AUTORITÉ DES MARCHÉS FINANCIERS

JOURNÉE PROFESSIONNELLE EN AIPVP
9 février 2023
LOI 25 – LES DISPOSITIONS LÉGALES ET LES MESURES ADMINISTRATIVES EN PROTECTION DES RENSEIGNEMENTS PERSONNELS-

L'INTÉGRATION DES ENJEUX EN SÉCURITÉ NUMÉRIQUE DANS VOS PRATIQUES EN PROTECTION DE LA VIE PRIVÉE (PVP)

VERSION EXPRESS

Conférencier:

- **M. Mark Kaven Lamothe Lafrenière, CD,** directeur de la sécurité de l'information, responsable organisationnel en sécurité de l'information, Direction principale des technologies de l'information, Autorité des marchés financiers

SOMMAIRE DE LA PRÉSENTATION

Les technologies de l'information font partie du travail au quotidien et nombre de tâches sont désormais effectuées grâ[illegible]'informatique. Les experts en PRP et ceux de la Sécurité de l'infor[illegible]es TI doivent travailler en collaboration pour garantir la PV[illegible]jours et à tous les niveaux.

30 MIN !!

- Comment intégrer d[illegible]aisonnables compte tenu des renseignements colle[illegible]isés et communiqués?
- Quelles sont les questi[illegible]s que l'un à l'autre doivent se poser et pourquoi?
- La présentation permettra aux professionnels de se constituer leurs propres outils d'analyse.

REMARQUES PRÉLIMINAIRES

- Plusieurs éléments sont basés sur un retour d'expérience dans notre contexte. Ces éléments peuvent être inspirants, mais doivent être adaptés à votre contexte.

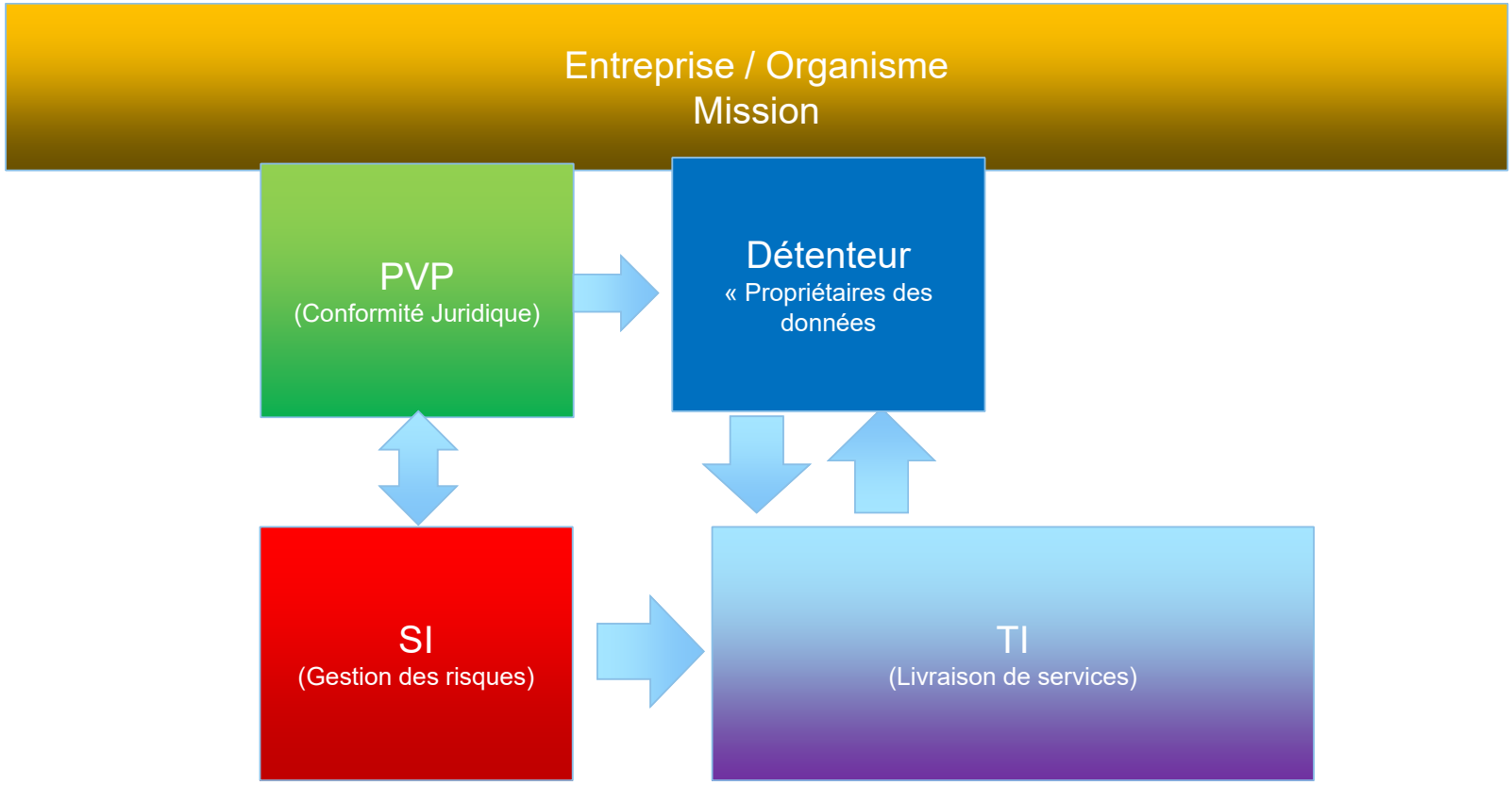
#WHOAMI

- Analyste en renseignement militaire – Forces Armées canadiennes
  - Cmdt-Adjoint du détachement de cybersécurité Montréal - (CFNOC) (2014)

- Responsable de la sécurité de l'information numérique
  - Coordonnateur organisationnel en gestion d'incident (2015-2021)
- Directeur de la sécurité de l'information
  - Responsable organisationnel en sécurité de l'information (2021-…)

AUTORITÉ DES MARCHÉS FINANCIERS

L'ÉQUIPE PROJET

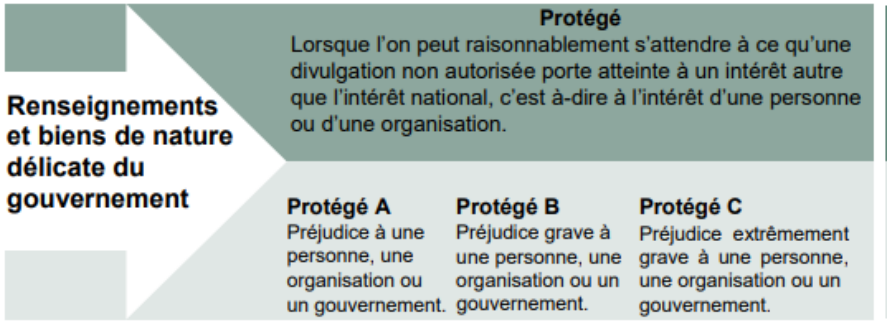


QUESTIONS IMPORTANTES EN SI/TI

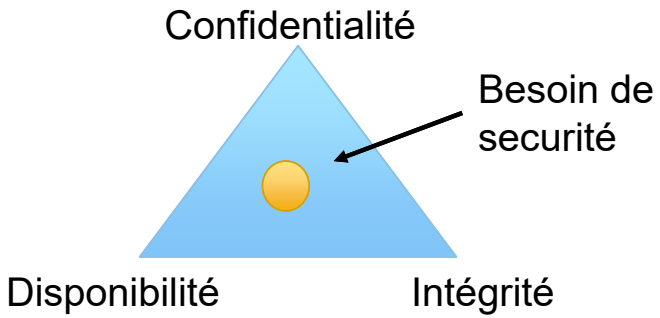
- (SI) Suis-je en présence de Renseignements personnels?
- (SI) Quel **niveau de protection** dois-je apporter à ces informations?
- (PVP) Les mesures de protection et le risque présenté répond-il a mes obligations en matière de PVP?
- (PVP) Quel est le besoin d'affaire et quelles sont les obligations de l'organisation en matière de PVP dans ce domaine?

LA BASE - CONNAITRE LA SENSIBILITÉ DES RP CONCERNÉS

- Bien que confidentiels au sens de la loi, tous les RP n'ont pas les mêmes **impacts** en cas de bris de sécurité. Le contexte revêt son importance:
  - Vos coordonnées
  - Votre T4/Relevé 1
  - Un dossier médical
  - Un dossier criminel



Source: Gouvernement du canada



LA SÉCURITÉ DE L'INFORMATION UNE GESTION DE RISQUE

Évaluer la sensibilité de l'information dans son contexte

Identifier les requis légaux

Évaluer les menaces

Identifier les vulnérabilités

Évaluer les risques inhérents

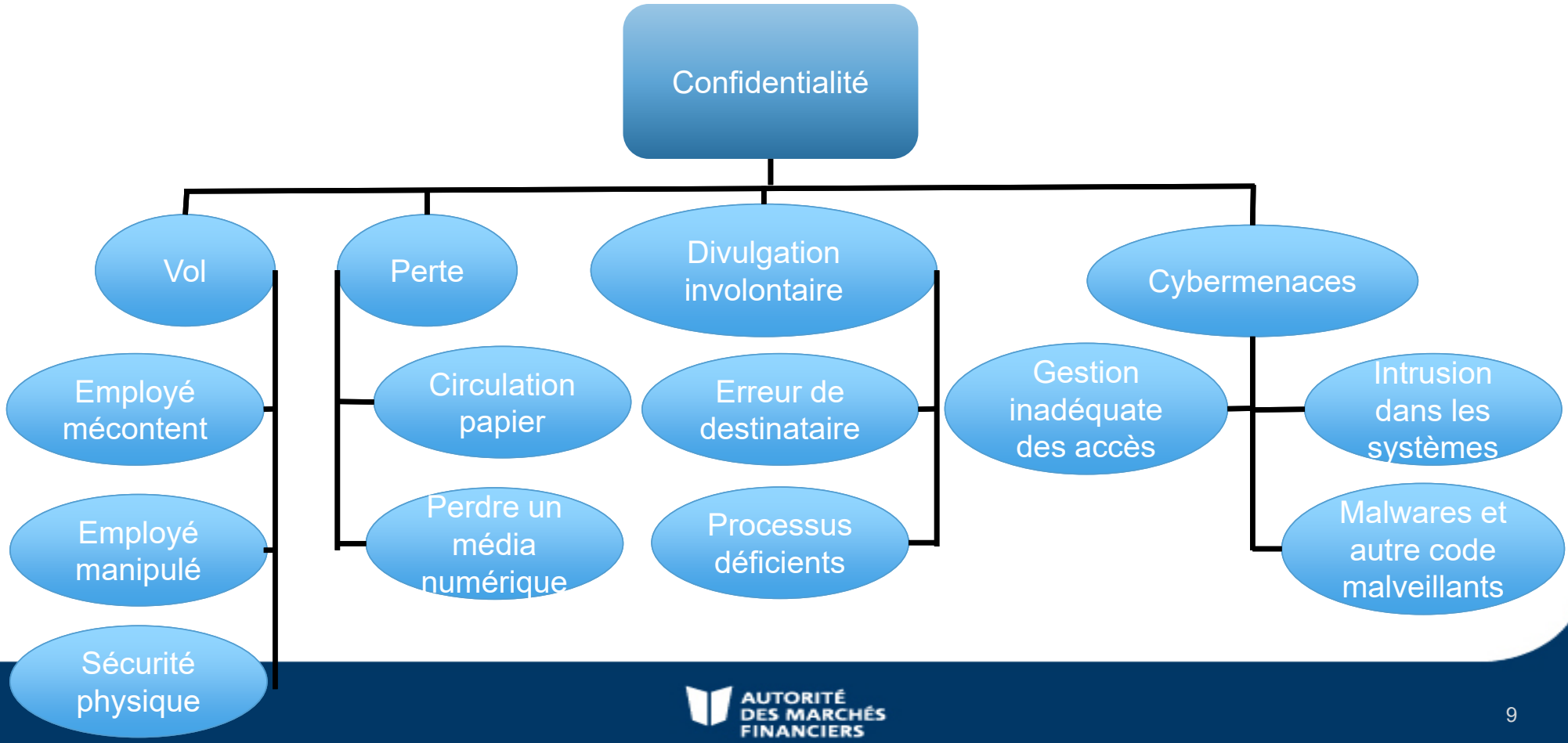
Identifier les contrôles en place

Implanter des contrôles de mitigation des risques

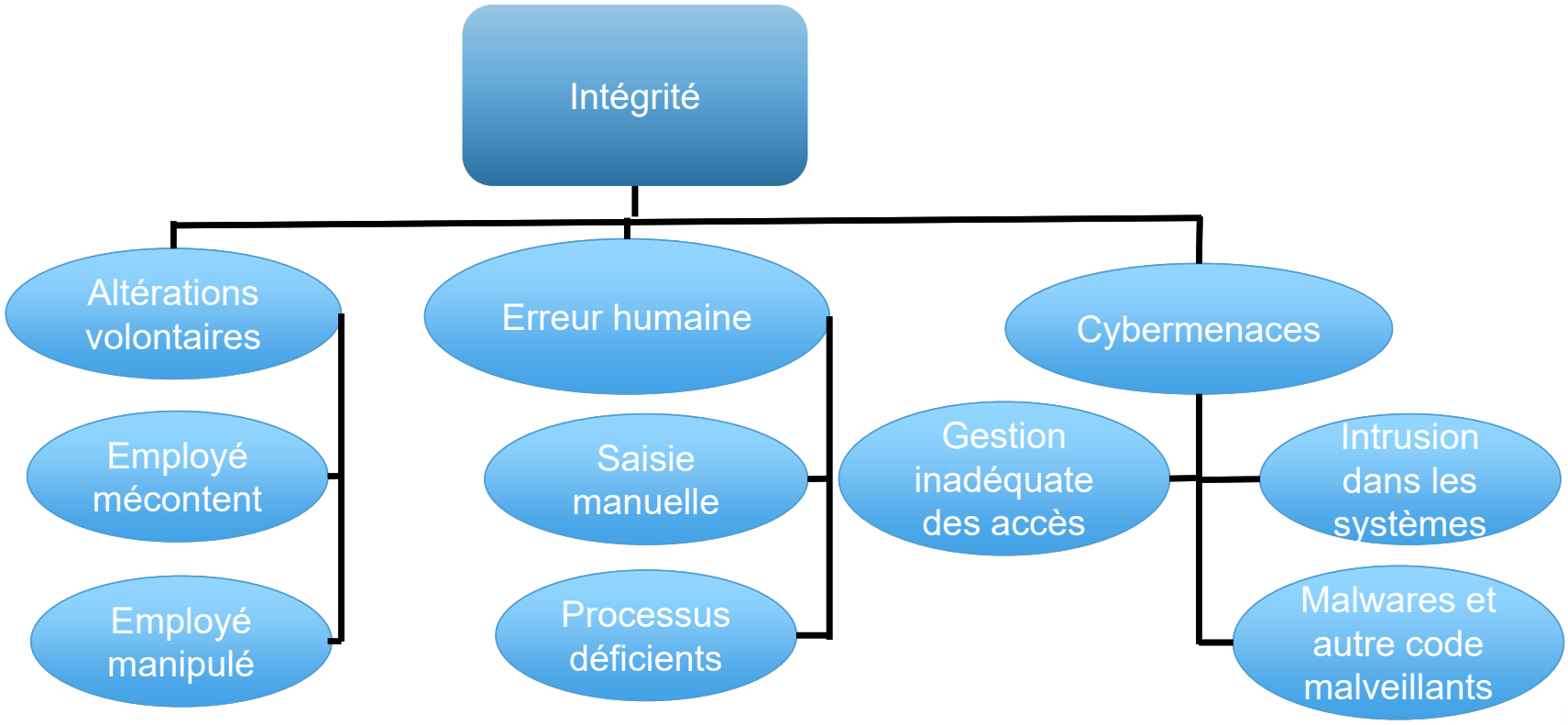
Évaluer le risque résiduel

S'assurer que le risque est dans l'appétit du risque de l'organisation

MENACES TYPIQUES (NON EXHAUSTIVES)



MENACES TYPIQUES (NON EXHAUSTIVES)

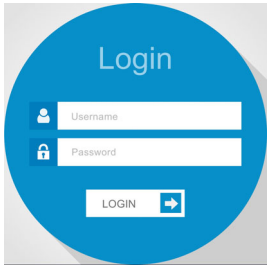


AUTORITÉ DES MARCHÉS FINANCIERS

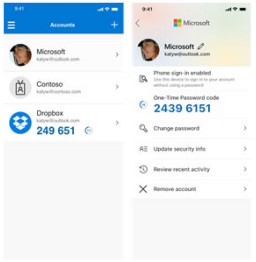
COMPRENDRE LES CONTRÔLES COMMUNS

* En l'absence d'un professionnel de la SI

QUEL EST LE NIVEAU D'AUTHENTIFICATION?



- Identification (public, Faible, (A))
  - Identifier l'usager d'un système
  - Habituellement : Usager / Mot de passe (12+)
- Authentification (Modéré, Élevé, (B-C))
  - Preuve que la personne effectuant les actions sur un système est celui identifié
  - Authentification multifactorielle
    - Identifiant
    - Mot de passe
    - Un jeton ou autre élément possédé par l'utilisateur qui ne peut être copié ou découvert



LES IDENTITÉS ET ACCÈS SONT-ILS CORRECTEMENT GÉRÉS?

- Accès basé sur le besoin de savoir
- Processus de gestion des arrivés, départ, changement de service
- Les accès sont ils journalisés?
  - Combien de temps sont conservés les journaux?
  - Sont-ils lisibles?
- L'Administrateur TI
  - Énormément de droits dans les environnements TI
  - Reddition de compte
  - « One time acess »

OÙ SONT MES DONNÉES?

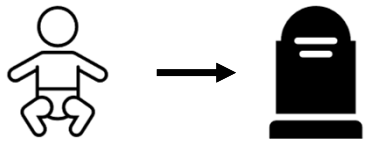
- Dématérialisation du périmètre TI
  - Les données sont-elles à l'interne de l'organisation
  - Sont-elles hébergés chez un fournisseur?
  - Sont-elles dans le nuage?
- Possibilité d'exiger que les données soient dans une zone géographique précise (Canada-Est)
  - Doit être mis en balance avec le besoin de résilience aux désastres
  - ATTENTION! Résilience des infrastructures ne signifie pas qu'elles sont sauvegardés!
- Les nouvelles fonctionnalités infonuagiques

CHIFFREMENT DES DONNÉES

- Chiffrer c'est bien, mais qui à la clé?
  - L'organisation?
  - Le fournisseur infonuagique?
- Types de chiffrement:
  - Chiffrement en transit
  - Chiffrement au repos
- Normes de chiffrement
  - PCI-DSS une valeure sure

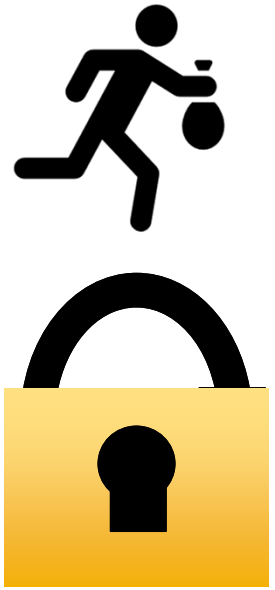
A QUI APPARTIENDRONT LES DONNÉES ET RENSEIGNEMENTS PERSONNELS?

- Certains fournisseurs veulent vos données.
  - Si c'est gratuit, vous êtes le produit!
  - Amélioration du produit
  - Statistiques
  - Revente commerciale
- Selon le besoin, assurez-vous que votre organisation demeure propriétaire des données tout au long de son cycle de vie.
  - N'oubliez pas les sauvegardes!



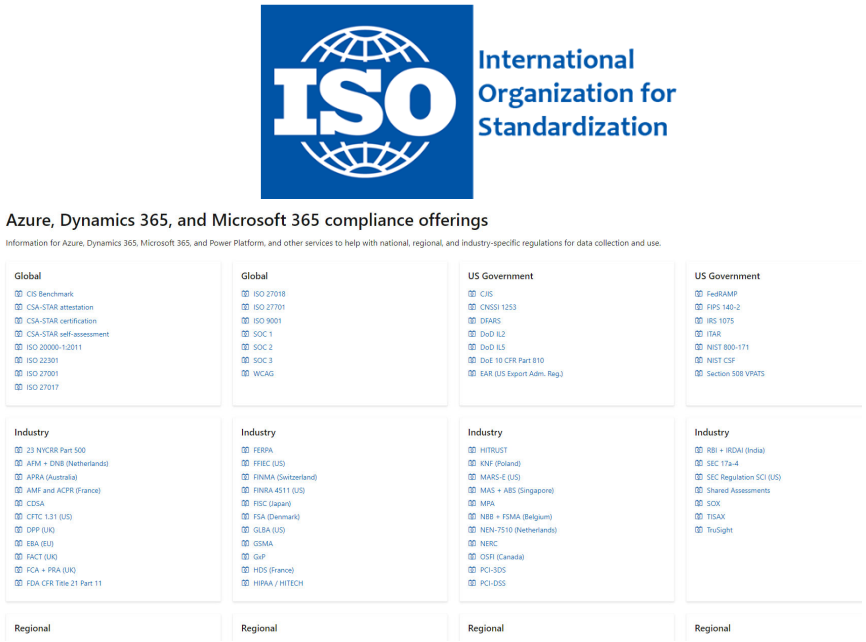
LA SÉCURITÉ PHYSIQUE EXISTE ENCORE!

- Les documents
- Sécuriser les locaux et les contenants
- Les médias numériques
- Les antécédents des employés et fournisseurs
- La destructions sécuritaire
  - Des documents
  - Des médias numérique
  - Des supports informatiques
- Vos fournisseurs sont-ils sécurisés?



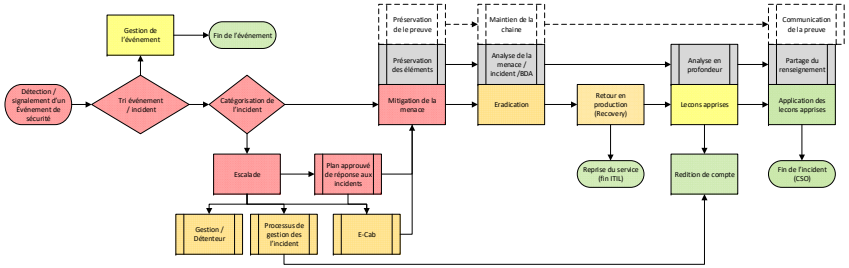
ÉVALUER UN GAFAM OU AUTRE?

- David contre Goliath?
- Les certifications de sécurité
  - ISO 27001, 27018…
  - CSAE3416
  - SOC II Type 2
  - ISAE 3402
  - PCI-DSS?
- Les tests de sécurité
  - Tests d'intrusions



SE PRÉPARER A UN INCIDENT DE PVP

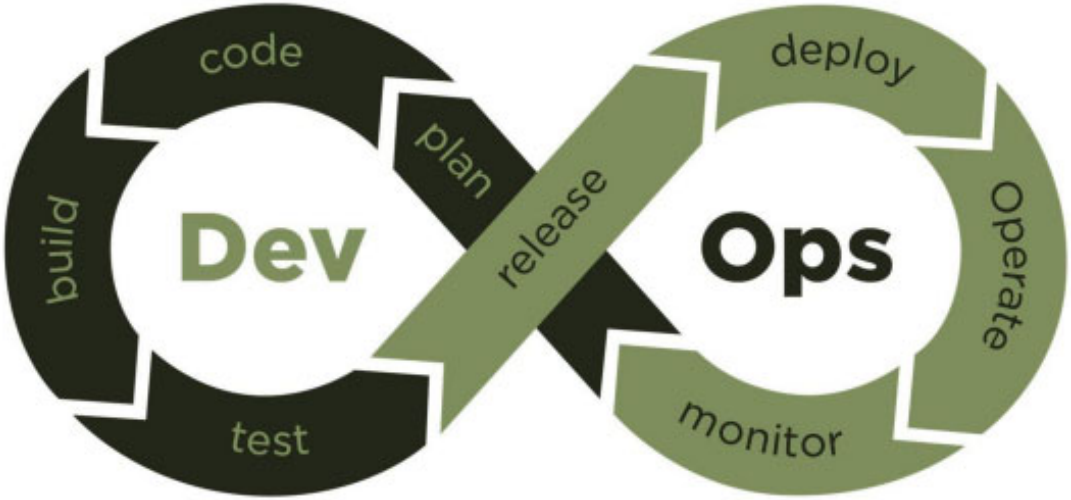
- Faire l'évaluation d'impact en amont
- Préparer ses scénarios d'intervention
- Définir les rôles et responsabilités au sein du plan de gestion d'incident
- S'assurer de pouvoir recevoir un signalement en PVP
- Savoir comment déclarer l'incident à la CAI



LES PIÈGES

- Sur classifier / catégoriser son information
  - Devient un bloquant à l'atteinte de l'objectif de l'organisation
- Ne pas comprendre le contexte d'affaire
  - Protéger un concours vs les relevés fiscaux
- Considérer le représentant en SI comme le détenteur d'actif et du risque
  - Vous devez vous impliquer auprès du détenteur pour le sensibiliser à ses obligations en matière de PVP
- Ne pas se préparer a un incident en PVP

L'APPROCHE DEVSECOPS



CONCLUSION

- L'intervenant en PVP est un **intervenant à part entière** dans la gouvernance des données d'une organisation
- Il est souvent **complémentaire à une équipe en SI** qui doit assurer la Disponibilité, Intégrité et Confidentialité de l'information
- Développer sa maturité en matière de **catégorisation des l'information** est impératif
- Les **contrôles de bases** sont souvent les plus efficaces pour gérer la protection de la vie privée.

AUTORITÉ DES MARCHÉS FINANCIERS

QUESTIONS?

Merci!