
  - le niveau de sécurité autour des données nominatives : le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi 78-17 du 6 janvier 1978 est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (C. pén., art. 226-17).
  - La CNIL a publié un guide de la sécurité des données personnelles qui constitue de fait un référentiel [18]. Il mentionne notamment des exemples de ce qu'il ne faut pas faire !

■ Contrôle fiscal des comptabilités informatisées

C'est assurément LE domaine où le commissaire aux comptes peut s'illustrer. Le support RGI proposé cible donc l'essentiel :

- existence d'un "sachant" qui organise la conformité au CFCI ;
- modalité de déclenchement de l'archivage fiscal de fin d'année ;
- existence et test de la procédure de production du FEC [19] rendu obligatoire ;
- tableau de collecte pour chaque application de gestion.

Conclusion

L'objectif de cet article était de présenter les points-clés, en termes de complexité ou d'enjeux qui peuvent motiver le commissaire aux comptes pour « *passer le cap* » et tenter une RGI. Assurément, cette volonté doit s'accompagner d'un travail, éventuellement, d'une formation préparatoire. C'est plus particulièrement le cas des contrôles de sécurité physique et logique. Il faut garder à l'esprit que le numérique est partout et à l'origine des données qu'il faut auditer. Dès lors, la prise en compte de l'environnement informatique ne peut être remise à plus tard ou simplement ignorée. Il faut anticiper et s'attendre à l'arrivée de progiciels globaux intégrés en PME qui imposeront encore d'autres compétences. Vaste programme et perspectives de création de valeurs pour les professionnels du chiffre. ■

17. Business to Consumer se dit des entreprises qui opèrent avec le public.

18. http://www.cnil.fr/documentation/guides/ La Cnil publie également une FAQ et répond aux questions écrites ou téléphoniques (Contact : 01 53 73 22 22).

19. Le Fichier des Ecritures Comptables est un format de communication des données comptables à l'administration en cas de contrôle (LPF art 47 AI).