Technologies de l'information

Cours:

Sécurité des systèmes informatiques

DESS

Séance # 3

Préparé par: Blaise Arbouet

Contenu de la séance

- Pratique WoocLap
- Matrice de classification
- Cours # 3
- Quizz noté

Objectif de la séance

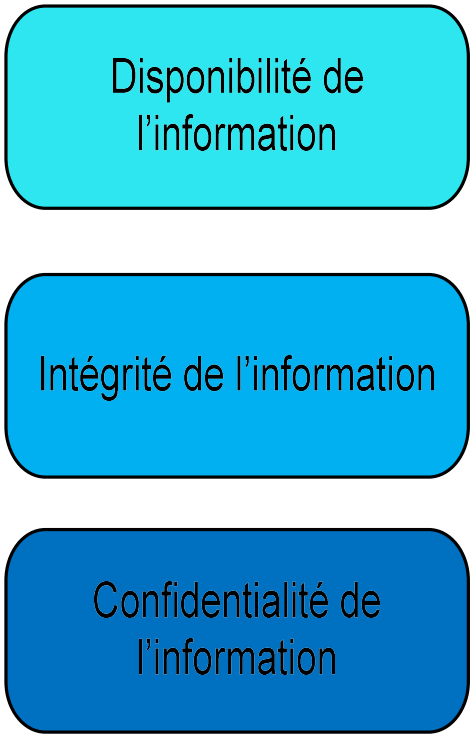
Comprendre les concepts de base en sécurité de l’information et reconnaitre les différents cadres de gouvernance et des stratégies en cybersécurité.

Sécurité de l’information

- Quoi protéger?
- Les **propriétés** de l’information notamment :
  - Sa disponibilité ;
  - Son intégrité ;
  - Sa confidentialité.

Sécurité de l’information

- Disponibilité :
  - Rendre l’information accessible et utilisable sur demande par une entité autorisée lorsque nécessaire.
- Intégrité :
  - Sauvegarder la cohérence, l’exactitude et l'exhaustivité de l’information.
- Confidentialité :
  - S’assurer que l’information n’est pas mise à la disposition ou divulguée à des personnes, des entités ou des processus non autorisés.



Source: Tarantino p.174

Autres définitions

GESTION DE RISQUE: le processus qui permet d'identifier et d'évaluer les risques en vue d'élaborer un plan visant à minimiser et à maîtriser ces risques et leurs conséquences potentielles pour une entreprise.

ACTIF: Ce qui est important pour l'organisation

MENACE: Quelque chose qu'on droit craindre

VULNÉRABILITÉ: Une faille ou une faiblesse d'un actif

RISQUE: L**a vraisemblance qu'une menace exploite une vulnérabilité afin d'impacter un actif**.

Survol de la notion de gouvernance

Gouvernance

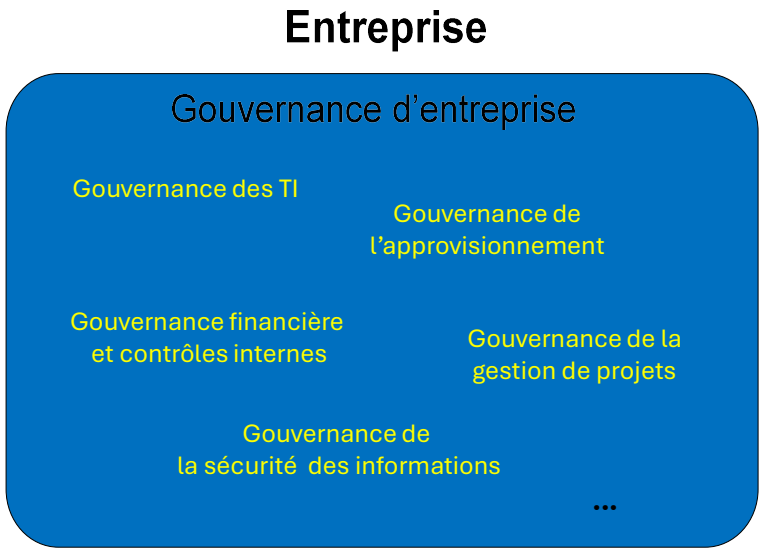
- Une définition

  « Manière d'orienter, de guider, de coordonner les activités d'un pays, d'une région, d'un groupe social ou d'une organisation privée ou publique »*

Source: Grand dictionnaire terminologique

Différents types de gouvernance

- La gouvernance d'entreprise couvre **plusieurs domaines** avec comme objectif principal l'atteinte des objectifs de l'organisation



La gouvernance de la sécurité de l’information

Objectifs de la gouvernance de la sécurité de l’information

- La livraison de valeur à l’entreprise en s’assurant de fournir de l’information **sûre**, **fiable** et **complète** en tout temps, et de protéger les actifs informationnels de l’entreprise.

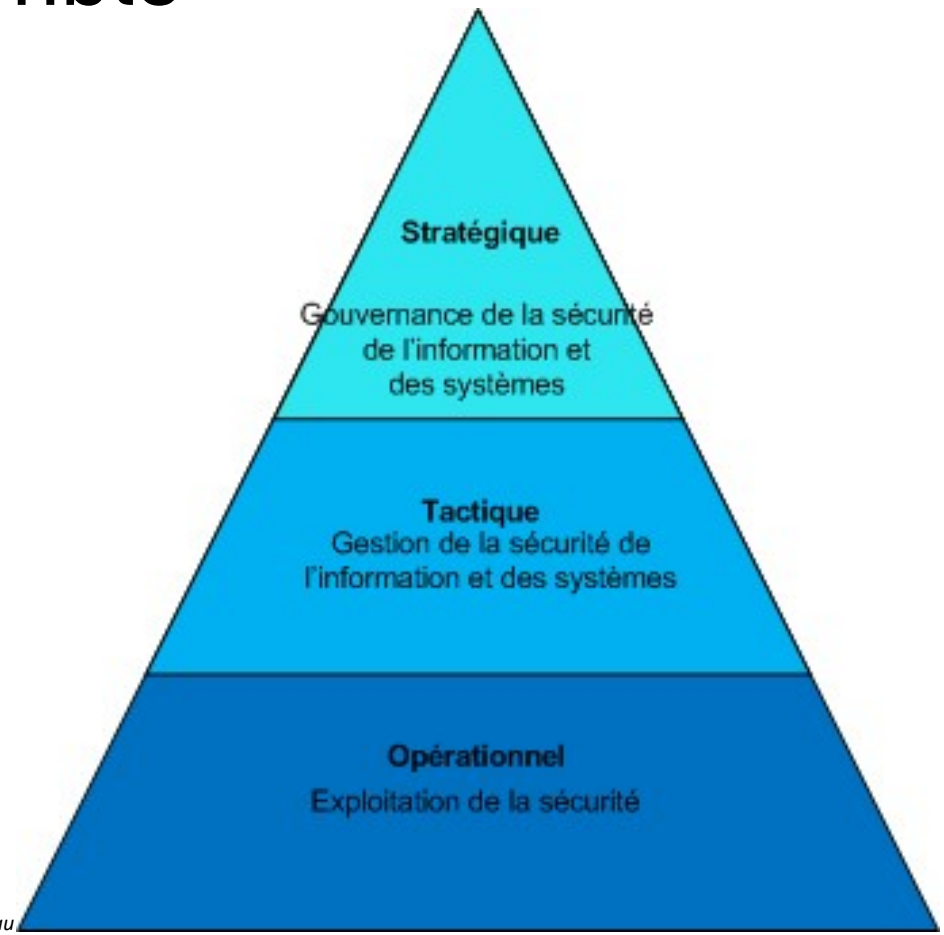
Objectifs de la gouvernance de la sécurité de l'information

- Mettre en place des processus décisionnels adéquats et définir les rôles et responsabilités, afin de s'assurer d'une saine gestion de l'entreprise, ainsi que le respect des lois, des exigences réglementaires et des contrôles internes auxquels elle est assujettie.

Défis

- Adhésion et appui de la haute direction
- Positionnement de la gestion de la sécurité de l’information
- Efforts en sécurité souvent fragmentés
- Disponibilités des ressources
- Culture de l’entreprise

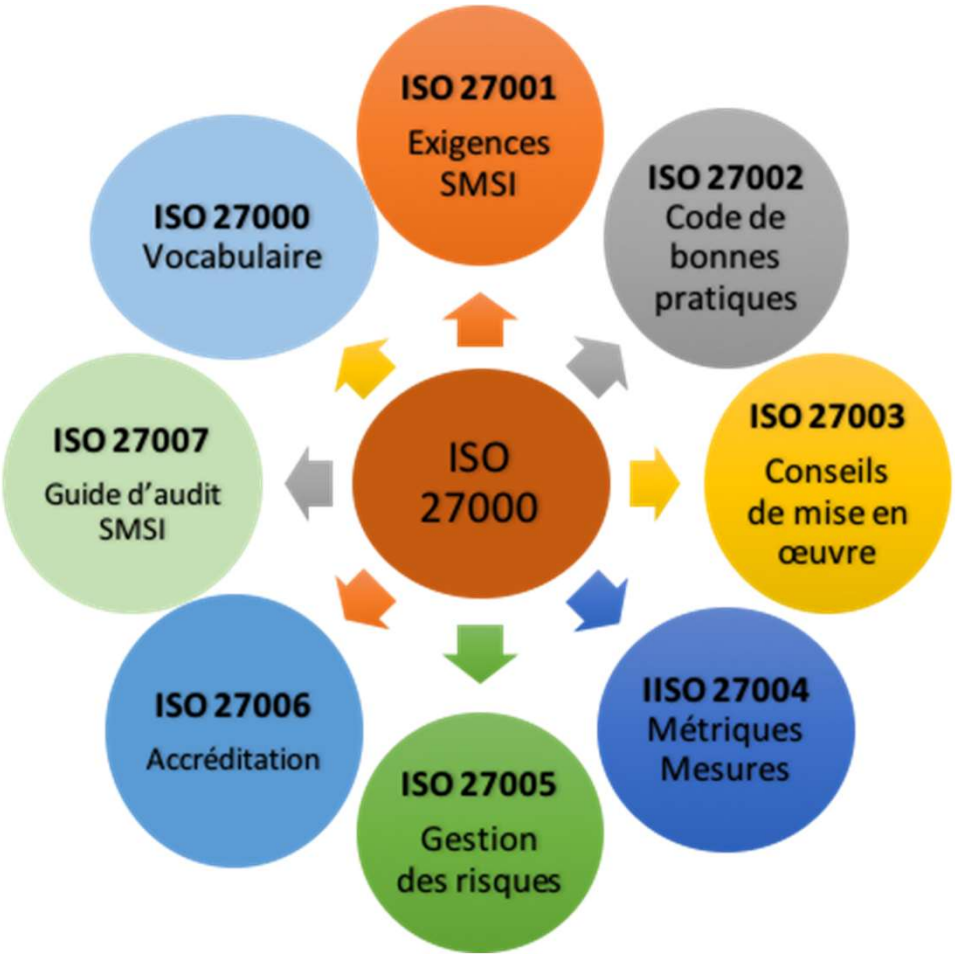
Vue d’ensemble



Source: Pellerin, Pilon, Thibodeau

Survol de quelques cadres de gouvernance en sécurité de l'information

Survol de la famille ISO 27000



La série de normes ISO/IEC 27000

Un SMSI (système de management de la sécurité de l'information) selon la norme ISO/IEC 27001.

La norme ISO/CEI 27002: fournit des conseils aux organisations cherchant à établir, mettre en œuvre et améliorer (SMSI).

ISO 27005 est la norme qui décrit comment réaliser une évaluation des risques liés à la sécurité de l'information conformément aux exigences de la norme ISO 27001.

La norme ISO/IEC 27001

ISO/IEC 27001 est la norme la plus connue au monde pour les systèmes de gestion de la sécurité de l'information (ISMS). Il définit les exigences auxquelles un SMSI doit répondre.

La norme ISO/IEC 27001 fournit aux entreprises de toute taille et de tous secteurs d'activité des lignes directrices pour établir, mettre en œuvre, maintenir et améliorer continuellement un système de management de la sécurité de l'information.

Mise en place SMSI

La mise en place d’un **Système de Management de la Sécurité de l’Information (SMSI)** repose sur la norme **ISO/IEC 27001** et suit une approche systématique basée sur l'amélioration continue. Voici les étapes essentielles:

- Définition des objectifs et de la portée
- Engagement de la direction et gouvernance
- Analyse des risques liés à la sécurité de l’information
- Sensibilisation et formation des employéition et mise en œuvre des mesures de sécurité
- Surveillance et amélioration continue
- Certification (optionnelle)

Définition des objectifs et de la portée

Identifier les besoins et les attentes des parties prenantes.

Définir les objectifs du SMSI alignés avec la stratégie de l'organisation.

Déterminer le périmètre du SMSI (services, processus, sites concernés).

Engagement de la direction

OBTENIR LE SOUTIEN DE LA DIRECTION POUR GARANTIR LES RESSOURCES NÉCESSAIRES.

DÉSIGNER UN RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSSI).

DÉFINIR UNE POLITIQUE DE SÉCURITÉ DE L'INFORMATION (PSI).

Analyse des risques liés à la sécurité de l’information

- Identifier les actifs informationnels et les menaces associées.
- Évaluer les vulnérabilités et les impacts potentiels.
- Appliquer une méthodologie de gestion des risques (ISO 27005, EBIOS, MEHARI, etc.).
- Mettre en place un plan de traitement des risques (réduction, transfert, acceptation, évitement).

Définition et mise en œuvre des mesures de sécurité

Sélectionner et appliquer des mesures de sécurité basées sur l'**Annexe A** de l'ISO 27001.

Mettre en place des contrôles techniques, organisationnels et humains (chiffrement, authentification, sensibilisation, etc.).

Rédiger et diffuser les procédures et politiques de sécurité

Sensibilisation et formation des employés

ORGANISER DES FORMATIONS SUR LA SÉCURITÉ DE L'INFORMATION.

SENSIBILISER AUX BONNES PRATIQUES ET AUX MENACES (PHISHING, INGÉNIERIE SOCIALE, ETC.)

Surveillance et amélioration continue

Définir des indicateurs de performance et des audits internes.

Mettre en place un processus de gestion des incidents de sécurité.

Réaliser des revues de direction pour évaluer l'efficacité du SMSI.

Améliorer continuellement le système en appliquant le cycle **PDCA (Plan-Do-Check-Act)**

Certification (optionnelle)

Réaliser un audit interne pour évaluer la conformité avec ISO 27001.

Effectuer un audit externe par un organisme de certification accrédité.

Obtenir la certification ISO 27001 et assurer sa maintenance annuelle.

Différence entre ISO 27001 et ISO 27002

	ISO 27001	ISO 27002
Définition	Norme qui explique comment concevoir le système de gestion de la sécurité de l'information	Norme supplémentaire pour implementer les contrôles de sécurité
Description	Liste les contrôles de sécurité dans l'annexe A	Donne des détails sur comment implémenter chaque contrôle de sécurité dans l'annexe A
Certification	Oui	Non

Annexe A. Contrôles de sécurité de l'information ISO 27001: 2022

Nombre total de contrôles – 93, dont 11 nouveaux (2022)

Les contrôles sont classés comme suit :

a) Les personnes, si elles concernent des personnes individuelles

b) Physiques, s'ils concernent des objets physiques

c) Technologiques, s'ils concernent la technologie

d) sinon, ils sont classés comme organisationnels

La norme ISO/IEC 27002

ISO/IEC 27002 EST UNE NORME INTERNATIONALE QUI FOURNIT DES CONSEILS AUX ORGANISATIONS CHERCHANT À ÉTABLIR, METTRE EN ŒUVRE ET AMÉLIORER UN SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION (ISMS) AXÉ SUR LA CYBERSÉCURITÉ.

ALORS QUE LA NORME ISO/IEC 27001 DÉCRIT LES EXIGENCES D'UN SMSI, LA NORME ISO/IEC 27002 PROPOSE LES MEILLEURES PRATIQUES ET LES OBJECTIFS DE CONTRÔLE LIÉS AUX ASPECTS CLÉS DE LA CYBERSÉCURITÉ, NOTAMMENT LE CONTRÔLE D'ACCÈS, LA CRYPTOGRAPHIE, LA SÉCURITÉ DES RESSOURCES HUMAINES ET LA RÉPONSE AUX INCIDENTS.

ISO 27001:2013 (plus utilisée)

La version de 2013 avait 114 contrôles pour 14 domaines.

ISO 27002: 2022

ISO 27002: 2022 -11 nouveaux contrôles ajoutés

Survol de NIST CSF

Présentation de NIST

La version 2.0 a été publiée le 26 février 2024.

- Développé par le National Institute of Standards and Technology (NIST).
- Il vise à améliorer les processus de cybersécurité et de gestion de risque dans des organisations de tous les secteurs.
- Le cadre est largement reconnu pour sa capacité d'adaptation, ce qui permet aux organisations de toutes tailles et de tous types d'appliquer efficacement ses principes.

Composants du NIST CSF 2.0

1) CSF Core : Une taxonomie des résultats de cybersécurité de haut niveau qui peut aider toute organisation à gérer ses risques de cybersécurité.

2) CSF Organizational Profiles : Un mécanisme pour décrire la posture de cybersécurité actuelle et / ou cible d'une organisation en termes de résultats de l'essentiel du CSF.

3) Niveaux CSF : Peut être appliqué aux profils organisationnels CSF pour caractériser la rigueur des pratiques de gouvernance et de gestion de risque de cybersécurité d'une organisation.

Noyaux CSF (CSF Core)

Un ensemble de résultats de cybersécurité classés par fonction, puis catégorie et enfin sous-catégorie, comme le montre la figure 1.

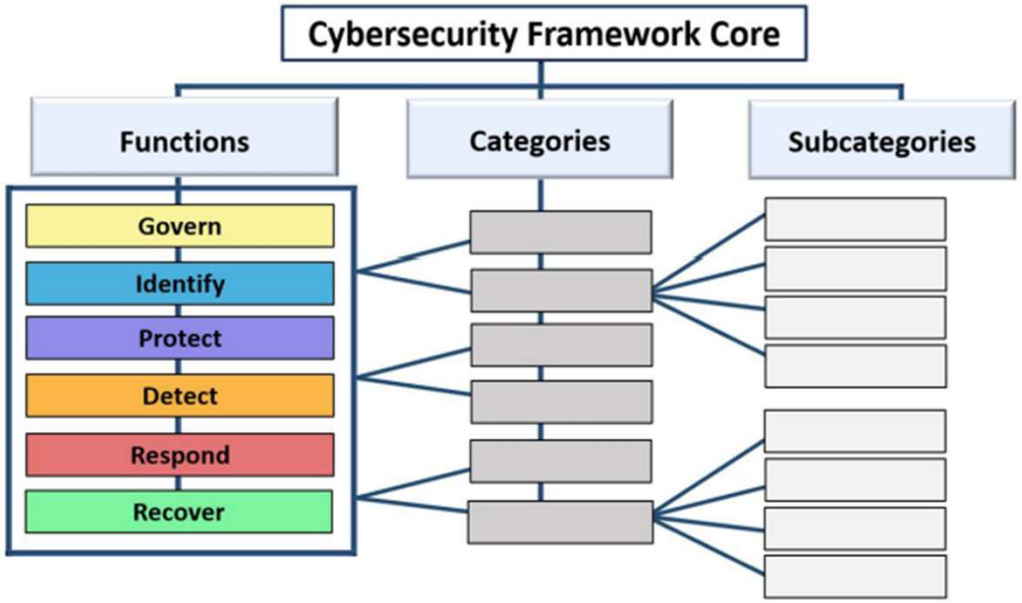
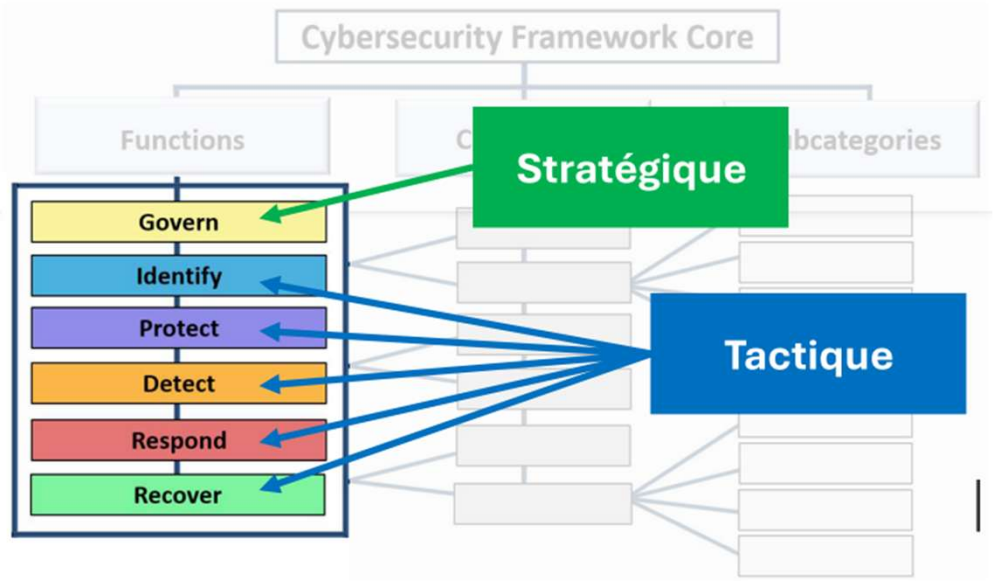


Fig. 1. CSF Core structure

Présentation des noyaux dans la gouvernance



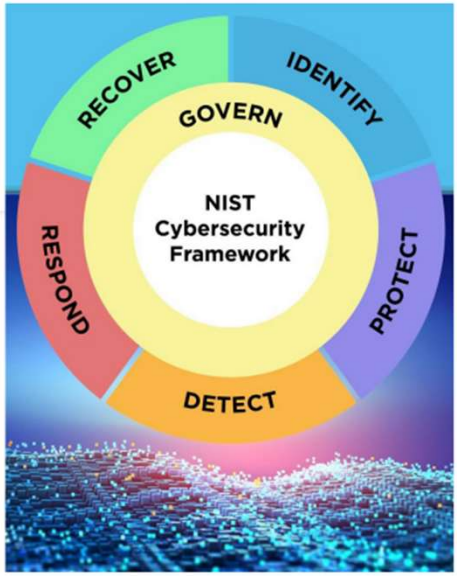
Profil organisanisationnel

- Décrit la posture de cybersécurité actuelle ou cible d'une organisation en termes de résultats en matière de cybersécurité à partir du noyau du Cadre de cybersécurité (CSF).
- Utilisé pour comprendre, adapter, évaluer et hiérarchiser les résultats en matière de cybersécurité en fonction des objectifs de la mission d'une organisation, des attentes des parties prenantes, du paysage des menaces et des exigences.

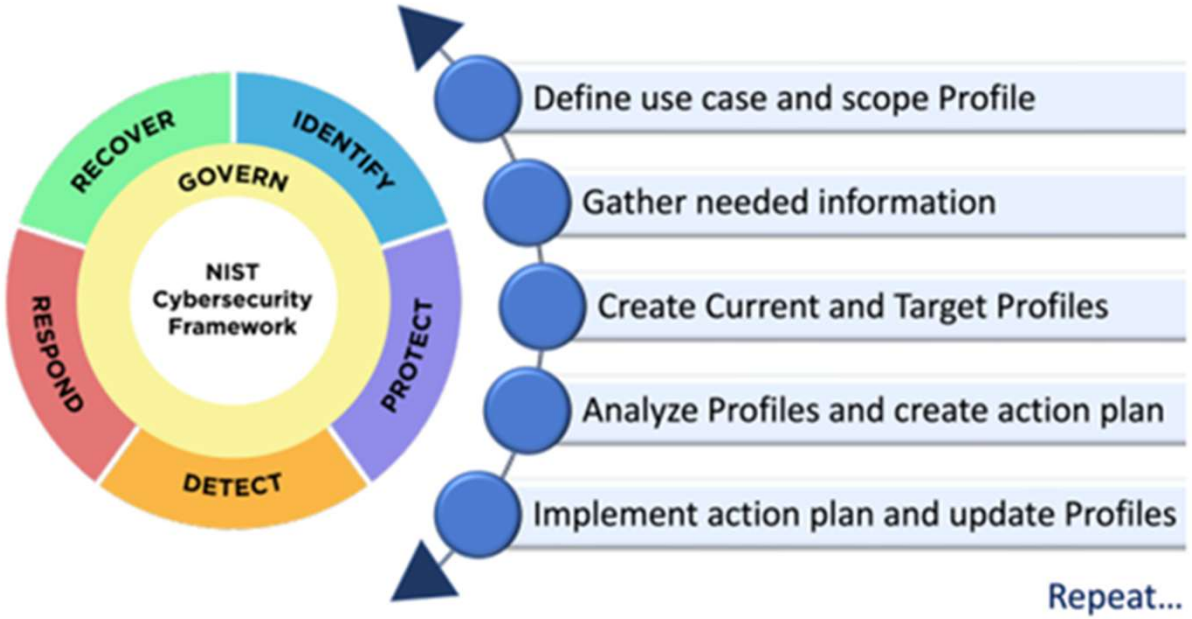
Le 6 fonctions

Les fonctions

- Govern,
- Identify,
- Protect,
- Detect,
- Respond,
- Recover.



Détermination d’un profil organisationnel



Quand les fonctions se produisent?

Les actions qui prennent en charge GOVERN, IDENTIFY, PROTECT et DETECT doivent toutes se produire en continu.

Les actions qui soutiennent RESPOND et RECOVER doivent toujours être prêtes et se produire lorsque des incidents de cybersécurité se produisent.

Les fonctions NIST

GOVERN (GV)

La stratégie, les attentes et la politique de l'organisation en matière
de gestion de risque de cybersécurité sont établies, communiquées et surveillées.

IDENTIFY (ID)

Les risques actuels de cybersécurité de l'organisation sont compris.

PROTECT (PR)

Des mesures de protection pour gérer les risques de cybersécurité de l'organisation sont utilisées.

Les fonctions NIST (suite)

DETECT (DE)
Les attaques et les compromissions possibles en matière de cybersécurité sont trouvés et analysés.

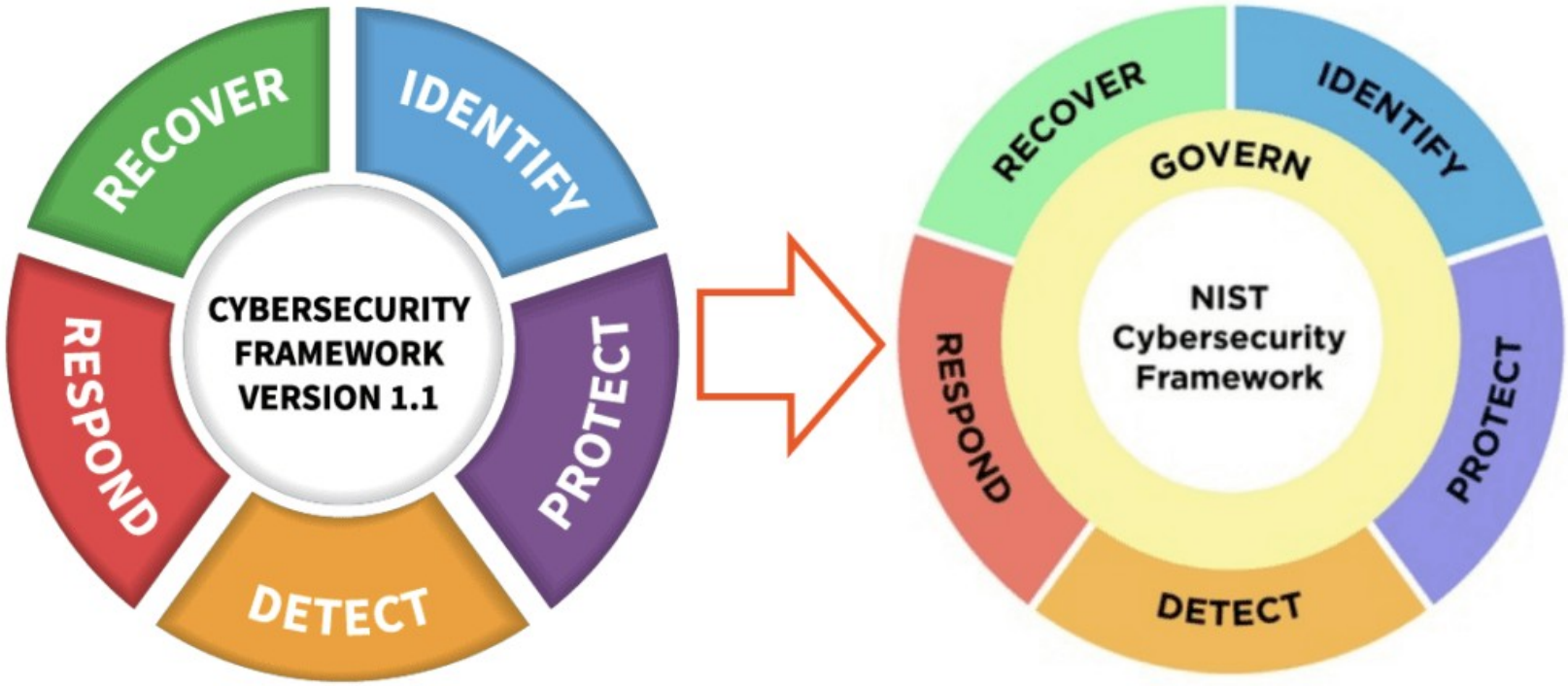
RESPOND (RS)

Des mesures concernant un incident de cybersécurité détecté sont prises.

RECOVER (RC)

Les actifs et les opérations touchés par un incident de cybersécurité sont restaurés.

NIST 1.1 vs NIST 2.0



Survol de CIS

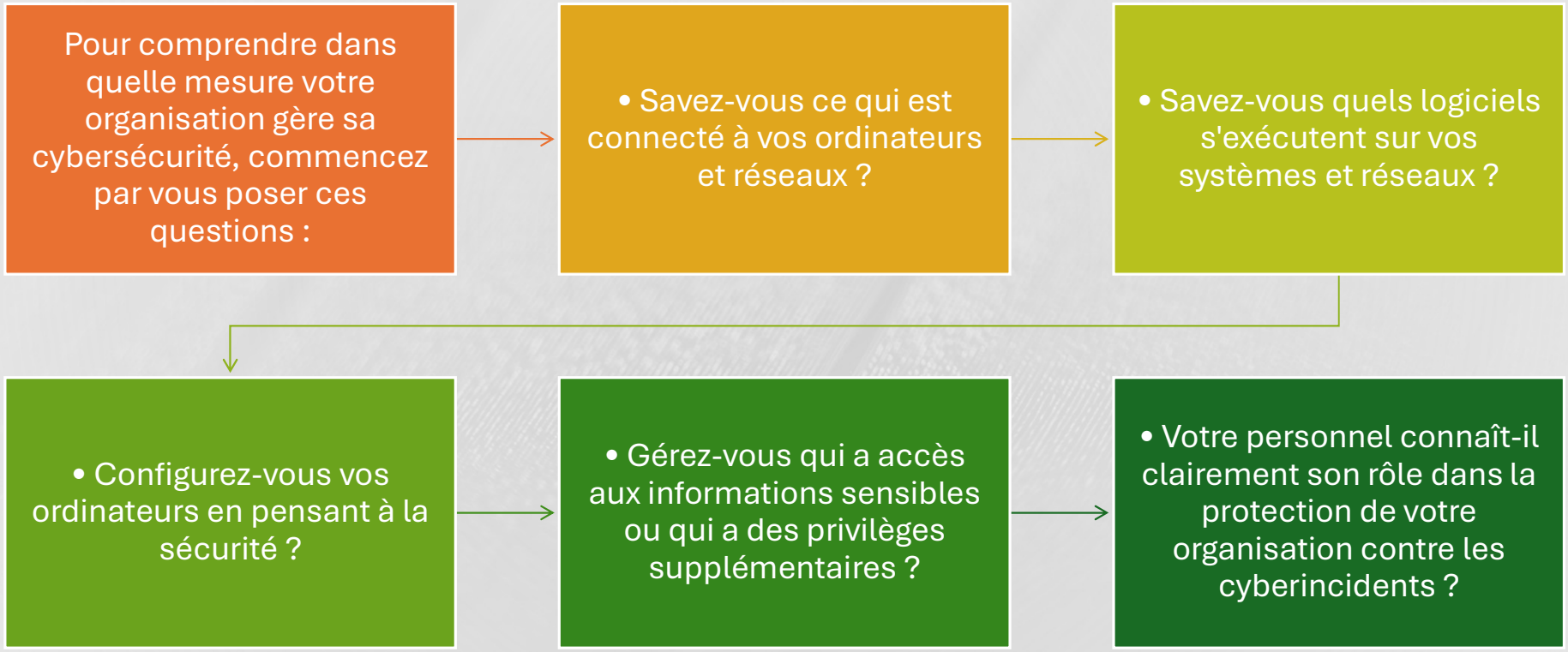
Contrôles CIS

Les contrôles CIS sont un ensemble de mesures de sécurité concrètes et hiérarchisées (appelées safeguards) qui servent à se défendre contre les cyberattaques les plus courantes contre les systèmes et les réseaux.

En particulier pour les organisations qui n'ont pas encore de programme de sécurité en place, ils fournissent des conseils et une assistance précieuse pour démarrer leur propre programme de sécurité. Les contrôles CIS font référence à divers cadres reconnus tels que le NIST CSF, ISO 27000, PCI DSS, etc., et consistent en des mesures concrètes qui peuvent être mises en œuvre de manière pragmatique.

Les 18 contrôles CIS (version 8)

Mise en œuvre des contrôles CIS



Priorité sur les efforts

Phase 1: consiste à connaître ce qui se trouve sur votre réseau et à comprendre vos bases de cybersécurité.

Phase 2: se concentre sur la protection des acquis de sécurité par l'éducation et la prévention.

Phase 3: aide son organisation à se préparer à l'avance à un événement perturbateur (un cyberincident)

Phase 1: Connaitre son environnement

Solutions rentables :

- Nmap : célèbre scanner de réseau polyvalent, utilisé par les administrateurs système et les pirates du monde entier pour identifier les appareils connectés à votre réseau(https://nmap.org/)
- ZenMap : interface utilisateur graphique facile à utiliser pour Nmap (https://nmap.org/zenmap/)
- Spiceworks : logiciel gratuit d'inventaire informatique et de gestion des actifs pour identifier les appareils et logiciel sur votre réseau (https://www.spiceworks.com/)

Phase 2: protéger les actifs

Solutions rentables :

• Bitlocker : chiffrement intégré pour les appareils Microsoft® Windows

(https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx)

• FireVault : chiffrement intégré pour les appareils Mac (https://support.apple.com/en-us/HT204837)

• Qualys Browser Check : outil pour vérifier si votre navigateur est à jour avec tous ses correctifs

(https://browsercheck.qualys.com/)

• OpenVAS : outil permettant d'analyser les systèmes afin de vérifier les bases de sécurité (www.openvas.org)

• Microsoft Baseline Security Analyzer : outil Microsoft® gratuit pour comprendre comment les ordinateurs Windows peuvent être configurés en toute sécurité

(https://www.microsoft.com/en-us/download/details.aspx?id=7558)

• Benchmarks CIS : PDF gratuits avec des directives de configuration consensuelles pour plus de 100 technologies.

Phase 3: Préparer son organisation

Solutions rentables :

• Windows Backup » : outil utilitaire de sauvegarde installé sur les systèmes d'exploitation Microsoft®.(https://support.microsoft.com/en-us/help/17127/windows-back-up-restore)

• Apple Time Machine : outil de sauvegarde installé sur les systèmes d'exploitation Apple®(https://support.apple.com/en-us/HT201250)

• Amanda Network Backup : outil de sauvegarde gratuit et open source (http://www.amanda.org/)

• Bacula : solution de sauvegarde et de restauration réseau open source (http://blog.bacula.org/)

La loi 25

La Loi 25 repose sur des fondements solides qui visent à limiter les incidents de confidentialité dans le secteur privé du Québec. Pour mieux comprendre son impact, explorons:

Ses principaux objectifs,

Les parties concernées et

Ses principales dispositions et ses exigences.

Survol de la Loi 25

Objectifs principaux de la Loi

- Renforcer la protection de la vie privée
- Favoriser la transparence
- Responsabiliser les entreprises
- Harmoniser le Québec avec les standards internationaux

Résumé de la loi

La Loi, adoptée en 2021, modernisant des dispositions législatives en matière de protection des renseignements personnels exige que toutes les organisations soient responsables dans le traitement des renseignements personnels et qu'elles assurent que la cueillette, l'utilisation, la divulgation, la conservation, la protection et la destruction se fassent de manières appropriées.

Qui est concerné par cette Loi?

- Les entreprises privées
- Les Organisations à But Non Lucratif
- Les Institutions publiques
- Les particuliers

Principales dispositions et exigences

- Obtention du consentement
- Droit à la portabilité des données
- Droit à l’oubli

CONSÉQUENCES DIRECTES DE LA LOI 25

SOURCE: https://mylittlebigweb.com/blogue/loi-25/

Comment se conformer?

- **Évaluation initiale**
- **Mise en conformité**
- **Nomination d’un responsable de la protection des renseignements personnels**
- **Évaluation des Facteurs Relatifs à la Vie Privée (EFVP)**

Pénalités

La non-conformité à la Loi 25 peut entraîner des répercussions majeures pour les PME, tant sur le plan légal que financier. Les entreprises qui ne se conforment pas à cette réglementation risquent de lourdes sanctions financières, pouvant s’élever à plusieurs millions de dollars.

Pour les personnes physiques :

- **Manquement mineur à très grave: de 500$ a 50000$**

Pour les entreprises et organismes publics :

- **Manquement mineur à très grave :** de 1 000 $ à 10 $ M ou 2 % du CA

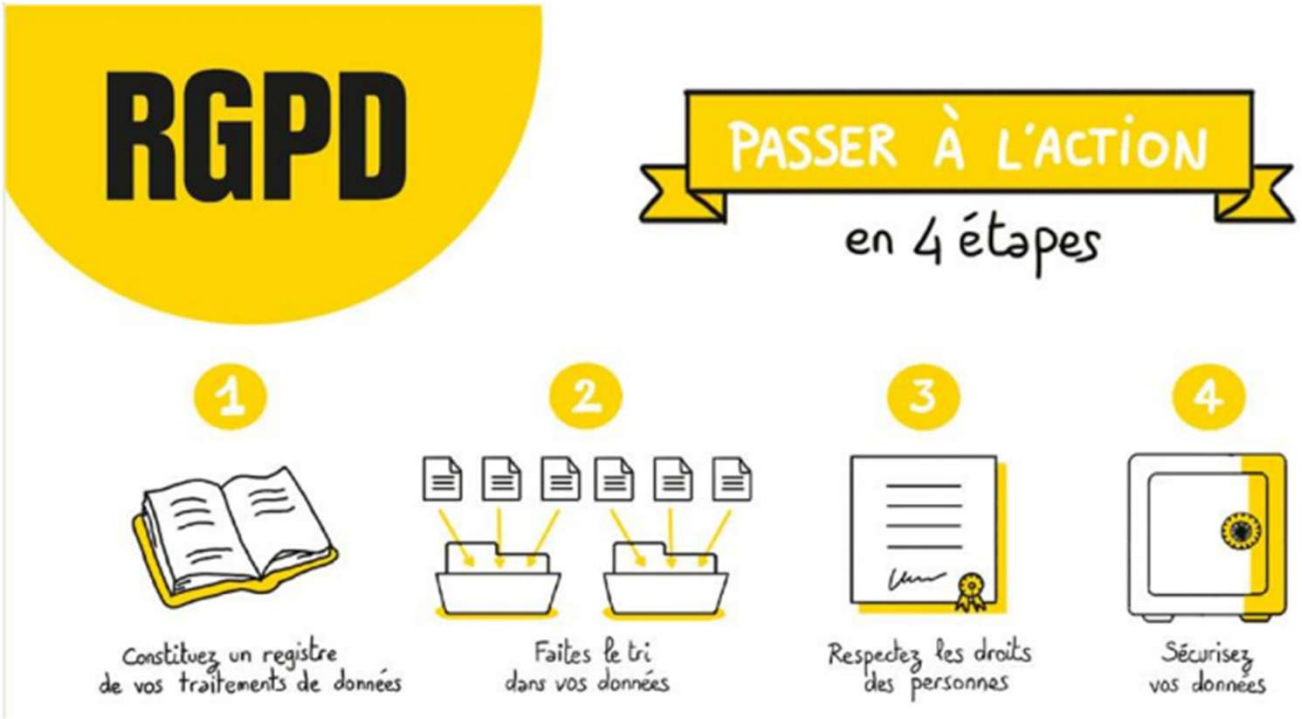
Survol de RGPD

RGPD:

- Texte reglémentaire publié par le parlement européen et le Conseil le 27 avril 2016.
- Il vise à protéger les personnes physiques résidant dans l'UE, à l'égard du traitement de leurs données à caractère personnel et garantir la libre circulation de ces données
- Tout le monde est concerné
- Il est appliqué depuis le 25-mai 2018

Quelques principes du RGPD

Le RGPD en resumé (suite)



LES ÉTAPES RECOMMANDÉES POUR SE CONFORMER

Étape	Détail
Étape 1 : Nommer un délégué à la protection des données	Disposer d'un pilote est indispensable pour gérer les données personnelles collectées par une entreprise. Celui-ci est chargé d'un rôle d'information, de conseil et de contrôle interne.
Étape 2 : Recenser les traitements des données	Un registre des traitements des données personnelles est une documentation qui permet de faire le bilan sur l'effet du règlement.
Étape 3 : Définir les actions correctives	Afin de respecter les règles en matière de droits et libertés personnels, il est nécessaire de déterminer quelles sont les actions prioritaires à mettre en œuvre. La priorisation est déterminée en fonction du niveau de risque et grâce au registre des traitements.
Étape 4 : Analyser les risques	Il convient de gérer au mieux les risques pouvant avoir des conséquences sur la sécurité des données.
Étape 5 : Établir des procédures internes	Les procédures internes permettent de constamment assurer la protection des données personnelles. Il faut ici anticiper les événements éventuels pouvant affecter les traitements en cours.
Étape 6 : Tenir une documentation	La documentation permet de justifier la conformité d'une entreprise au règlement. Il est également essentiel de fréquemment reconsidérer et ajuster les actions et documents afin de garantir une protection des données durable.

Les risques et sanctions

Risques économiques

Contrôle des garanties par un client

Risques juridiques

Plainte en ligne

Contrôle par la CNIL

Sanctions de la CNIL

LES SANCTIONS

Administratives	**Amendes**	**Pénales**
• Avertissement • Mise en demeure • Injonction • Limitation ou suspension temporaire d'un traitement	Jusqu'à 4% du CA *ou* 20 millions d'euros d'amende	Jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende

Circulaire 126 BRH

Le 13 janvier 2022, la Banque de la République d'Haïti (BRH) a publié la circulaire numéro 126, établissant des exigences en matière de sécurité informatique aux institutions financières du pays. Elle vise à garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des données et des informations gérées à travers les systèmes informatiques des institutions financières.

Contenu du circulaire 126

- **Adoption d'une politique de sécurité informatique**
- **Mise en place d'un comité de sécurité informatique**
- **Organisation de la sécurité informatique**
- **Inventaire**
- **Classification de l’information**
- **Protection des systèmes et données**
- **Etc..**

Quoi retenir?

- Plusieurs outils complémentaires disponibles sur le marché
- Chaque outil a des forces et des faiblesses
- Pas de solution unique « *one size fit all* »
- Approche privilégiée :
- « *Mix and Match* » et personnalisation
- Utiliser les modèles pour s'inspirer…

Références

- https://www.rapid7.com/blog/post/2020/04/07/8-steps-to-successfully-implement-the-cis-top-20-controls-in-your-organization/
- https://www.cisecurity.org/controls/cis-controls-list
- https://divineflavor.com/2020/06/01/c-tpat-minimum-security-requirements/
- https://mylittlebigweb.com/blogue/loi-25/
- https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd
- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- https://www.strongdm.com/blog/iso-27001-controls
- https://www.brh.ht/wp-content/uploads/Circulaire-126-pdf.pdf
- https://mti-securite.ca/les-actifs-informationnels/