



LA PLACE DE LA VÉRIFICATION INFORMATIQUE DANS LA GESTION INTÉGRÉE DES RISQUES D'ENTREPRISE

Depuis 2002, les pressions réglementaires et les investisseurs ont poussé les organisations à identifier, évaluer, traiter et communiquer les risques sur leurs activités par la mise en place d'un cadre de gestion intégrée des risques.

Ce cadre de gestion intégrée des risques doit comprendre l'ensemble des politiques, pratiques et procédures permettant d'identifier les risques, les analyser et les traiter de manière à assurer l'exploitation viable de l'organisation. Cette gestion intégrée des risques vise à rapprocher les différentes communautés de gestion de risque : financière, technologique, industrielle, toxicologique ou autre, dans un but commun de réduction des risques d'affaires.

De son côté, la vérification interne a pour mission de donner une opinion sur le degré d'assurance à accorder aux différentes pratiques, cadres de contrôle et informations utilisés au sein de l'organisation de manière à outiller la Direction dans sa stratégie de gestion des risques.

Ce monde de la vérification s'est vu façonner son fonctionnement interne au gré des différentes exigences réglementaires internationales telles que SOX, Bâle II pour les institutions financières, Solvabilité II pour l'assurance, NERC pour le secteur de l'énergie, HIPAA pour la santé. Plus global, le cadre de contrôle interne COSO créé en 1992 est devenu un standard incontournable dans la plupart des organisations matures.

En parallèle, du côté des technologies de l'information, nombre d'outils et de cadres de références se sont déployés opérationnellement avec le niveau de maturité croissant des entreprises dans ce secteur ; les services informatiques se sont inscrits dans la mouvance ITIL®, tandis que le contrôle interne informatique s'est renforcé avec des référentiels tels que COBIT® et la communauté sécurité s'est rassemblée autour de standards tels que ISO 27002 ou autour de méthodes d'analyse de risque telle que la méthode MEHARI.

Ont donc coexisté pendant des années, deux communautés d'analyse de risques issues d'environnements hétérogènes et utilisant des outils et donc des langages différents.

Pourtant, que l'on utilise les référentiels SOX, COSO, COBIT, ISO 27002, MEHARI ou autre, tous ces référentiels communiquent entre eux (d'ailleurs l'ISACA® a mis au point un certain nombre de passerelles le démontrant) et visent le même objectif : identifier les risques susceptibles *in fine*, de nuire à la capacité de production de l'entreprise. On pourra se référer au schéma en figure 1 pour une représentation du recouvrement de certains des référentiels les plus communs en gouvernance T.I.

Il en demeure qu'il faut être capable de démontrer comment des risques d'origine technologique peuvent se traduire en risques d'affaires. Le problème tourne essentiellement autour de la sous-estimation de la valeur de l'informatique et de sa contribution aux performances de l'entreprise. Ceci s'explique principalement par la difficulté qu'ont d'une part les vice-présidences T.I à traduire leur préoccupation en langage d'affaires et d'autre part, par la difficulté qu'ont les vice-présidences d'affaires à reconnaître leurs différentes responsabilités de donneur d'ordre vis-à-vis de la vice-présidence T.I. Il existe pourtant des outils disponibles pour faciliter cette communication. Val IT™, cadre de référence pour

la valeur ajoutée de l'informatique et les investissements T.I peut contribuer à faciliter les échanges tout autant que la sensibilisation des vice-présidences d'affaires vis-à-vis de leur responsabilité en matière de contrôle et protection des données dont elles ont la charge.

Les risques informatiques les plus courants sont ceux liés à une inadéquation des besoins informatiques vis-à-vis des besoins d'affaires, à un mauvais paramétrage des règles de gestion notamment dans les ERP, au non respect du principe de ségrégation des tâches dans les applications d'affaires, à la rupture de la piste d'audit, au non-respect des contraintes réglementaires et à l'indisponibilité des applications. On voit ici aisément le lien avec les risques de contrôle interne. Ceci peut se traduire par exemple par des paiements en double, des erreurs de référencement dans les catalogues produits, des erreurs de tarification, la divulgation d'informations personnelles sur les salariés, des secrets industriels ou de la stratégie d'affaires, l'altération de résultats de R&D, de la fraude ou encore des attaques en déni de services sur les serveurs critiques.

Restreindre le contrôle interne et l'informatique à des centres de coûts consiste à se reposer sur une vision altérée de la gestion des risques du fait de l'absence d'outils d'analyse et de mesure adéquats permettant de mettre en perspective le coût de remédiation face au risque de ne rien faire. On comprend donc aisément le besoin de disposer d'un cadre d'analyse et de mesure de ces risques tout autant que d'auditeurs qualifiés et certifiés pour identifier et interpréter ces risques à leur juste mesure.

L'intérêt à faire communiquer les référentiels de gestion des risques et de gestion des risques T.I dans un seul référentiel intégré réside dans la synergie qui en résulte : démonstration de la valeur de l'informatique en montrant comment elle contribue à l'atteinte des objectifs d'affaires globaux et rationalisation des coûts d'analyse de risques par une mise en commun des moyens. Il en résulte une transparence de l'outil informatique pour la direction, et un cadre de gestion des risques plus fluide et plus précis pour la prise de décision.

Delphine Pramotton

CISA, CISM, Auditeur principal ISO 27002

Directrice de la communication

ISACA – Chapitre de Montréal

NOUVELLES DES MEMBRES

Jacques Lavallée a été nommé au poste Vice-président principal, opérations et technologie, à la Caisse de dépôt et placement du Québec.

Caroline Bineau a été nommée au poste de Vice-présidente, vérification interne, à la Caisse de dépôt et placement du Québec.

Veillez faire parvenir vos nominations pour publication dans l'Auditeur Libre à l'adresse suivante :

jonathan.allard@navigantconsulting.com

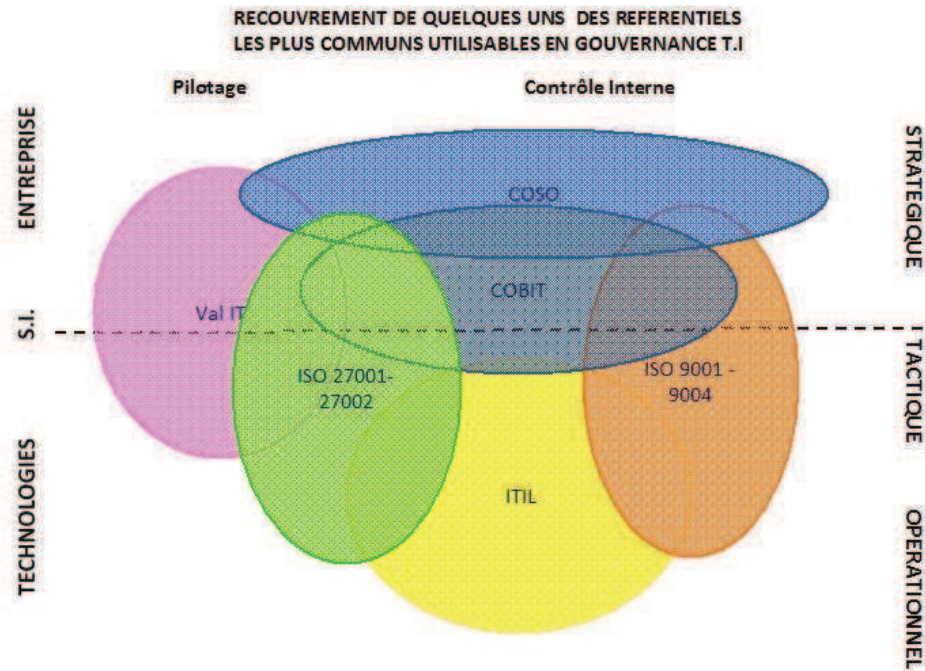


Table des acronymes utilisés

SOX	(sociétés cotées) Loi Sarbanes-Oxley du 31 juillet 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs imposant de nouvelles règles sur la comptabilité et la transparence financière notamment par la formulation d'exigences en matière de contrôle interne.
Bâle II	(domaine bancaire – 2004) Normes issues du nouvel accord de Bâle et qui recommandent un dispositif prudentiel destiné à mieux appréhender les risques bancaires et principalement le risque de crédit ou de contrepartie et les exigences en fonds propres.
Solvabilité II	(assurances - 2006) Réforme réglementaire européenne du monde de l'assurance dont l'objectif est de mieux adapter les fonds propres exigés des compagnies d'assurances et de réassurance avec les risques que celles-ci encourent dans leur activité. Solvabilité II encourage notamment les entreprises à adopter une démarche de gestion des risques d'entreprise.
NERC	North American Electric Reliability Corporation - organisme sans but lucratif nord-américain fondé en 1968 chargé de faire appliquer des normes de fiabilité pour les réseaux de transport de l'électricité des États-Unis, du Canada et de certaines régions du Mexique. Suite à la panne de courant nord-américaine de 2003, le Congrès américain a adopté l'Energy Policy Act of 2005, donnant au NERC la responsabilité d'élaborer et de faire respecter des normes de fiabilité obligatoires sur tous les réseaux de transport d'électricité. Il en est notamment sorti des exigences en matière de sécurité des réseaux (normes CIP du NERC).
HIPAA	Health Insurance Portability and Accountability Act (HIPAA) (Etats- Unis 1996)- La section II de l'HIPAA requiert des standards en matière de transactions électroniques de santé et protection des données personnelles des patients.
COSO	Référentiel de contrôle interne défini par le Committee Of Sponsoring Organizations of the Treadway Commission. Il est utilisé notamment dans le cadre de la mise en place des dispositions relevant des lois Sarbanes-Oxley.
ITIL	Information Technology Infrastructure Library - ensemble de bonnes pratiques pour la gestion des services informatiques
COBIT	Control Objectives for Information and related Technology –cadre de gouvernance des systèmes d'information définissant les objectifs de contrôle et les bonnes pratiques, par domaine informatique et par processus, en les reliant aux exigences métiers et permettant d'intégrer d'autres référentiels tels que ISO 9000 ou ITIL.
ISO 27002	La norme ISO/CEI 27002 concernant la sécurité de l'information, publiée en juillet 2007 par l'ISO, dont le titre en français est « Code de bonnes pratiques pour la gestion de la sécurité de l'information. »
Val IT	Val IT (Enterprise Value : Governance of IT investments) est un cadre de référence défini par l'ISACA pour la gouvernance des investissements informatiques.
MEHARI	La méthode harmonisée d'analyse des risques (MEHARI) est une méthode visant à la sécurisation informatique d'une entreprise ou d'un organisme. Elle a été développée et est proposée par le CLUSIF (Club de la Sécurité Informatique Français).
ERP	Enterprise Resource Planning : progiciel de gestion intégré permettant de gérer l'ensemble des processus opérationnels d'une entreprise.