UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Programme de Cybersécurité

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

CONTENTS

CONTEXTE 3

DÉFINITIONS 3

RELATION ENTRE LES CADRES DE GESTION DE LA SÉCURITÉ, LES CATALOGUES DE CONTRÔLE ET LES PROCESSUS DE SÉCURITÉ 4

ÉLABORATION D'UN PROGRAMME DE GESTION DE LA CYBERSÉCURITÉ 5

ÉTAPES DE L'ÉLABORATION DU PROGRAMME DE SÉCURITÉ 5

SÉLECTION D'UN RÉFÉRENTIEL 6

FACTEURS INFLUENÇANT LE CHOIX DU CADRE DE SÉCURITÉ ET DU CATALOGUE DE CONTRÔLE 6
CHOIX D'UN RÉFÉRENTIEL 7
COMPOSANTES DU CADRE DE GESTION DE LA CYBERSÉCURITÉ 7
CADRE DE CONTRÔLE 9

SITUATION ACTUELLE 15

BILAN DE LA SÉCURITÉ DE L'INFORMATION 15
INTERPRÉTATION DES RÉSULTATS 15

CONTRIBUTION DU CESI DANS LE RENFORCEMENT DE LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS 16

RÉFÉRENCES 17

RÉVISION 17

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

CONTEXTE

Les établissements qui se limitent qu'à la conformité lorsqu'elles cherchent à mettre en place un programme de sécurité ne sont pas aptes à répondre efficacement à l'évolution des risques liés à la cybercriminalité et à l'augmentation des cybers menaces. Cette approche les amène à produire généralement beaucoup de documentation et investir massivement dans la technique, mais elles ne consacrent que peu ou pas de temps à la mise en place d'une gouvernance efficace ou à la capacité d'évaluer et d'interpréter efficacement les risques.

Ce document vise à outiller les établissements du réseau de l'université du Québec (UQ) afin de déterminer les priorités et les efforts requis pour renforcer leur sécurité. Ce n'est pas un cadre normatif, par conséquent, il n'y a pas d'obligation à implémenter chacune des actions et l'ordre d'exécution proposée. Chaque établissement est libre de choisir les mesures à mettre en place en fonction de son profil et de son appétit pour le risque.

DÉFINITIONS

Concepts	Définition	Utilisations et applicabilité	Exemples
Cadre de sécurité	Un ensemble complet et structuré de processus pour la gestion de la sécurité et des risques.	Fournis une structure pour organiser les contrôles de sécurité afin de s'assurer qu'ils sont complets et cohérents.	ISO27001:2017, NIST CSF, COBIT, HITRUST CSF
Catalogue de contrôle	Un menu organisé de contrôles de sécurité techniques et de processus.	Favorise une approche systématique du déploiement d'un ensemble efficace de contrôles de sécurité.	CIS CSC, ASD Essential 8, U.K. Cyber Essentials, NIST SP 800-53, ISO/IEC 27002: 2013, HIPAA

Processus de sécurité	Une série d'actions interdépendantes et liées entre elles, exécutées de manière orchestrée pour réaliser une tâche ou un résultat spécifique en matière de sécurité.	Contribue à favoriser une approche normalisée et évolutive des activités de sécurité les plus courantes, qui permet d'obtenir des résultats cohérents, fiables, efficaces et mesurables en matière de sécurité.	Gouvernance de la sécurité, gestion de la politique de sécurité, sensibilisation et éducation à la sécurité, gestion des identités et des accès, gestion de la vulnérabilité, réponse aux incidents.

RELATION ENTRE LES CADRES DE GESTION DE LA SÉCURITÉ, LES CATALOGUES DE CONTRÔLE ET LES PROCESSUS DE SÉCURITÉ

CADRE DE GESTION DE LA SÉCURITÉ

Fournir une structure pour organiser les contrôles afin de s'assurer qu'ils sont complets et cohérents
(Ex.: ISO 27001, NIST CSF)

Guide

CATALOGUE DE CONTRÔLE DE SÉCURITÉ

Un menu de contrôles dans lequel vous choisissez un sous-ensemble en fonction du cadre de sécurité sélectionné
(Ex.: ISO 27002, NIST SP 800-53, CIS)

Oriente

PROCESSUS DE SÉCURITÉ

Actions opérationnelles obligatoires ou discrétionnaires exécutées pour atteindre les objectifs du contrôle de sécurité
(Ex.: Gestion de vulnérabilité, gestion des accès)

ÉLABORATION D'UN PROGRAMME DE GESTION DE LA CYBERSÉCURITÉ

Les responsables de la gestion des risques des organismes publics sont confrontés à un ensemble déroutant de cadres de sécurité de l'information, d'exigences légales et de catalogues de contrôle conçus pour guider la mise en place et l'exécution de programmes de sécurité et de gestion des risques. Le défi reste significatif pour les responsables de la sécurité qui sont appelés à :

- Concevoir un programme de sécurité adapté.
- Intégrer des contrôles de sécurité efficaces et efficients dans des processus opérationnels.

ÉTAPES DE L'ÉLABORATION DU PROGRAMME DE SÉCURITÉ

Les étapes ci-dessous décrivent la marche à suivre pour développer un programme de sécurité efficace, c'est-à-dire un programme qui est aligné sur la stratégie des établissements.

1. CHOIX D'UN RÉFÉRENTIEL	•Selectionner une ligne de base •Déterminer un modèle de mesure des capacités
2. SITUATION ACTUELLE	•Mesurer la maturité des processus •Identifier les principaux définis
3. SITUATION CIBLE	•Définir l'état futur désiré •Identifier les écarts
4. FEUILLE DE ROUTE	•Identifier des initiatives qui visent à combler les écarts •Prioriser les initiatives
5. IMPLÉMENTATION	• Intégrer les capacités, les outils et les technologies •Développer les compétences essentielles et former les personnes souhaitant acquérir les compétences manquantes

SÉLECTION D'UN RÉFÉRENTIEL

Le choix d'un cadre de gestion reste un défi pour les responsables étant la multiplicité et la diversité des référentiels qui existent sur le marché. Parallèlement, développer un programme cybersécurité en dehors des cadres généralement éprouvés pourrait entraîner un gaspillage de ressources et un épuisement des équipes.

Pour décider du cadre de sécurité, du catalogue de contrôle et des processus de sécurité appropriés, les responsables de la sécurité et de la gestion des risques doivent :

- Faire la différence entre les référentiels et le programme de sécurité;
- Identifier les cadres spécifiques au secteur d'activité en question;
- Choisir un cadre et des contrôles compatibles avec les capacités de l'équipe de sécurité et la maturité de l'établissement en matière de sécurité.

FACTEURS INFLUENÇANT LE CHOIX DU CADRE DE SÉCURITÉ ET DU CATALOGUE DE CONTRÔLE

Facteurs de contexte internes	Facteurs contextuels externes
Secteur d'activité	**Exigences réglementaires et législatives**
Maturité des processus informatiques	**Exigences gouvernementales en matière de sécurité**
Maturité des capacités de sécurité	**Exigences des fournisseurs**
	Accès au marché local des talents et des compétences en matière de sécurité
	Le paysage de la menace

CHOIX D'UN RÉFÉRENTIEL

La première étape de la sélection d'un cadre de sécurité et d'un catalogue de contrôles consiste à déterminer si un cadre de sécurité ou un catalogue de contrôles a été élaboré pour votre secteur d'activité spécifique. Les normes sectorielles telles que le populaire NIST CSF — conçu à l'origine pour les fournisseurs d'infrastructures critiques américains — et d'autres renvoient souvent à d'autres cadres mondialement acceptés tels qu'ISO27001.

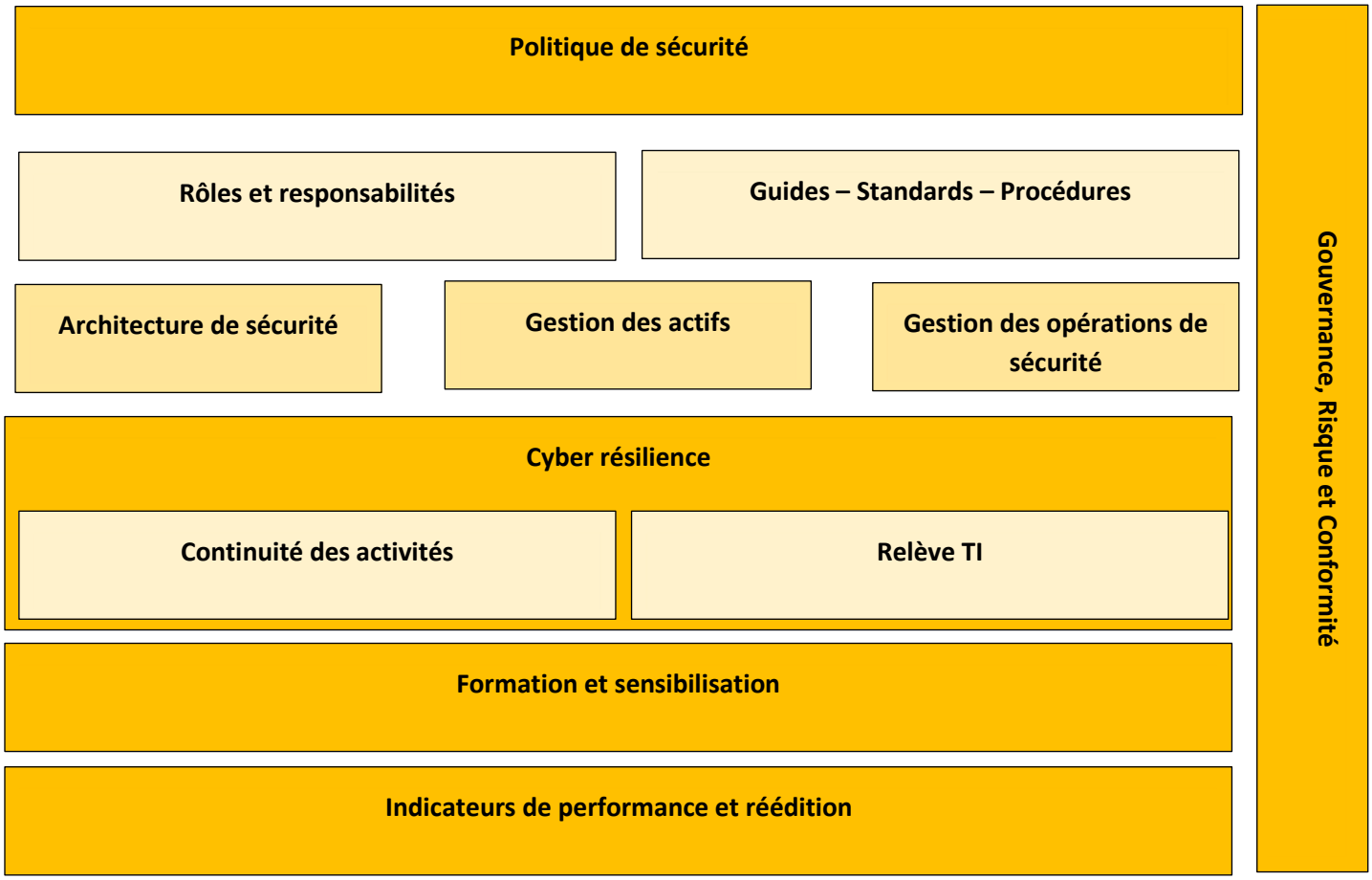
À défaut d'avoir un cadre de sécurité ou un catalogue de contrôles spécifique au secteur éducatif québécois, nous avons personnalisé un cadre en combinant :

- Les référentiels NIST CSF, ISO 27001, CIS;
- Les exigences du MCN, de la loi modernisant la protection des renseignements personnels et la loi sur la gouvernance des systèmes d'information;
- Les contrôles de sécurité qui sont audités aux cinq ans selon les exigences la loi sur la gouvernance des systèmes d'information.

Afin de s'assurer que les attentes du gouvernement sont satisfaites tout en maintenant le niveau de risque des établissements à un niveau acceptable.

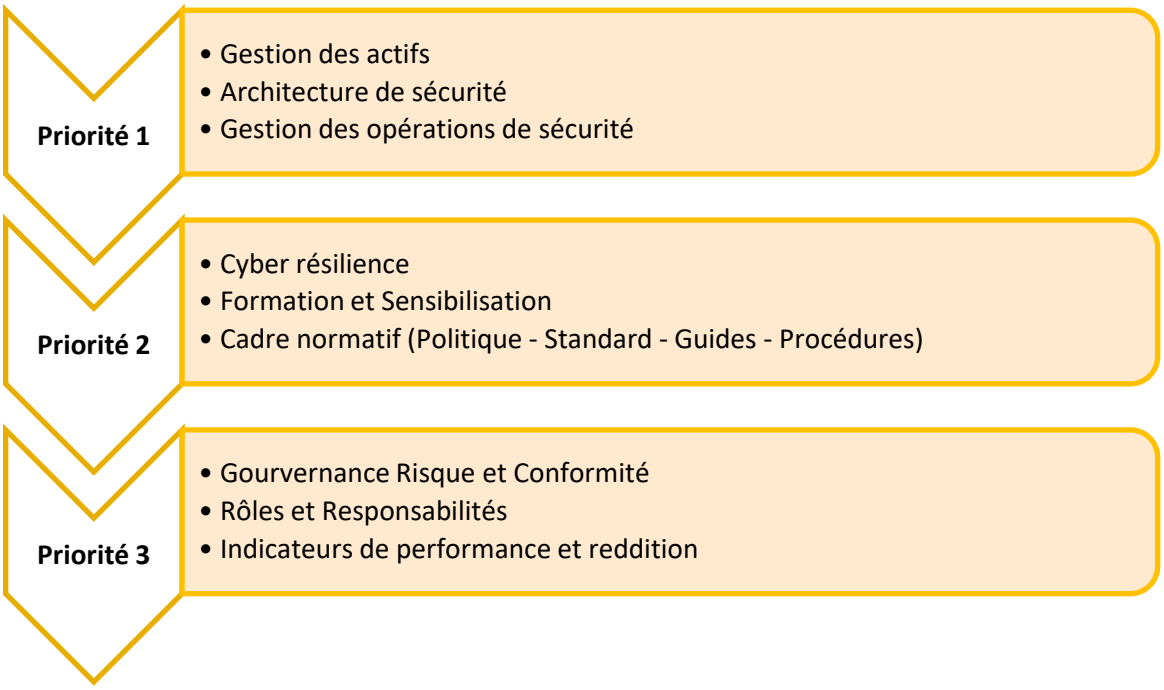
COMPOSANTES DU CADRE DE GESTION DE LA CYBERSÉCURITÉ

Les piliers du cadre sont répertoriés dans le tableau ci-dessous et couvrent l'ensemble des éléments d'un programme de sécurité qui permet de faire face aux menaces actuelles et émergentes conformément aux attentes des parties prenantes.



Il est certainement tentant de vouloir atteindre une maturité exceptionnelle pour chacun des piliers, en revanche, ça prend des ressources considérables et ce n'est pas une gestion optimale de la cybersécurité. Par conséquent, nous recommandons une approche basée sur les risques tout en prenant en compte le niveau de maturité de chaque établissement.

L'ordre proposé est le suivant :



CADRE DE CONTRÔLE

Étant donné que l'approche préconisée n'est pas d'implémenter l'ensemble des contrôles d'un cadre existant parce que cela risque de créer un environnement surcontrôlé qui ne reflète pas la réalité des établissements du réseau. Nous avons décidé de sélectionner un ensemble de mécanismes de défense généralement accepté par les experts du domaine et qui satisfait les attentes du ministère de la cybersécurité.

En nous basant sur la version 2.0 du modèle de défense communautaire (Community Defense Model – CDM) publié par CIS, nous avons une assurance raisonnable que les mécanismes sélectionnés peuvent nous protéger adéquatement contre les principaux types d'attaques. Toutefois le choix et l'ordre d'implémentation restent à la discrétion des établissements.

Ces mesures sont regroupées en 15 catégories et colligées dans le tableau ci-dessous.

Catégories	Objectifs	Mécanismes	MCN	LGGRI	Loi 25
Inventaire des informations et autres actifs associés	Identifier les informations et autres actifs associés de l'organisation afin de préserver leur sécurité et d'en attribuer la propriété de manière appropriée	■ Établir et tenir à jour un inventaire détaillé des actifs de l'établissement ■ Établir et maintenir un inventaire des logiciels ■ Établir et maintenir un inventaire des données	✓		
Terminaux finaux des utilisateurs	Protéger les informations contre les risques liés à l'utilisation de terminaux finaux des utilisateurs	■ Chiffrer les données sur les appareils des utilisateurs finaux ■ Établir et maintenir un processus de configuration sécurisé ■ Mettre en œuvre et gérer un pare-feu sur les appareils des utilisateurs finaux ■ Veiller à n'utiliser que des navigateurs et des clients de messagerie entièrement supportés ■ Déployer et maintenir un logiciel anti-maliciel ■ Renforcer la capacité d'effacement à distance sur les appareils portatifs des utilisateurs finaux	✓		
Culture et programme de sensibilisation à la sécurité de l'information	S'assurer que le personnel et les parties intéressées pertinentes connaissent et remplissent leurs responsabilités en matière de sécurité de l'information.	■ Établir et maintenir un programme de sensibilisation à la sécurité ■ Former les membres du personnel à reconnaître les attaques d'ingénierie sociale ■ Former les membres du personnel à reconnaître et à signaler les incidents de sécurité ■ Former le personnel sur la manière d'identifier et de signaler si les mises à jour de sécurité manquent sur les actifs de l'entreprise ■ Former le personnel aux dangers de la connexion et de la transmission de données	✓	✓	✓

Catégories	Objectifs	Mécanismes	MCN	LGGRI	Loi 25
		des établissements sur des réseaux non sécurisés			
Gestion des identités et des accès	Assurer l'accès autorisé et empêcher l'accès non autorisé aux informations et autres actifs associés.	■ Configurer les listes de contrôle d'accès aux données ■ Établir une procédure d'octroi et de révocation des accès ■ Exiger MFA pour les applications critiques exposées en externe ■ Exiger le MFA pour l'accès aux réseaux à distance ■ Configurer le verrouillage automatique des sessions sur les actifs de l'établissement	✓	✓	✓
Droits d'accès privilégiés	S'assurer que seuls les utilisateurs, composants logiciels et services autorisés sont dotés de droits d'accès privilégiés.	■ Établir et tenir à jour un inventaire des comptes à privilège élevé ■ Limiter les privilèges « administrateur » à des comptes « administrateur » dédiés ■ Gérer les comptes par défaut des actifs et des logiciels de l'entreprise ■ Exiger le MFA pour les accès privilégiés	✓	✓	✓
Gestion des configurations et des changements opérationnels	S'assurer que le matériel, les logiciels, les services et les réseaux fonctionnent correctement avec les paramètres de sécurité requis, et que la configuration n'est pas altérée par des changements non autorisés ou incorrects.	■ Établir et maintenir un processus de configuration sécurisé ■ Établir et maintenir un processus de configuration sécurisé pour l'infrastructure du réseau ■ Configurer le verrouillage automatique des sessions sur les biens d'entreprise ■ Utiliser des modèles de configuration standard pour les applications de l'infrastructure ■ Désinstaller ou désactiver les services inutiles sur les actifs et les logiciels de l'entreprise	✓		

Catégories	Objectifs	Mécanismes	MCN	LGGRI	Loi 25
Gestion des fournisseurs TI	Maintenir le niveau de sécurité de l'information convenu dans les relations avec les fournisseurs.	■ Établir et tenir à jour un inventaire des prestataires de services ■ Établir les exigences de sécurité de l'information appropriée avec chaque fournisseur, selon le type de relation avec le fournisseur ■ Définir et de mettre en œuvre des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC. ■ Procéder régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et de prestation de services.	✓	✓	✓
Protection contre les programmes malveillants (maliciel)	S'assurer que les informations et autres actifs associés sont protégés contre les programmes malveillants.	■ Déployer et maintenir un logiciel anti-maliciel ■ Configurer les mises à jour automatiques des signatures antivirus et anti-programmes malveillants ■ Former les membres du personnel à reconnaître les attaques d'ingénierie sociale	✓		
Gestion des vulnérabilités	Empêcher l'exploitation des vulnérabilités techniques.	■ Établir et maintenir un processus de gestion des vulnérabilités ■ Établir et maintenir un processus de correction ■ Effectuer une gestion automatique des correctifs des systèmes d'exploitation ■ Effectuer une gestion automatique des correctifs des applications ■ Établir et maintenir un programme de tests de pénétration	✓	✓	

Catégories	Objectifs	Mécanismes	MCN	LGGRI	Loi 25
Gestion des incidents de sécurité	L'établissement doit s'assurer de planifier et préparer la gestion des incidents de sécurité de l'information en procédant à la définition, à la mise en place et à la communication des processus, fonctions et responsabilités liés à la gestion des incidents de sécurité de l'information.	■ Désigner le personnel chargé de gérer les incidents ■ Établir et maintenir un processus de notification des incidents au niveau de l'établissement ■ Établir et tenir à jour les coordonnées des personnes à contacter pour signaler les incidents de sécurité ■ Définir des mécanismes de communication pendant la réponse à l'incident ■ Effectuer des exercices de routine de réponse aux incidents	✓	✓	
Sécurité des données/confidentialité	Limiter l'exposition des données sensibles, et se conformer aux exigences légales, statutaires, réglementaires et contractuelles.	■ Établir et maintenir un système de classification des données ■ Chiffrer les données sensibles en transit ■ Chiffrer les données sensibles au repos ■ Détecter et empêcher la divulgation et l'extraction non autorisées d'informations par des personnes ou des systèmes.	✓	✓	✓
	Permettre la récupération en cas de perte de données ou de systèmes.	■ Effectuer des sauvegardes automatiques ■ Établir et maintenir un processus de récupération des données ■ Protéger les données de restauration ■ Établir et maintenir une copie isolée des données de récupération	✓	✓	✓
Sécurité des réseaux	Protéger les informations dans les réseaux et les moyens de traitement de l'information support contre les compromissions via le réseau.	■ Utiliser les services de filtrage DNS ■ Collecter les journaux d'audit ■ Déployer une solution de détection des intrusions sur le réseau	✓		

Catégories	Objectifs	Mécanismes	MCN	LGGRI	Loi 25
	Diviser le réseau en périmètres de sécurité et contrôler le trafic entre eux en fonction des besoins métier.	■ Filtrage du trafic entre les segments du réseau ■ Collecter les journaux de flux de trafic du réseau ■ Déployer une solution de prévention des intrusions dans le réseau	✓		
Système de protection des applications	L'établissement doit s'assurer que les exigences de sécurité de l'information soient identifiées, spécifiées et approuvées lors du développement ou de l'acquisition d'applications.	■ Établir et maintenir un processus de développement d'applications sécurisées ■ Établir et maintenir un processus d'acceptation et de traitement des vulnérabilités des logiciels ■ Utiliser des modèles de durcissement de la configuration pour les applications ■ Former les développeurs aux concepts de sécurité des applications et au codage sécurisé	✓		
	L'établissement doit s'assurer que les exigences de sécurité de l'information soient identifiées, spécifiées et approuvées lors du développement ou de l'acquisition d'applications.	■ Veiller à ce que les contrats des fournisseurs de services incluent des exigences en matière de sécurité ■ Évaluer les fournisseurs de services ■ Surveiller les prestataires de services	✓		
Gestion des journaux et événements	Enregistrer les événements, générer des preuves, assurer l'intégrité des informations de journalisation, empêcher les accès non autorisés, identifier les événements de sécurité de l'information qui peuvent engendrer un incident de sécurité de l'information et assister les investigations.	■ Établir et maintenir un processus de gestion des journaux d'audit ■ Collecter les journaux d'audit ■ Assurer un stockage adéquat des journaux d'audit	✓	✓	

Catégories	Objectifs	Mécanismes	MCN	LGGRI	Loi 25
Continuité des activités informatiques et reprise après sinistre	S'assurer du fonctionnement continu des moyens de traitement de l'information.	■ Identifier les exigences relatives à la disponibilité des services et des systèmes d'information ■ Concevoir et mettre en œuvre une architecture de systèmes avec une redondance appropriée pour satisfaire à ces exigences. ■ Mettre en place les mécanismes de notifications de toute défaillance des moyens de traitement de l'information ■ Tester pour s'assurer que le basculement d'un composant à un autre composant fonctionne comme prévu	✓	✓	

SITUATION ACTUELLE

BILAN DE LA SÉCURITÉ DE L'INFORMATION

Conformément à la Loi sur la gouvernance et la gestion des ressources informationnelles (LGGRI ou Loi 133) exigeant l'audit de sécurité de l'information selon une périodicité quinquennale ou à la suite d'un changement majeur, le regroupement des universités du réseau de l'UQ a procédé à un bilan de la maturité des processus et des contrôles en lien avec la sécurité de l'information

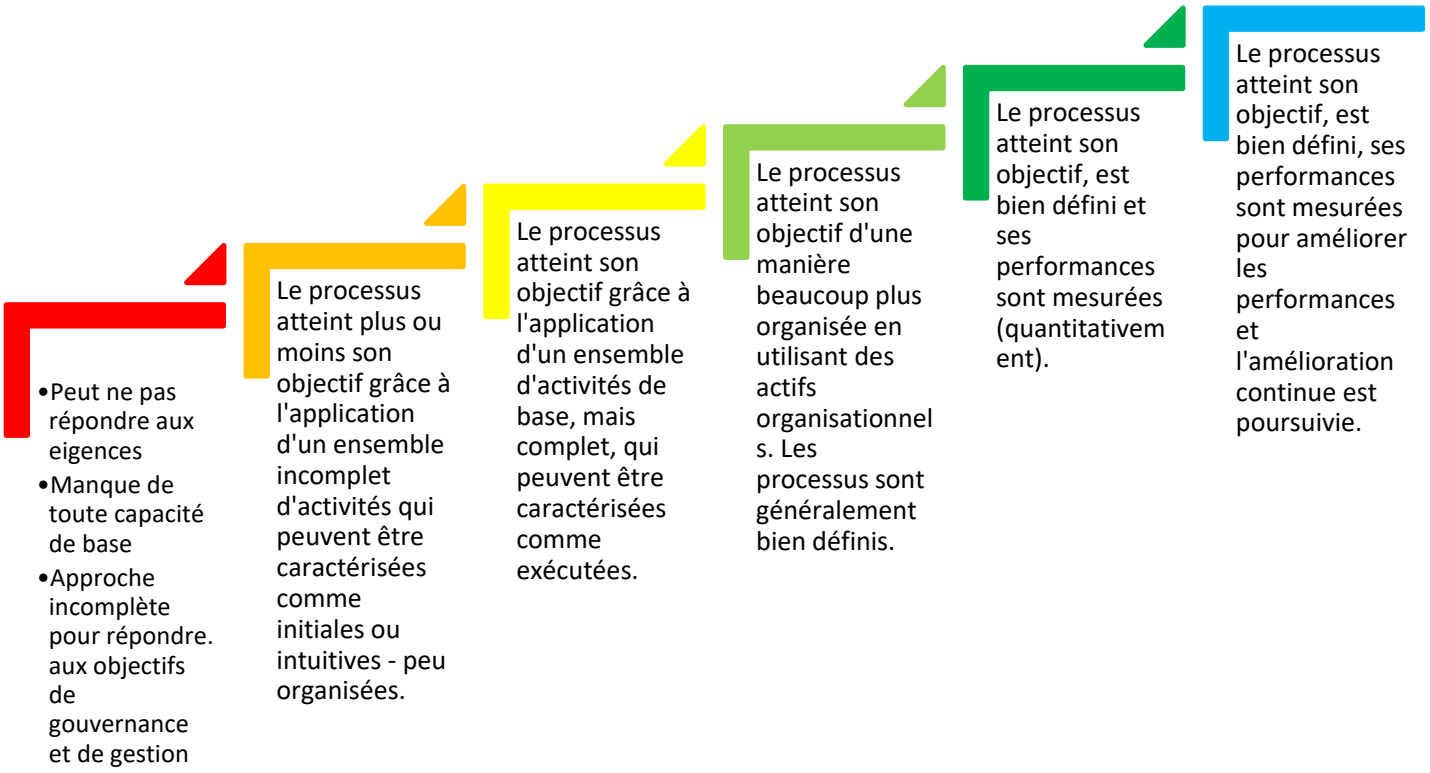
Le rapport d'audit de la maturité des processus de sécurité est un bon point de départ pour évaluer l'état actuel des contrôles de sécurité.

Des codes de couleur sont assignées à chacun des processus de sécurité comme suit :

0— Non existant	1— État initial	2— Reproduisible	3— Défini	4— Géré	5— Optimisé

INTERPRÉTATION DES RÉSULTATS

L'évaluation suit le « Modèle d'intégration de maturité des capacités » (CMMI) adopté par COBIT. Le terme « maturité » fait référence au degré de formalité et d'optimisation des processus, des pratiques ad hoc, aux étapes formellement définies, aux indicateurs de résultats gérés et à l'optimisation active des processus.



CONTRIBUTION DU CESI DANS LE RENFORCEMENT DE LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS

Conformément à son mandat de soutenir et accompagner les 10 établissements du réseau de l'UQ à renforcer leur posture de cybersécurité, Le CESI a mis un ensemble de guides à disposition des acteurs impliqués dans le renforcement des contrôles de sécurité.

Étant un partenaire stratégique fiable, le CESI fait évoluer constamment son offre de service pour aider à faire face aux enjeux cyber auxquels les établissements sont confrontés, c'est ainsi qu'il a lancé un service d'évaluation de risques des fournisseurs et un programme de cyber résilience.

Les efforts continus pour renforcer les relations avec les partenaires parce que les défis sont tels que nous devons mutualiser nos capacités pour les aborder.

RÉFÉRENCES

Norme ISO 27001

COBIT 2019

NIST CSF

https://www.nist.gov/cyberframework

https://www.cisecurity.org/controls

https://www.gartner.com/en/information-technology/trends/the-it-roadmap-for-cybersecurity

Implementation Guide for Small- and Medium-Sized Enterprises

https://www.cisecurity.org/insights/white-papers/implementation-guide-for-small-and-medium-sized-enterprises-cis-controls-ig1)

CIS Community Defense Model

https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

RÉVISION

Date	Action	Auteur	Ver.
2023-11-23	Version initiale	Anglade Perrier CESI de l'UQ	0.9