

Processus de sécurisation de l'information

1 

Identifier les actifs

La sensibilité de l'information est évaluée par l'organisme public selon le préjudice qu'il encourt en termes de **disponibilité**, d'**intégrité** et de **confidentialité (DIC)**.

2 

Évaluer la sensibilité de l'information gouvernementale

3 

Choisir le modèle infonuagique approprié

Les modèles d'infonuagique (nuage externe ou gouvernemental) et les profils de mesures minimales de sécurité de l'information correspondants (profil A, B ou C) sont déterminés préalablement par ITQ. L'organisme public choisit le modèle d'infonuagique ainsi que le profil des mesures minimales correspondant selon le niveau de sensibilité de l'information. Les mesures minimales vont en croissant du profil A au profil C et sont proportionnelles aux risques encourus.

4 

Réaliser une revue diligente conjointe (ITQ/OP)

Une revue diligente est conjointement réalisée par l'OP et ITQ. Des ajustements sont encore possibles à cette étape.

5 

Déterminer les responsabilités

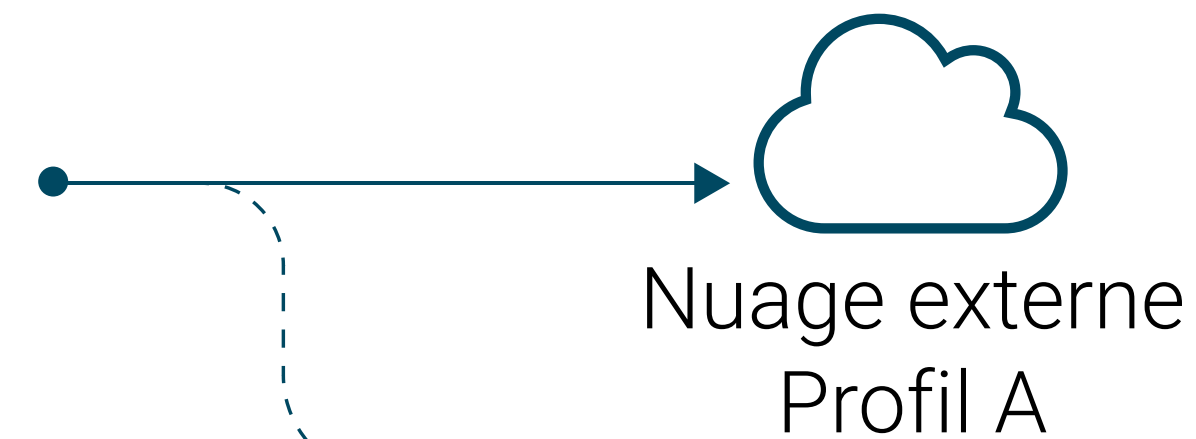
Les responsabilités des parties prenantes (OP, fournisseur, ITQ) sont clairement déterminées par l'OP, en fonction du modèle d'infonuagique retenu et du profil correspondant.

6 

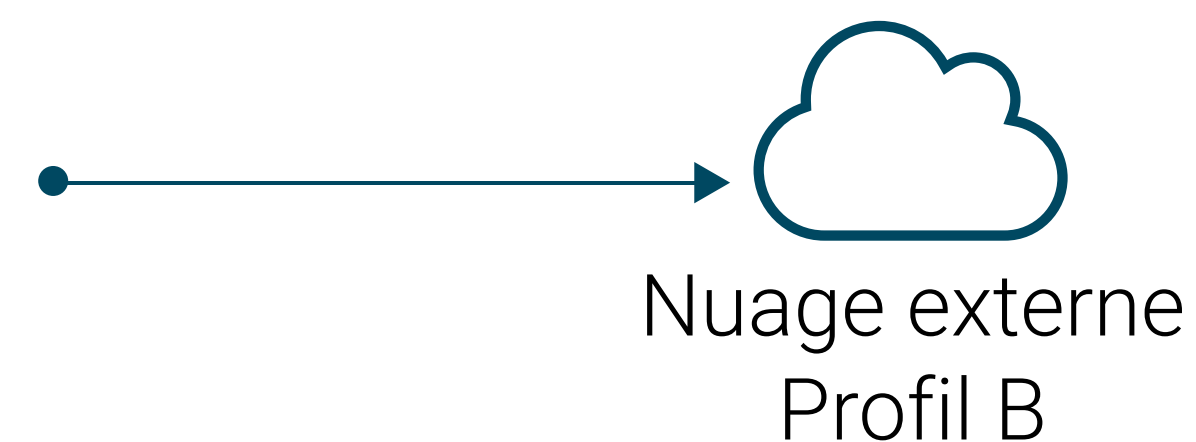
Gérer les risques de sécurité de l'information

Le passage en mode exploitation de la solution infonuagique retenue par l'OP n'est possible que si ce dernier a l'assurance que les **risques afférents ont été analysés**, qu'ils sont **acceptés**, aussi bien par lui-même qu'au plan gouvernemental, et qu'un **processus de surveillance** continu de leur évolution est mis en place.

Information non-sensible

Nuage externe
Profil A

Information sensible

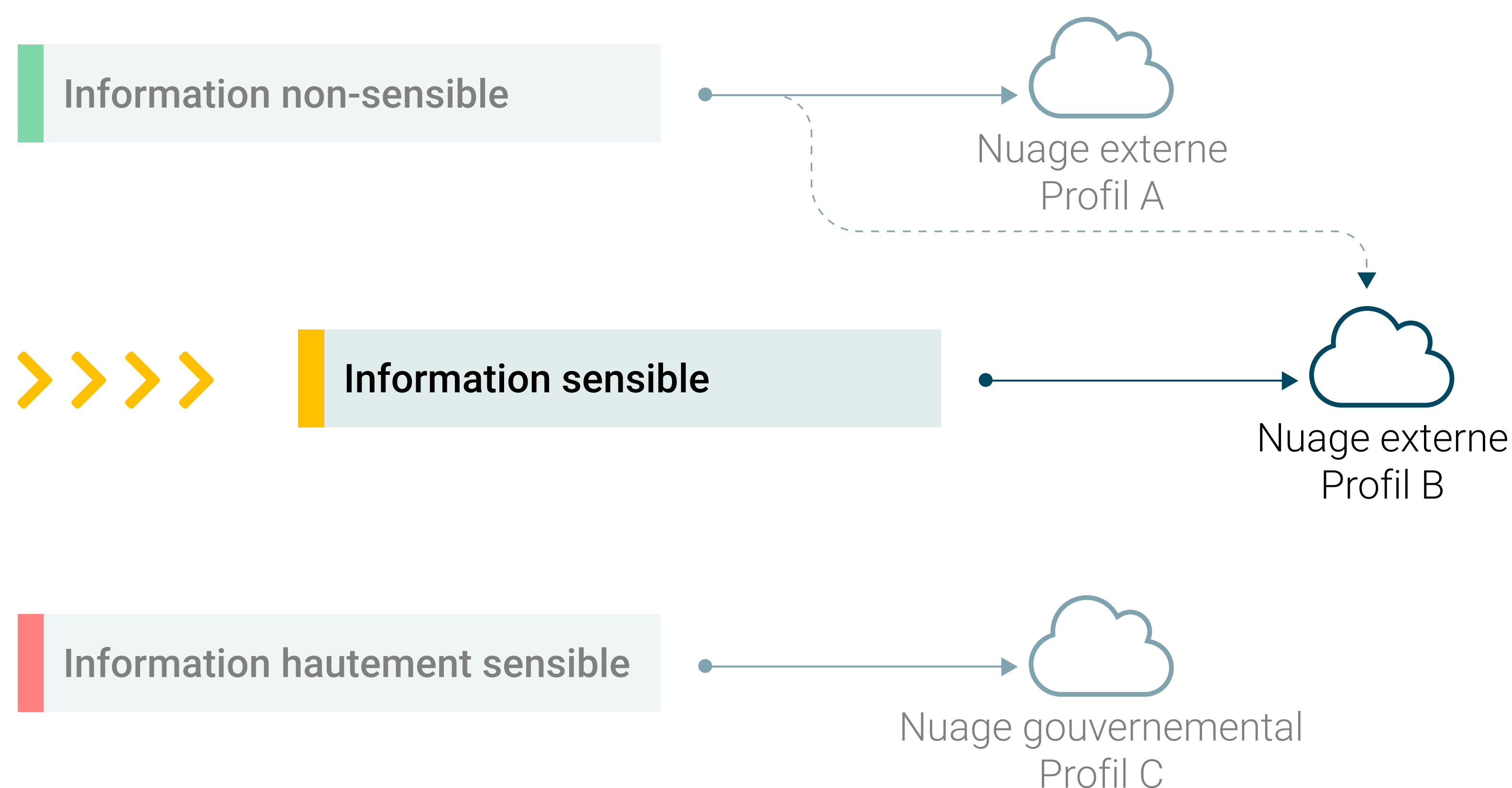
Nuage externe
Profil B

Information hautement sensible

Nuage gouvernemental
Profil C

1 **Identifier les actifs**

La compromission de la confidentialité ou de l'intégrité peut engendrer des préjudices modérés. L'information est classée « **sensible** ».

2 **Évaluer la sensibilité de l'information gouvernementale**3 **Choisir le modèle infonuagique approprié**

L'OP a choisi de migrer son système dans le nuage externe avec les mesures de protection des informations de nature **sensible**, répondant au **Profil B**.

4 **Réaliser une revue diligente conjointe (ITQ/OP)**

Une analyse est conjointement réalisée par l'organisme public détenteur de l'information et ITQ quant au choix du mode de traitement et de stockage et des mesures de sécurité applicables.

5 **Déterminer les responsabilités**

L'OP a déterminé les responsabilités suivantes :

- Le fournisseur offre la capacité de chiffrer les données stockées.
- L'organisme public chiffre les données stockées avec ses propres clés de chiffrement.

6 **Gérer les risques de sécurité de l'information**

L'OP procède à une analyse des risques pour :

- Rechercher de nouvelles failles de sécurité et les corriger.
- Identifier de nouvelles menaces.
- Déployer les mesures supplémentaires de protection.
- Mettre en place un processus de surveillance de l'évolution des risques de sécurité.
- Passer en mode exploitation après avoir accepté les risques résiduels.