

Atelier 3: Maîtrise des risques et système d'information

Risques
comptables

Risques
techniques

Opposabilité
juridique



Risques comptables

Au travers des axes d'échanges des expériences pays, les risques liés à la fonction comptable découlent:

- D'erreurs de saisies des opérations comptables (saisies multiples ou double saisie);
- Du traitement des comptes d'imputations provisoires et de comptes de transfert;
- De la mauvaise tenue de comptabilité dans les postes déconcentrés;
- De la remontée tardive ou incomplète des données comptables;
- D'erreurs d'imputations budgétaires ou comptables;
- De la non maîtrise du passage de la comptabilité de caisse à la comptabilité patrimoniale en droits et obligations constatés;



Risques techniques

Les risques techniques peuvent être liés à:

- ❑ un système d'information non robuste dont l'architecture ne permet pas une bonne intégration des équipements et des solutions logicielles;
- ❑ un défaut d'audit périodique du système d'information pour déceler d'éventuelles vulnérabilités;
- ❑ un défaut de sécurité physique de datacenter, de contrôle d'accès physique et logiciel;
- ❑ des niveaux d'habilitations mal définies;
- ❑ la mauvaise sauvegarde des bases de données, absence de réplication de données ou de backup sur un site distant ou un hébergement sur le cloud (plan de restauration);
- ❑ des fonctions comptables mal implémentées ou qui présentent des anomalies;
- ❑ un défaut de documentation pour assurer la continuité du service (affectation de personnel);
- ❑ la non maîtrise de la confidentialité et de l'intégrité des données;



Opposabilité juridique

La dématérialisation comporte des aspects techniques et opérationnels mais également juridiques relatifs à l'opposabilité à savoir la valeur juridique des actes budgétaires et comptables dématérialisés. Il s'agit de:

- ❑ La valeur juridique des pièces justificatives des opérations budgétaires et comptables notamment les factures et contrats ou marchés publics dématérialisés;
- ❑ L'opposabilité et la valeur juridique de la signature électronique;
- ❑ Les faits générateurs à conserver dans la base de données (archivage électronique des pièces);
- ❑ L'acceptation des données générées par le système d'information par le juge des comptes.

Recommandations (1/2)

Quelques pistes de recommandations à prendre en compte:

- ❑ Encourager l'implémentation des systèmes intégrés de gestion budgétaire et comptable;
- ❑ Elaborer des plans de sécurité physique et des logiciels du système d'information;
- ❑ adopter une politique d'habilitation rigoureuse (les droits d'accès) à surveiller par un dispositif de contrôle et d'audit interne;
- ❑ Instaurer un contrôle interne : un contrôle mutuel ou de validation et de supervision notamment la saisie des données;
- ❑ Instaurer des contrôles « embarqués » informatiques et automatisés;



Recommandations (2/2)

- ❑ convenir de normes et processus avec la Cour des comptes dès la conception du système d'information (validité des pièces justificatives et des factures dématérialisées);
- ❑ Veiller à la couverture de tous les métiers du Trésor et tous les acteurs par le système d'information adopté ;
- ❑ Disposer d'un logiciel d'analyse ou d'audit du système d'information;
- ❑ Créer un cadre juridique relatif à la validité de la signature électronique et à la protection des données personnelles;
- ❑ convenir avec la Cour des comptes de l'intégration dans la détermination du résultat des comptes d'imputation provisoire de dépenses relatifs aux avances au budget; ce qui permet de régulariser les comptes d'imputation provisoires de dépenses en gestion n+1.