UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide d'évaluation des menaces et des risques - CESI

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIÈRES

INTRODUCTION

CONTEXTE

Chaque université a la responsabilité de protéger adéquatement tous les actifs de son organisation, qu'elle soit numérique ou non. Pour ce faire, il est important de connaitre toutes les menaces et vulnérabilités auxquelles sont exposés tous ces actifs.

De nos jours, tous les actifs informationnels sont exposés à des menaces de tous genres qui peuvent avoir des effets néfastes sur les actifs des universités, des étudiants, et porter atteinte aux intérêts de sécurité nationale du Québec et du Canada. C'est pour cela que le Centre d'expertise en sécurité de l'information (CESI) recommande que les universités effectuent une analyse des menaces et des risques et de prendre les mesures nécessaires afin de les remédier.

Les évaluations des menaces et des risques sont utilisées pour identifier, estimer et hiérarchiser les risques résultant de l'exploitation et de l'utilisation des systèmes d'information.

Plusieurs méthodes existent pour effectuer l'analyse des menaces et des risques. Ainsi, pour des actifs communs aux universités, l'analyse des menaces pourrait être différente d'une université à une autre. Cela pourrait avoir une incidence sur les mesures de contrôle à mettre en place. Le résultat est que l'actif ne sera pas protégé adéquatement d'une université à une autre. Cette situation a conduit le CESI à identifier une approche lui permettant d'obtenir des résultats consensuels et harmonisés.

Afin d'uniformiser la méthode utilisée par les universités, le CESI a choisi d'élaborer un guide des menaces et des risques en se basant sur la méthodologie harmonisée d'évaluation des menaces et des risques qui a été publiée en 2007 par la Gendarmerie royale du Canada (GRC/RCMP) et le Centre de la Sécurité des Télécommunications (CST/CSE).

OBJECTIF DU DOCUMENT

Le présent document vise à expliquer la nécessité d'effectuer l'analyse des menaces et des risques des actifs des universités du Québec et décrit de manière explicite la méthode utilisée, ainsi que les étapes nécessaires à la réalisation de l'analyse. Il permettra aussi d'informer les décideurs et de soutenir les réponses aux risques en identifiant les menaces pertinentes ainsi que les vulnérabilités internes et externes pour les universités.

PORTÉE

Ce document s'adresse à tous les établissements d'enseignement supérieur, aux détenteurs de l'information, aux professionnels de la sécurité de l'information et à toutes les ressources qui seront sollicitées dans la démarche d'analyse des menaces et des risques des actifs organisationnels.

ÉVALUATION DES MENACES ET DES RISQUES (EMR)

QU'EST-CE QUE L'ÉVALUATION DES MENACES ET DES RISQUES

L'évaluation des menaces et des risques (EMR) est un outil critique, pratique, permettant de mieux comprendre les différentes menaces auxquelles doivent faire face les systèmes informatiques des universités du Québec. L'EMR permet aussi d'énumérer les risques et leurs niveaux auxquels sont exposés les systèmes informatiques. Une fois les risques connus, l'EMR permet de recommander des mesures de contrôle pour abaisser ceux-ci à des niveaux acceptables par les universités du Québec.

L'EMR offre une analyse et une interprétation des risques présents au sein des universités du Québec.

RÔLES ET RESPONSABILITÉS

Rôle	Responsabilité
DIRECTION GÉNÉRALE OU RECTORAT	▪ S'assurer de la mise en place de mesures de réduction des risques de sécurité de l'information ▪ Valider les plans de traitement des risques.
CHEF DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNELLE **(CSIO)**	▪ Présenter les plans de traitement des risques à la direction générale ou rectorat ▪ Inviter les entités administratives visées à désigner leurs représentants aux différents ateliers de gestion des risques ▪ Ajuster les priorités de traitement des risques.
COORDONNATEUR ORGANISATIONNEL DES MESURES DE SÉCURITÉ DE L'INFORMATION **(COMSI)**	▪ Effectuer et participer aux analyses de risques en sécurité de l'information ▪ Maintenir le registre des événements et des incidents liés à la sécurité de l'information

RÉVISION DE L'ÉVALUATION DES MENACES ET DES RISQUES

Dans la mesure où le paysage des menaces change continuellement, et par conséquent les vulnérabilités qui sont propres aux universités du Québec, il est donc nécessaire d'effectuer des EMR périodiques sur les environnements existants.

Le CESI encourage fortement que la révision de l'EMR des systèmes informatiques se fasse sur une base annuelle ou à chaque changement significatif au niveau de l'actif et encourage tous les établissements de l'Université de Québec à mettre en place un processus, afin de s'assurer que la révision se fasse conformément à la recommandation de celui-ci. Cependant, en fonction des ressources disponibles, chaque université pourra décider de la fréquence la plus appropriée pour effectuer l'EMR des systèmes informatiques.

À QUELLE CONDITION DEVRAIT-ON FAIRE UNE ÉVALUATION DES MENACES ET DES RISQUES

Les établissements de l'Université du Québec doivent réaliser une EMR pour s'assurer que les actifs sont adéquatement protégés en tout temps. L'EMR devra être effectué lorsqu'on veut :

- Ajouter de nouvelles applications ou de nouveaux systèmes à votre environnement;
- Faire des modifications à votre environnement TI existant;
- Partager des informations avec de nouvelles entités externes.

LA MÉTHODE D'ANALYSE DES MENACES ET DES RISQUES

PHASE 1 : PRÉPARATION

ENGAGEMENT DE LA DIRECTION

Avant de commencer l'EMR, il est important de rencontrer la direction afin de s'assurer qu'elle comprenne bien son rôle et ses responsabilités dans la définition et l'approbation de niveaux acceptables de risques résiduels avant de déployer les actifs en production. Le CESI recommande que :

- Les niveaux de risques très faible et faible soient acceptés par les universités;
- Les niveaux de risque modéré, élevé et très élevé ne soient acceptés par les universités.

Sans l'engagement de la haute direction, il pourrait être difficile d'obtenir les ressources nécessaires afin de réaliser une EMR avec la collaboration de toutes les parties associées à l'évaluation.

Le CESI recommande que le niveau de risque acceptable devra être connu avant de commencer l'évaluation des menaces et des risques.

PORTÉE

Lors de l'EMR, il sera important de définir clairement la portée et fixer les limites raisonnables de l'évaluation. Cela aura pour effet d'éviter une perte de temps, un gaspillage d'efforts et des retards inutiles. Si on ne fixe pas des limites réalistes dès le départ, les étapes, telles que la collecte et l'analyse des données, risquent de ne plus en finir et par conséquent, le projet, de s'enliser sous le poids de l'effort.

La portée pourra être révisée à tout moment si l'on constate l'introduction de nouveaux sous-systèmes, la découverte des menaces ou des vulnérabilités inconnues jusque-là.

COMPOSITION DE L'ÉQUIPE

- Le conseiller en sécurité est responsable de l'EMR;
- Le détenteur de l'actif est responsable de connaitre les menaces, d'accepter les risques identifiés lors de l'EMR et de prendre les mesures nécessaires afin d'y remédier;
- Le pilote est la personne qui connait très bien l'actif. Il est responsable de fournir toutes les informations sur l'actif;
- Le gestionnaire de projet.

PLAN DE TRAVAIL

Avant de démarrer l'EMR, il sera important d'élaborer un plan de travail. Celui-ci comprendra le calendrier du projet dressant la liste des activités avec les dates de début et d'achèvement de chaque phase de l'évaluation.

APPROBATION

Le plan devra être approuvé par le responsable de l'acceptation des risques qui, en dernier ressort, examinera les recommandations et acceptera ou rejettera les risques résiduels prévus et recensés dans le rapport de l'EMR.

EXEMPLE D'UN PLAN D'UNE ÉVALUATION DES MENACES ET DES RISQUES

	Activités	Ressources affectées	Date de début	Date de fin
1	Identifier la liste des actifs applicables que l'organisation veut protéger	Le conseiller en sécurité, le détenteur de l'actif, le pilote, le gestionnaire de projet et le responsable de l'impact sur la vie privée		
2	Attribuer une valeur aux actifs en fonction de la disponibilité, de l'intégrité, de la confidentialité et de l'impact de la compromission	Le conseiller en sécurité, le détenteur de l'actif, le pilote, le gestionnaire de projet et le responsable de l'impact sur la vie privée		

	Activités	Ressources affectées	Date de début	Date de fin
3	Identifier la liste des menaces malveillantes et accidentelles qui pourraient affecter les actifs	Le conseiller en sécurité, le détenteur de l'actif, le pilote et le gestionnaire de projet		
4	Attribuer une valeur à la menace en fonction de sa probabilité et de son impact	Le conseiller en sécurité		
5	Identifier les contrôles de sécurité ITSG-33 nécessaires et évaluer si les contrôles sont mis en œuvre ou non	Le conseiller en sécurité		
6	Identifier la liste de toutes les mesures de protection existantes	Le conseiller en sécurité, le détenteur de l'actif, le pilote et le gestionnaire de projet		
7	Attribuer une valeur à la vulnérabilité en fonction de l'impact sur la probabilité de compromission et de la gravité du résultat	Le conseiller en sécurité		
8	Évaluation des risques	Le conseiller en sécurité		
9	Identifier les recommandations à mettre en place afin d'atteindre le risque résiduel souhaité	Le conseiller en sécurité		
10	Préparer le rapport de l'évaluation des menaces et des risques	Le conseiller en sécurité		

Figure 1 : Exemple d'un plan d'une Évaluation des menaces et des risques

PHASE 2 : ÉVALUATION DES ACTIFS

IDENTIFICATION DES ACTIFS

Cette étape consiste à dresser la liste de tous les actifs qui sont inclus dans la portée de l'évaluation à un niveau approprié de détail.

Quel que soit le niveau de granularité souhaité lors de l'inventaire, chacun des actifs doit être caractérisé par les éléments suivants :

- Nom de l'objet de catégorisation;
- Nom du processus opérationnel;
- La ou les composante(s) du processus opérationnel (services);
- Description de la ou les composante(s) du processus opérationnel (services);
- Type objet.

ÉVALUATION DES PRÉJUDICES

Cette étape consiste à déterminer le préjudice qui pourrait vraisemblablement résulter d'une atteinte à la confidentialité, à la disponibilité ou à l'intégrité de chaque actif.

FORMATION DU COMITÉ POUR L'ÉVALUATION DES PRÉJUDICES

Le processus d'évaluation du préjudice devrait être confié à des équipes composées de représentants des secteurs responsables des opérations, des questions juridiques, de l'accès à l'information et de la sécurité et du respect de la vie privée. Le détenteur ou son délégué devra également faire partie de ces équipes, de même que le responsable de l'autorisation (si cette tâche n'a pas été confiée au propriétaire opérationnel) et les représentants et analystes opérationnels de chaque programme ou secteur d'activité. Dans la présente, on désigne ce groupe par le nom collectif « Comité d'évaluation ».Voici quelques compétences nécessaires à la réalisation de l'analyse des préjudices :

- Pilote du système évalué;
- Conseiller en sécurité;
- Utilisateur du système;
- Architecte d'affaires;
- Détenteur ou son représentant.

ÉVALUATION DES PRÉJUDICES

L'objectif de l'évaluation du préjudice est de déterminer le préjudice prévu lié aux menaces de compromission pour chaque processus opérationnel et chaque bien d'information déterminé à l'étape précédente. Idéalement, les universités doivent évaluer les préjudices associés à leurs processus opérationnels et aux biens d'information connexes en recourant à un processus auquel participent des équipes multidisciplinaires qui regroupent des représentants des domaines opérationnels, juridiques, de l'accès à l'information et du respect de la vie privée.

La réussite de l'évaluation des préjudices prend en compte la démarche suivante :

1. **Le scénario de compromission ou de défaillance** : C'est la description des événements pouvant engendrer des préjudices si les critères de sécurité du système étaient compromis;
2. **Type et niveau de préjudice** : Choisir le préjudice (cellule) applicable dans le tableau de préjudices;
3. **Facteurs spéciaux** : La prise en compte de certains éléments pourrait influencer sur les préjudices;
4. **Analyse** : Justification du choix, argumentaire et observation.

Il est à noter que les quatre étapes de l'évaluation de préjudice ci-dessus sont effectuées par rapport à chaque objectif de sécurité de l'information (disponibilité, intégrité et confidentialité).

Le tableau ci-dessous doit être utilisé pour identifier les préjudices applicables lors de la compromission des critères de sécurité.

Type de préjudices	Niveau				
	Très faible	Faible	Modéré	Élevé	Très élevé
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleur physique, blessure, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse, traumatisme psychologique	Maladie ou trouble mental	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort et stress causé	Qualité de vie affectée	Sécurité financière compromise	Sans objet
Perte financière pour des entreprises	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	Sans objet
Perte financière pour le gouvernement du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement du service	Incidence sur les résultats du service	Viabilité du service compromise	Viabilité des services essentiels compromise
Préjudice causé à l'économie québécoise	Sans objet	Sans objet	Incidence sur le rendement	Perte de la compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, obstruction publique	Émeute	Acte de sabotage à l'égard des biens essentiels (ex. : infrastructure essentielle)	Émeute générale ou acte de sabotage nécessitant l'imposition d'une loi martiale
Préjudice causé à la réputation du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	Perte de la confiance du public	Embarras (au Québec ou à l'étranger)	Dommage aux relations avec les autres provinces	Relations diplomatiques et internationales compromises
Perte de l'autonomie du Québec	Sans objet	Sans objet	Entrave à l'établissement de politiques gouvernementales importante	Entrave à l'application efficace de la loi, cessation des activités du gouvernement	Sans objet

Figure 2 : Tableau de la liste des préjudices

Référence : Programme de Consolidation des CTI - Guide d'analyse des préjudices de sécurité

CATÉGORISATION DES ACTIFS BASÉE SUR L'ANALYSE DES PRÉJUDICES

Cette étape consiste à attribuer une valeur à chaque actif sur les plans de la confidentialité, de la disponibilité et de l'intégrité, selon le cas, en se fondant sur des critères de préjudice courants.

Une fois l'évaluation des préjudices terminée, il est recommandé que le comité d'évaluation produise un rapport final de la catégorisation des actifs basé sur l'approche par l'analyse des préjudices pour communiquer les résultats.

Ce comité d'évaluation devra documenter et accepter formellement les résultats de l'activité de catégorisation de la sécurité.

VALEUR ASSOCIÉE DES NIVEAUX POSSIBLES DES ACTIFS

Niveau possible de la valeur de l'actif	Très Faible	Faible	Modéré	Élevé	Très Élevé
Valeur associée au niveau de l'actif	1	2	3	4	5

Figure 3 : Tableau des valeurs associées aux niveaux possibles des actifs

PHASE 3 : ÉVALUATION DES MENACES

IDENTIFICATION DES MENACES

Une menace est un événement indésirable ayant le potentiel de compromettre la disponibilité, l'intégrité ou la confidentialité des données de l'université. Une menace peut aussi être définie comme tout acte délibéré ou accidentel qui pourrait porter préjudice aux employés ou aux biens.

L'étape d'identification des menaces consiste à produire une liste de toutes les menaces susceptibles d'avoir une incidence sur les actifs prévus dans la portée de l'évaluation.

Les menaces peuvent être catégorisées en 3 grands types de menaces :

- Menaces délibérées : ce sont des menaces planifiées ou préméditées par des individus.
- Menaces accidentelles : ce sont des menaces qui sont dues à des erreurs humaines.
- Menaces naturelles : ce sont des menaces qui résultent d'événements naturels tels que les tremblements de terre, éruptions volcaniques, cyclone, tsunami, etc.

LISTE DES MENACES

Le CESI recommande que chaque université crée sa propre liste de menaces possibles basée sur l'historique des données des menaces. Celle-ci devra être maintenue à jour au fur et à mesure que l'on identifie de nouvelles menaces.

Exemple - Agent de la menace : Employés, contractants, visiteurs

Les menaces internes constituent une menace particulièrement complexe pour la cybersécurité d'une organisation en raison de la quantité d'accès dont elle dispose en travaillant de l'intérieur et de leur niveau de motivation inconnu.

Certaines d'entre elles ne sont pas intentionnellement malveillantes, mais peuvent causer des dommages importants. De simples erreurs d'utilisation peuvent aboutir à une catastrophe en raison de permissions élevées, où des données peuvent être compromises en raison d'un manque de sensibilisation à la sécurité.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Délibérée	Fraude Corruption			
Délibérée	Vandalisme Dégâts matériels Accès physique non autorisé			
Délibérée	Supprimer Détruire Corrompre Crypter des enregistrements			
Délibérée	Violation délibérée de la politique et des procédures par un employé administrateur ou non			

Figure 4 : Tableau de l'agent de la menace - Employés, contractants, visiteurs

Exemple - Agent de la menace : Terrorisme

Terrorisme international : Actes criminels violents commis par des individus et/ou des groupes inspirés par des organisations ou des nations terroristes étrangères désignées (parrainées par l'État) ou qui y sont associés.

Terrorisme national : Actes criminels violents commis par des individus et/ou des groupes dans le but de poursuivre des objectifs idéologiques découlant d'influences nationales, tels que celles de nature : politique, religieuse, sociale, raciale ou environnementale.

Les conséquences du terrorisme national et international peuvent inclure des blessures aux personnes, la destruction de biens de valeur et l'interruption de services importants, avec une disponibilité potentiellement grave.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Délibérée	Assassinat Enlèvement			
Délibérée	Attentat à la bombe Lettre piégée			

Figure 5 : Tableau de l'agent de la menace – Terrorisme

Exemple - Agent de menace : Dangers naturels

Un risque naturel est un événement d'origine naturelle qui peut constituer une menace pour les êtres humains, leurs biens ou leurs environnements. Cet effet négatif est ce que nous appelons une catastrophe naturelle. En d'autres termes, lorsque la menace dangereuse se produit réellement, nous appelons celle-ci une catastrophe naturelle.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Dangers naturels	Tremblements de terre			
Dangers naturels	Inondations/Tornades/Tempêtes			
Risque Dangers	Pandémie			

Figure 6 : Tableau de l'agent de la menace - Dangers naturels

Exemple - Agent de la menace : Acteurs/concurrents parrainés par des gouvernements/États

Ces acteurs de la menace sont financés, dirigés ou parrainés par des nations. Ils piratent les systèmes informatiques afin de voler et d'exfiltrer la propriété intellectuelle, les informations sensibles et même les fonds pour faire avancer les causes d'espionnage de leur nation. Les acteurs sophistiqués sont très motivés pour infiltrer les entreprises et les organisations gouvernementales d'autres pays.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Délibérée	Effacer/détruire/altérer/séparer/perturber des enregistrements d'informations			
Délibérée	Attaques spécifiquement conçues/ciblées			
Délibérée	Vol d'informations/d'identité			

Figure 7 : Tableau de l'agent de la menace - Acteurs/concurrents parrainés par des gouvernements/États

Exemple – Agent de la menace : Crime organisé/cybercriminels

Les criminels peuvent voler des données sensibles, de l'argent et des informations personnelles pour commettre un vol d'identité. Cependant, comme ils recherchent un gain financier, les données qu'ils prennent ont tendance à se retrouver sur le marché noir ou à être vendues aux plus offrants.

Ces acteurs de la menace sont également connus pour utiliser des « ransomwares » afin d'extorquer directement les propriétaires d'entreprises. Leur motivation est le gain financier et ils sont implacables dans leur quête. Ils aiment cibler les organisations et les entreprises riches en données et cherchent surtout à compromettre les personnes non informées au sein des organisations ciblées afin de s'y implanter.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Délibérée	Exploitation du réseau			
Délibérée	Attaques spécifiquement conçues/ciblées			
Délibérée	Vol d'informations et d'identité			
Délibérée	Accès non autorisé à des données, destruction, modification			

Figure 8 : Tableau de l'agent de la menace - Crime organisé/cybercriminels

Exemple - Agent de la menace : les pirates informatiques

Les pirates informatiques sont des utilisateurs non autorisés qui s'introduisent dans des systèmes informatiques afin de voler, de modifier ou de détruire des informations, souvent en y installant des logiciels malveillants dangereux, et ce, à votre insu et sans votre consentement. La plupart du temps, les pirates peuvent détourner vos noms d'utilisateur et vos mots de passe, voler vos données et votre argent, et vendre vos informations sur le marché noir.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Délibérée	Vol d'informations/d'identité			
Délibérée	Extorsion/intimidation des employés			
Délibérée	Attaque DoS/ dégradation de site web			
Délibérée	Infection par code malveillant/virus			
Délibérée	Corruption de fichiers			

Figure 9 : Tableau de l'agent de la menace - les pirates informatiques

Exemple - Agent de la menace : Erreurs logicielles/défaillances matérielles/erreurs humaines

Problèmes matériels tels que des erreurs de configuration, des dysfonctionnements ou des dégâts des eaux qui entraîneraient l'indisponibilité des serveurs de production.

Erreurs de logiciels telles que les bogues, les erreurs de codage, les erreurs de configuration, les versions non stables, le tout pourrait produire un résultat incorrect ou inattendu.

Une erreur de logiciel peut se traduire par un message d'erreur du serveur et peut être utilisée par un attaquant pour obtenir des informations sur l'application.

Classe de menaces	Événements menaçants	Probabilité de la menace	Gravité de la menace	Niveau de la menace
Délibérée	Bogues logiciels/failles de conception/erreurs de codage			
Délibérée	Erreurs de configuration du logiciel/erreurs de maintenance			
Délibérée	Dysfonctionnement du logiciel/matériel			
Délibérée	Suppression/modification/perte de données/oubli de mot de passe			
Délibérée	Violation de politique/procédure due à l'ignorance			

Figure 10 : Tableau de l'agent de la menace - Erreurs logicielles/défaillances matérielles/erreurs humaines

ÉVALUATION DES PROBABILITÉS DES MENACES

Colonne 1	Colonne 2	Colonne 3	Colonne 4
Fréquence passée	**Même endroit, Biens semblables**	**Endroit distant, mais bien semblable Même endroit, mais bien différent**	**Endroit distant Autres biens**
Quotidienne	Élevée	Élevée	Élevée
1 à 10 jours	Élevée	Élevée	Moyenne
10 à 100 jours	Élevée	Moyenne	Faible
100 à 1000 jours	Moyenne	Faible	Très faible
1000 à 10000 jours	Faible	Très faible	Très faible
Plus de 10000 jours	Très faible	Très faible	Très faible

Figure 11 : Tableau des probabilités des menaces

Pour des menaces qui se sont manifestées au même endroit ou sur des biens semblables, il faudra déterminer la fréquence des événements passés en sélectionnant la gamme appropriée dans la [colonne 1], puis choisir le niveau de probabilité correspondant dans la [colonne 2] ;

Pour des menaces qui se sont manifestées à des endroits différents ou sur des biens différents, il faudra déterminer la fréquence des événements passés en sélectionnant la gamme appropriée dans la [colonne 1], puis choisir le niveau de probabilité correspondant dans la [colonne 3] ;

Pour des menaces qui se sont manifestées à des endroits différents et sur des biens différents, il faudra déterminer la fréquence des événements passés en sélectionnant la gamme appropriée dans la [colonne 1], puis choisir le niveau de probabilité correspondant dans la [colonne 4] .

ÉVALUATION DE LA GRAVITÉ DE LA MENACE

La conséquence ou la gravité d'un incident est la mesure de l'importance éventuelle des dommages ou de la compromission si l'incident se matérialise. Pour évaluer la gravité de la menace, on tient compte de la capacité des agents de menace et de l'ampleur des accidents et des risques naturels en terme.

Capacité de l'agent de menace délibérée	**Magnitude des accidents ou risques naturels**	**Incidence ou gravité de la menace**
Connaissances/compétences étendues et ressources considérables	• Hautement destructifs • Erreur extrêmement grave • Utilisation abusive généralisée	**Élevée**
Connaissances/compétences étendues et ressources considérables Connaissances/compétences étendues et ressources limitées Connaissances/compétences modérées et ressources moyennes	• Modérément destructifs • Erreur grave • Utilisation abusive importante	**Moyenne**
Connaissances/compétences limitées et ressources limitées	• Peu destructifs • Erreur mineure • Utilisation abusive limitée	**Faible**

Figure 12 : Tableau de la gravité des menaces

ÉVALUATION DES NIVEAUX DES MENACES

Le niveau de la menace se calcule en fonction de la probabilité de la menace et de l'incidence de celle-ci, tel que décrit dans la figure ci-dessous :

Incidence de la menace	**Probabilité de la menace**			
	Très faible	**Faible**	**Moyenne**	**Élevée**
Élevée	Faible	Moyenne	Élevée	Très Élevée
Moyenne	Très faible	Faible	Moyenne	Élevée
Faible	Très faible	Très faible	Faible	Moyenne

Figure 13 : Tableau du niveau des menaces

VALEUR ASSOCIÉE DES NIVEAUX POSSIBLES DES MENACES

Niveau possible de la menace	Très Faible	Faible	Modéré	Élevé	Très Élevé
Valeur associée au niveau de la menace	1	2	3	4	5

Figure 14 : Tableau des valeurs associées aux niveaux possibles des menaces

PHASE 4 : ÉVALUATION DES VULNÉRABILITÉS

IDENTIFIER LES MESURES DE PROTECTION EXISTANTES

Avant d'identifier et d'évaluer les vulnérabilités affectant les actifs des universités du Québec, il sera important de dresser la liste de mesures de protection existantes.

Les mesures de protection existantes ont pour but d'atténuer la probabilité que la menace se concrétise afin de réduire la probabilité de compromission au cas où un incident se produirait.

Il est aussi primordial d'évaluer le niveau d'efficacité pour chaque mesure de protection existante. Plus les mesures de protection en place sont efficaces, plus le niveau de vulnérabilité et le niveau de risque diminueront.

SÉLECTIONNER ET TESTER LES MESURES DE CONTRÔLES DE SÉCURITÉ

Une vulnérabilité est une faiblesse dans un système informatique qui peut être exploitée par un attaquant pour réussir une attaque. Elle peut provenir de failles, de fonctionnalités ou d'une erreur de l'utilisateur que les attaquants chercheront à exploiter pour atteindre leur objectif final.

La vulnérabilité fait aussi référence à une faiblesse dans votre système matériel, vos logiciels ou vos procédures. En d'autres termes, il s'agit d'un moyen pour les pirates de s'introduire facilement dans votre système.

Source : https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Le gouvernement du Canada a développé un guide qui contient la liste et la définition des contrôles de sécurité sur laquelle les spécialistes de la sécurité peuvent se fonder pour sélectionner les contrôles qui serviront à protéger les actifs du gouvernement du Canada et à gérer les risques liés à la sécurité des TI.

https://cyber.gc.ca/sites/default/files/cyber/publications/itsg33-ann3a-fra.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

L'un des contrôles généralement utilisés pour trouver des vulnérabilités dans un système est les numérisations de vulnérabilité et ce sont des outils comme Tenable.sc, on peut rouler des numérisations et détecter des failles de sécurité dans nos systèmes. Le CESI recommande que pour chaque évaluation des menaces et des risques, le spécialiste en sécurité informatique sélectionne les contrôles appropriés et les adapte en fonction de son organisation. La liste des contrôles sélectionnée devra être envoyée au pilote et détenteur de l'actif afin de produire les évidences nécessaires pour confirmer l'implémentation des contrôles.

Les critères du Center of Internet Security (CIS) sont un ensemble de meilleures pratiques mondialement reconnues et consensuelles pour configurer un système de manière sécurisée.

Les contrôles du CIS correspondent à de nombreuses normes et cadres réglementaires établis, y compris, mais sans s'y limiter, les suivants :

- Le cadre de cybersécurité du NIST (CSF)
- NIST SP 800-53
- La série de normes ISO 27000
- PCI DSS
- HIPAA
- Etc....

Par ailleurs, une fois que les évidences de l'implémentation des contrôles sont envoyées au spécialiste en sécurité informatique, celui-ci, en collaboration avec le détenteur de l'actif, pourra choisir au hasard un nombre maximal de contrôles à vérifier (entre 10 à 25% des contrôles) afin de confirmer si oui ou non, les contrôles sélectionnés ont été implémentés correctement.

PROBABILITÉ DE COMPROMISSION

Pour chaque contrôle évalué lors du test des mesures de contrôles de sécurité, il faudra identifier la probabilité de compromission. Pour chaque vulnérabilité entraînant des répercussions sur les biens inclus dans l'évaluation des menaces et des risques, il faudra déterminer la probabilité de compromission. Par exemple, si les mesures de prévention en place sont très efficaces, la probabilité de compromission qui en découle sera faible. Le tableau ci-dessous nous aidera à évaluer le niveau de probabilité de compromission.

Efficacité des mesures de protection	**Vulnérabilités connexes**	**Probabilité de compromission**
Aucune mesure de protection Mesure de protection inefficace en grande partie Probabilité de compromission > 75%	Facilement exploitables Besoin de peu de connaissances/compétences/ ressources Biens hautement accessibles Employés mal informés/formés	**Élevée**
Mesure de protection modérément efficace Probabilité de compromission 25-75%	Pas facilement exploitables Besoin de certaines connaissances/compétences/ ressources Biens modérément accessibles Employés modérément informés/formés	**Moyenne**
Mesure de protection très efficace Probabilité de compromission < 25%	Difficile à exploiter Besoin de très bonnes connaissances/compétences/ ressources Accès aux biens rigoureusement contrôlé Employés bien informés/formés	**Faible**

Figure 15 : Tableau d'évaluation du niveau de la probabilité de compromission

GRAVITÉ DES CONSÉQUENCES

Pour chaque contrôle évalué lors du test des mesures de contrôles de sécurité, il faudra identifier la gravité des conséquences. Cela veut dire que pour chaque vulnérabilité entraînant des répercussions sur les biens inclus dans l'évaluation des menaces et des risques, il faudra déterminer la gravité des conséquences. Par exemple, si aucune mesure de prévention n'est en place, ou si les mesures sont en grande partie inefficaces, la gravité des conséquences qui en découlera sera élevée.

Le tableau ci-dessous nous aidera à évaluer le niveau de gravité des conséquences.

Efficacité des mesures de protection	**Vulnérabilités connexes**	**Gravité des conséquences**
Aucune mesure de protection Mesure en grande partie inefficace Biens exposés à des préjudices importants	Détection improbable des compromissions Dommage difficile à contenir Employés mal informés/ formés	**Élevée**
Mesure de protection modérément efficace Biens exposés à des préjudices modérés	Compromissions probablement détectées au fil du temps Dommage partiellement contenu Employés modérément informés/formés	**Moyenne**
Mesure de protection très efficace Probabilité de compromission < 25%	Compromissions presque certainement détectées rapidement Dommage rigoureusement contenu Employés bien informés/bien formés	**Faible**

Figure 16 : Tableau d'évaluation du niveau de la gravité des conséquences

ÉVALUATION DES NIVEAUX DES VULNÉRABILITÉS

Pour déterminer le niveau de chaque vulnérabilité, il faut faire correspondre la probabilité de compromission et la gravité des conséquences.

Incidence sur la gravité des conséquences	**Probabilité de la menace**		
	Faible	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très Élevée
Moyenne	Faible	Moyenne	Élevée
Faible	Très faible	Faible	Moyenne

Figure 17 : Tableau du niveau des vulnérabilités

VALEUR ASSOCIÉE DES NIVEAUX POSSIBLES DES VULNÉRABILITÉS

Niveau possible de la vulnérabilité	Très Faible	Faible	Modéré	Élevé	Très Élevé
Valeur associée au niveau de la vulnérabilité	1	2	3	4	5

Figure 18 : Tableau des valeurs associées aux niveaux possibles des vulnérabilités

PHASE 5 : ÉVALUATION DES RISQUES

DÉFINITION DU RISQUE

Le risque est la possibilité qu'une **menace** exploite une **vulnérabilité** pour nuire à un **actif.**

L'évaluation des risques consiste à attribuer une valeur à chaque scénario de risque identifié durant la phase 2 à 4. Cette évaluation peut être quantitative ou qualitative.

ÉVALUATION QUANTITATIVE DU RISQUE

Risque = Valeur de l'actif X Valeur de la menace X Valeur de la vulnérabilité

ÉVALUATION DES NIVEAUX POSSIBLES DES RISQUES

Niveau du risque	Très Faible	Faible	Modéré	Élevé	Très Élevé
Valeur du risque	**[1-4]**	**[5-12]**	**[15-32]**	**[36-75]**	**[80-125]**

Figure 19 : Tableau des valeurs associées aux niveaux possibles des risques

ÉVALUATION QUALITATIVE DU RISQUE

L'évaluation qualitative est suggérée lorsqu'on ne dispose pas de chiffres ou de statistiques pouvant nous aider à faire des calculs mathématiques.

La figure suivante en donne un exemple (tiré de la norme ISO/IEC 27005) :

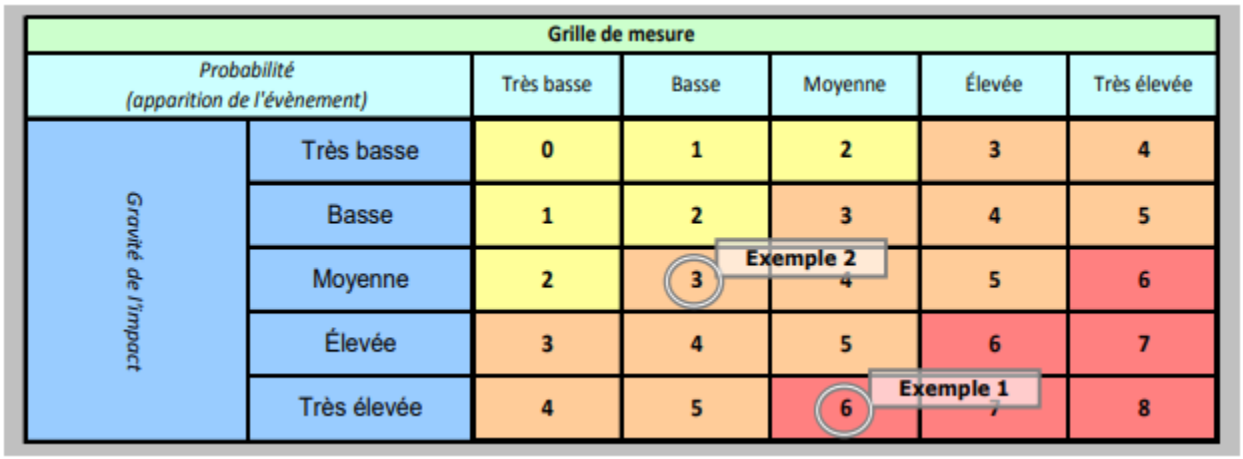

Figure 20 : Grille de mesure des risques (ISO/IEC 27005)

Dans ce cas, l'importance de chaque risque est évaluée en fonction d'une estimation de la probabilité d'apparition des menaces (qui déclencheront le risque) et en fonction de la gravité de l'impact si le risque se concrétise.

Exemple 1 : Une organisation pourrait évaluer à 6 sur 8 l'impact d'un risque d'intrusion de l'extérieur (au moyen d'Internet) qui utiliserait une vulnérabilité non identifiée et qui aurait un impact destructif sur une base de données. La probabilité d'apparition de cette menace pourrait être moyenne et la gravité de l'impact sera très élevée. La mesure de ce risque est de 6.

Exemple 2 : La divulgation volontaire d'information sensible peut être évaluée à 3 si la probabilité de survenance d'un tel événement est basse et que la gravité de l'impact est moyenne.

PHASE 6 : RECOMMANDATIONS

LA RÉPONSE AUX RISQUES IDENTIFIÉS LORS DE L'ÉVALUATION

Une fois l'analyse des risques terminée, la direction de l'université, en collaboration avec le détenteur de l'actif, devra s'attaquer à chaque risque spécifique. Il existe plusieurs réponses possibles au risque :

L'atténuation du risque consiste à réduire le risque, par la sélection et la mise en place de mesures de sécurité ou de contrôles de sécurité.

L'acceptation du risque consiste à prendre le risque, sans mettre de mesures particulières en place soit parce que le niveau de risque est acceptable, soit parce que les conséquences ne sont pas critiques pour l'université.

L'évitement du risque consiste à refuser de prendre le risque. Il sera alors nécessaire soit d'éviter les conditions d'apparition du risque, soit d'éviter une activité qui pourrait faire apparaître le risque.

Le transfert du risque consiste à faire prendre le risque éventuel par une tierce partie jugée plus apte à en assurer le traitement, notamment par le biais d'un contrat.

IDENTIFICATION DES RISQUES INACCEPTABLES

Comme défini dans l'engagement de la direction, chaque université devra définir un niveau de risque acceptable pour son université. Une fois que les risques ont été calculés dans la phase 5 de l'EMR, le CESI recommandera que les universités concentrent leurs efforts sur les risques qui dépassent le niveau de risque au préalablement accepté par chaque université.

Risque évalué	Très Faible	Faible	Modéré	Élevé	Très Élevé
Acceptabilité	**Tout à fait acceptable**	**Probablement acceptable**	**Peut-être inacceptables**	**Probablement inacceptable**	**Tout à fait inacceptable**

Figure 21 : Tableau de l'acceptabilité des niveaux de risques évalués lors de l'EMR

SÉLECTION DES MESURES DE CONTRÔLES POUR LES RISQUES INACCEPTABLES

Une fois les risques non acceptables identifiés, le conseiller en sécurité fournira une liste de contrôle à implémenter dans le but d'abaisser le niveau de risque à un niveau acceptable par les universités.

Une fois approuvées et mises en œuvre, les recommandations devront amener les risques inacceptables à des niveaux acceptables à moindre coût ou au coût le plus raisonnable pour les universités.

ÉVALUATION DES RISQUES RÉSIDUELS PROJETÉS

Le risque résiduel est le risque qui restera après avoir implémenté les recommandations du conseiller en sécurité.

Une fois que les recommandations seront mises en œuvre, il faudra revenir à la phase 4 de l'EMR et recalculer le niveau de vulnérabilité et faire l'étape 5 pour calculer le risque résiduel basé sur la nouvelle valeur de la vulnérabilité.

Ce niveau de vulnérabilité sera logiquement différent de celui calculé au début de l'EMR du fait de l'implémentation effective des recommandations de la phase 6.

PHASE 7 : RAPPORT FINAL

Le rapport de l'évaluation des menaces et des risques doit être présenté au détenteur de l'actif et doit comprendre les parties suivantes :

- Un sommaire des risques résiduels non acceptables et les recommandations à mettre en place pour abaisser ces niveaux de risques à des niveaux acceptables par l'université;
- Toutes les étapes de la phase de préparation;
- Le sommaire de l'identification et l'évaluation des actifs;
- Le sommaire de l'identification et l'évaluation des menaces;
- Le sommaire de l'identification et l'évaluation des vulnérabilités;
- Le calcul des niveaux de risques;
- Le sommaire des recommandations.

PHASE 8 : PLAN D'ACTION ET JALONS

Le plan d'action et jalons est un document qui permet de suivre et de planifier la résolution des risques inacceptables identifiés lors de l'évaluation des menaces et des risques. Il décrit les jalons qui devront être mis en œuvre ou planifiés et identifie les tâches, les ressources nécessaires pour accomplir les éléments du plan ainsi qu'une date d'achèvement.

Le plan d'action et jalons est requis pour chaque système comportant des risques inacceptables.

Numéro	Description du Risque	Impact sur l'université	Severité	Priorite	Actifs touchés	Recommandation	Responsable de la remediation	Statut	Date de la resolution	Actions posées

Figure 22 : Tableau du plan d'action et jalons

PHASE 9 : AUTORISATION D'EXPLOITATION

L'autorisation d'exploitation est un état dans lequel se trouve l'actif pendant la phase d'exploitation et de maintenance de son cycle de vie. Selon NIST, elle constitue une décision de gestion officielle prise par un ou plusieurs hauts fonctionnaires fédéraux d'autoriser l'exploitation d'un système d'information et d'accepter explicitement le risque pour les opérations.

Le CESI recommande que tous ses actifs informationnels obtiennent une autorisation d'exploitation avant de passer à la phase d'exploitation et de maintenance dans son environnement de production.

L'autorisation d'exploitation est un document qui fournit aux détenteurs des informations essentielles afin de prendre une décision crédible, éclairée et fondée sur les risques quant à l'autorisation ou non de l'exploitation de l'actif informationnel.

La décision d'autoriser ou non les opérations est prise sur la base du contenu du dossier d'autorisation du système.

L'auteur de l'autorisation peut émettre une autorisation d'exploiter avec ou sans condition, ou émettre un refus d'autorisation d'exploitation. La décision est basée sur l'acceptabilité des risques résiduels et la nature de la posture de sécurité du système.

RÉVISIONS

Date	Action	Auteur	Version
2023-03-24	Version finale	CESI de l'UQ	1.0

SOURCE

https://www.ncsc.gov.uk/information/understanding-vulnerabilities

https://cyber.gc.ca/sites/default/files/cyber/publications/itsg33-ann3a-fra.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

https://www.cms.gov/files/document/cms-poam-process-guide-v11.pdf

https://csrc.nist.gov/glossary/term/authorization_to_operate

https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/elaboration_miseenoeuvre_processus_gestion_risques_securite_information.pdf

GLOSSAIRE

Une menace représente tout événement ou acte éventuel, délibéré ou accidentel, qui pourrait porter préjudice aux employés ou aux biens et ainsi avoir une incidence négative sur la prestation de services.

Une menace accidentelle représente une menace sans préméditation causée par une personne.

Une menace délibérée représente une menace planifiée ou préméditée par une personne.

Les mesures de protection représentent des contrôles qui ont pour but de réduire les risques globaux à l'égard des employés, des actifs en abaissant la probabilité des incidents ou des compromissions ou en atténuant la gravité des conséquences par l'interaction directe ou indirecte avec les valeurs des actifs, les menaces ou les vulnérabilités.

Un préjudice représente un dommage résultant de la compromission d'un actif.

Le risque accepté représente le niveau de risque approuvé par le responsable de l'acceptation des risques.

Risque résiduel évalué représente la portion du risque qui demeure une fois que les mesures de sécurité visant à le réduire ont été sélectionnées lors de la phase de recommandation et mises en œuvre.

Une vulnérabilité représente une faiblesse quant à la sécurité qui pourrait permettre à une menace de causer préjudice. Elle augmente la probabilité d'un incident, la probabilité de compromission ou la gravité des conséquences. Les vulnérabilités sont inversement proportionnelles à l'efficacité des mesures de protection.