

## Points d'attentions de gouvernance et cyber sécurité

### Instaurer une politique et un cadre d'usage, d'accès, de partage et de protection de la donnée.

- **Définir sa stratégie et choisir le pilote de données** (Congo Stratégie Nationale de partage et d'accès aux données)  
Quelles sont les données à protéger et lesquelles libérées ? Cela passe par la classification des données et d'en libérer celles qui faut pour rendre possible le BigData
- **Principaux défis c'est le captage des données ou** Systématiser la captation des données à travers différents points
- **Favoriser l'interopérabilité pour permettre l'interconnexion entre les différentes données.**

Sans socle technologique moderne et ouvert en matière de données, les entreprises seront incapables de collaborer facilement et rapidement.

Interfaçage avec les outils et points de contact existants : comment systématiser la captation des informations clients sur les différents points de contact ? Comment connecter des technologies très hétérogènes, souvent très différentes, parfois dépassées, de manière fiable aujourd'hui comme demain ?

### Cybersécurité

Le mot cybersécurité est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non-répudiation)

Défis

- **Maîtriser les enjeux légaux de la donnée**

la perte économique : la violation des données de l'entreprise ou de l'organisme est susceptible de freiner voire d'interrompre son activité et donc de porter atteinte à sa productivité et à sa compétitivité, atteinte à la réputation et à l'image de l'entreprise, de la marque ; perte de confiance des utilisateurs, des consommateurs, du public.

- **Maitriser le contrôle des systèmes (dispositif technique et organisationnel)**

- Construction des infrastructures notamment des centres de calculs, ou de l'exploitation de celles disponibles
- Renforcement des capacités techniques (formation)
- Sensibilisation des populations pour la prise de consciences et des risques associés
- Comprendre les organisations à mettre en place pour structurer les données en lien avec les politiques de confidentialité