



## AIDE-MÉMOIRE

### UTILISER LES SERVICES D'UN TIERS

#### Objectif du document

Fournir des conseils et des outils pour les organisations qui confient une partie de la réalisation de leurs activités à au moins un tiers.

Les services retenus ici concernent uniquement les services d'infogérance, soit les prestations en lien avec les systèmes d'information (ex. : services d'infrastructure, services applicatifs, gestion des données).

**Destinataire du document :** Responsable des achats

**Date de la dernière modification :** 2017-06

#### Les types de services

Services d'infrastructure	Services applicatifs	Gestion de données
<ul style="list-style-type: none"><li>• Virtualisation</li><li>• Hébergement</li><li>• Maintenance</li><li>• Gestion des identités et des accès</li><li>• Surveillance des serveurs</li></ul>	<ul style="list-style-type: none"><li>• Développement applicatif</li><li>• Support applicatif</li><li>• Gestion des évolutions</li></ul>	<ul style="list-style-type: none"><li>• Sauvegarde informatique</li><li>• Migration et intégration de données</li><li>• Implantation de solutions de stockage et d'archivage</li></ul>



## Risques liés à l'externalisation

---

Voici une liste non exhaustive des risques liés à la sous-traitance :

- Service insatisfaisant ou non conforme
- Soutien inadéquat ou inexistant
- Encadrements inadéquats
- Non-respect des encadrements de l'organisation
- Incompatibilité de composantes logicielles ou matérielles
- Perte, vol, corruption de données ou fuite d'informations délibérée ou accidentelle
- Interruption ou dégradation du service causée par la défaillance
- Qualité de service inadéquate

En utilisant les services d'un fournisseur, l'organisation s'expose aussi à une perte de contrôle sur son système d'information et à une certaine dépendance technologique.

## Recommandations

---

Les interventions en matière de sécurité sont réalisées tout au long du processus d'externalisation.

### Appel de propositions et appel d'offres

- Cibler et quantifier les risques liés à l'externalisation du service visé.
- Obtenir l'engagement formel des soumissionnaires à ne pas divulguer l'information de l'organisation classifiée confidentielle, privée ou secrète.
- Inclure les exigences de sécurité proportionnelles au risque dans le cahier des charges des appels de propositions ou des appels d'offres.
- Évaluer la sécurité du fournisseur.
- Évaluer le risque des écarts entre les obligations de l'organisation et les mesures du fournisseur.
- Adopter une stratégie de réponse (accepter, réduire, transférer, refuser).

### Nouveau contrat, renouvellement ou modification de contrat existant

- Cibler et quantifier les risques liés à l'externalisation du service visé.
- Obtenir l'engagement formel des soumissionnaires à ne pas divulguer l'information de l'organisation classifiée confidentielle, privée ou secrète.
- Évaluer les pratiques de sécurité du fournisseur avant la signature du contrat.
- Inclure dans le contrat les exigences de sécurité proportionnelles au risque en fonction de la nature du contrat.
- Analyser le risque associé au refus de l'inclusion ou de la modification par un fournisseur d'une exigence de sécurité.



## Exigences de sécurité

---

Voici une liste d'exigences de sécurité que l'on devrait retrouver dans vos contrats en fonction de la nature de ceux-ci et de manière proportionnelle au risque :

- Confidentialité
- Responsabilités
- Pénalités en cas de manquement
- Obligations du fournisseur et du client
- Localisation des données (site principal et copies de sauvegarde)
- Tiers impliqués
- Vérification des antécédents
- Convention de services (taux de disponibilité du service, durée maximale d'indisponibilité mensuelle, temps moyen entre deux pannes)
- Coordonnées du responsable de la sécurité
- Gestion des incidents de sécurité (détecter, répondre, restaurer et suivre)
- Fin ou résiliation du contrat (récupération et destruction de l'information)
- Audit de sécurité