UNIVERSITÉ DE MONTRÉAL

ANALYSES-DIAGNOSTICS DES VULNÉRABILITÉS D'UNE ORGANISATION FACE AUX UTILISATIONS DES TECHNOLOGIES DE L'INFORMATION ET DE COMMUNICATION

MARIEME BEKKALI

DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INDUSTRIEL)

AOÛT 2018

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

ANALYSES-DIAGNOSTICS DES VULNÉRABILITÉS D'UNE ORGANISATION FACE AUX UTILISATIONS DES TECHNOLOGIES DE L'INFORMATION ET DE COMMUNICATION

présenté par : BEKKALI Marieme

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

M. AGARD Bruno, Doctorat, président

M. ROBERT Benoît, Ph. D, membre et directeur de recherche

Mme CORMIER Eve-Marie, PMP, MBCI, BCMS, membre

REMERCIEMENTS

Je voudrais présenter mes remerciements pour toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

En premier lieu, je tiens à remercier mon directeur de recherche Benoît Robert. Merci pour votre soutien, votre accompagnement et votre disponibilité malgré le fait que vous êtes en année sabbatique. J'apprécie sincèrement le temps que vous m'avez accordé et les réflexions que vous avez apportées durant nos discussions.

En second lieu, je tiens à remercier chaleureusement Yannick pour votre accompagnement tout au long de ce projet, votre disponibilité et vos conseils et aides précieux. Ça été un plaisir d'échanger avec vous sur la problématique des technologies de l'information.

Je tiens aussi à remercier tous les membres du CRP, plus particulièrement Delphine pour la bonne compagnie et l'amitié durant mes deux ans à la Polytechnique. Sans oublier le gang du trio Amine, Thierry et Arthur. Merci pour la bonne ambiance.

Je tiens également à remercier les membres du jury pour le temps accordé à la lecture et l'évaluation de ce travail ainsi que pour les propositions qui vont servir à enrichir cette recherche.

Enfin, mes remerciements vont à mes parents et à tous les membres de ma famille qui m'ont encouragé et soutenu tout au long de ma vie. Un grand merci à Hajar ma sœur et ma meilleure confidente qui est toujours là pour m'écouter et me soutenir malgré la distance.

RÉSUMÉ

Les technologies de l'information et de communication (TIC) représentent un élément incontournable pour le développement des organisations. Elles interviennent dans tous les aspects de la chaîne de valeur et leurs utilisations aident les organisations à atteindre leurs objectifs stratégiques et à réaliser leurs missions. Le Centre risque & performance (CRP) oriente actuellement ces travaux de recherche pour développer une nouvelle approche pour mieux identifier et comprendre les vulnérabilités liées aux utilisations effectives des TIC dans les organisations.

Ce mémoire présente la démarche proposée aux gestionnaires des organisations de type petite et moyenne taille pour effectuer des analyses-diagnostics des vulnérabilités liées aux utilisations des TIC. Le premier objectif vise à amener les gestionnaires à caractériser les vulnérabilités technologiques que leurs organisations doivent considérer dans les prises de décision concernant le choix d'une technologie et le choix des stratégies à mettre en place pour assurer le maintien, le rétablissement, la reprise et la sécurité de ces technologies. Le deuxième objectif est de permettre la compréhension des dépendances avec les fournisseurs de ces technologies et les vulnérabilités liées à l'externalisation des TIC.

La démarche proposée est centrée sur la caractérisation des vulnérabilités internes et externes face aux utilisations des TIC. La prise en compte des connaissances obtenues à partir du portrait de l'organisation, du profil des vulnérabilités et du portrait de l'état de préparation permet aux gestionnaires des organisations de concevoir une vision globale sur les enjeux technologiques de leurs organisations. La considération des dépendances avec les fournisseurs des services de TIC dans les analyses-diagnostics des vulnérabilités technologiques a permis de commencer une réflexion chez les gestionnaires sur les critères de choix de leurs fournisseurs de TIC et de les soutenir dans les prises de décision concernant les choix stratégiques.

ABSTRACT

Information and communication technologies (ICT) are considered an essential element for the development of organizations. Their uses help organizations achieve their strategic goals and accomplish their missions. The research center risk & performance of Polytechnique Montreal is currently trying to develop a new approach to better identify and understand vulnerabilities related to the actual uses of ICT in the organizations.

This thesis presents the approach proposed to the managers of organizations of small and medium size to carry out diagnostic analyzes of vulnerabilities related to the uses of ICT. The main purpose is to help managers to characterize all the technological vulnerabilities that their organizations need to consider when making decisions about selecting or changing technology and to choose the useful strategies to maintain, recover and to secure the selected technology. The second purpose is to get the managers to better understand the dependencies link between their organizations and its ICT suppliers and the vulnerabilities related to the outsourcing of their ICT.

The proposed approach focuses on characterizing internal and external vulnerabilities related to the uses of ICT. Using the knowledge obtained from the organization's portrait, the vulnerability profile and the readiness profile, the managers have a global vision on the technological issues of their organizations. Including the dependency link between the organizations and its ICT suppliers in the diagnostic analyzes has made it possible for managers to think about selecting new criteria for choosing their ICT suppliers and to support them in their decision-making about certain strategic choices.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

BIA	Bilan d'Impacts d'Affaires
BCI	Business Continuity Institute
CRP	Centre risque & performance
CEFRIO	Centre Facilitant la Recherche et l'Innovation dans les Organisations
DIMA	Durée d'Interruption Maximale Acceptée
ISO	International Standardization Organizations
MCA	Management de la Continuité d'Activité
NIST	National Institute of Standards and Technology
OCDE	Organisation de Coopération et de Développement Économiques
ORD	Objectif de Restauration des Données
OTR	Objectif du Temps de Restauration
MESI	Ministère de l'Économie, de Sciences et de l'Innovation du Québec
PME	Petites et Moyennes Entreprises
SI	Système d'Information
TI	Technologie de l'Information
TIC	Technologie de l'Information et de Communication

LISTE DES ANNEXES

CHAPITRE 1 INTRODUCTION

Les technologies de l'information et de communication (TIC) sont considérées comme un facteur critique au développement et à la prospérité des organisations (CEFRIO, 2011 ; Deltour & Lithiais, 2014). L'acquisition de ces technologies représente une opportunité de se démarquer par rapport aux compétiteurs et de devenir plus performant (Industrie Canada, 2014). Les organisations dans le monde entier expriment la volonté d'investir dans ce type de technologie (Organisation de coopération et de développement économique [OCDE], 2008). Les entités gouvernementales les encouragent aussi pour saisir l'opportunité du numérique. Pareillement, le gouvernement du Canada appuie cette vision et encourage les organisations du secteur industriel et en particulier les petites et moyennes entreprises (PME) « à accorder plus d'importance à l'adoption, à l'utilisation et à la mise à niveau des technologies numériques afin de conserver un avantage concurrentiel stratégique d'un bout à l'autre des chaînes de valeur » (Gouvernement du Canada, 2014). Dans cette perspective, le gouvernement du Québec, à travers le ministère des Finances et de l'Économie (MFEQ) a lancé sa Stratégie numérique PME 2.0 en 2012 pour encourager les PME à appréhender les TIC comme un levier de bénéfices (productivité, innovation, compétitivité, etc.) et un outil essentiel de contrôle de gestion (Ministère des Finances et de l'Économie du Québec [MFEQ], 2012). En 2017, le Ministère de l'Économie et de l'Innovation du Québec (MESI) en collaboration avec le Centre facilitant la recherche et l'innovation dans les organisations (CEFRIO) ont exprimé la volonté d'amener les organisations de types PME vers l'industrie 4.0.

Le passage à l'industrie 4.0 impose toutefois de nouveaux défis et de nouvelles façons de faire. Les principaux défis qui ressortent de l'utilisation des TIC sont : la sécurité des systèmes technologiques utilisés et la connectivité entre les systèmes industriels et les différentes composantes des outils technologiques (les données, les logiciels et les équipements). En effet, les interdépendances entre les différentes opérations de l'organisation et les outils technologiques utilisés pour les satisfaire augmentent considérablement les vulnérabilités des organisations aux technologies utilisées et aux fournisseurs de celles-ci.

Plusieurs méthodes et techniques ont été développées pour permettre aux gestionnaires des organisations d'analyser et d'évaluer les risques et plus particulièrement les vulnérabilités aux TIC. D'une manière classique, les méthodes et techniques développées accordent la priorité à la sécurité de l'information et servent à se munir de mesures de protection face aux attaques

cybernétiques. En revanche, les vulnérabilités provenant de l'utilisation effective des TIC dans les organisations ont été largement marginalisées.

Ce projet s'inscrit dans le cadre du projet résilience des PME lancé en 2017 par le centre risque & performance (CRP) de l'École Polytechnique de Montréal. La finalité est d'accompagner les gestionnaires des PME dans leurs quêtes d'appréhender les vulnérabilités liées aux utilisations des TIC.

Ce projet vise à proposer aux gestionnaires une démarche simple pour réaliser les analyses-diagnostics des vulnérabilités découlant des utilisations effectives des TIC. Cette démarche doit permettre d'avoir une perception des vulnérabilités technologiques internes et externes.

Ce mémoire est composé de cinq chapitres. Le premier chapitre présente l'introduction de ce projet de recherche. Le deuxième chapitre présente une revue critique de la littérature. La finalité est de positionner ce projet de recherche par rapport aux travaux déjà réalisés. Le troisième chapitre couvre la problématique, les objectifs et la méthodologie de recherche. Le quatrième chapitre porte sur la partie développement et les résultats de ce projet. Le cinquième chapitre est consacré à la discussion, les perspectives et la conclusion.

CHAPITRE 2 REVUE CRITIQUE DE LA LITTÉRATURE

Ce chapitre vise dans un premier lieu à établir un état de connaissance sur les notions clés qui font l'objet de cette recherche : les TIC, leurs utilisations et la notion de la vulnérabilité. Par la suite, une revue de la littérature sur les trois principaux mécanismes d'analyse les plus utilisés au Canada et les plus recommandés par les normes internationales de normalisation (International Standardization Organizations) (ISO) sera présentée. Pour conclure, deux méthodes de gestion des vulnérabilités technologiques dans les organisations seront présentées.

2.1 Les technologies de l'information et de communication

Au cours des deux dernières décennies, les TIC ont marqué la vie des organisations, toutes tailles confondues (Capgemini Consulting, 2013). Au début, elles ont été considérées comme des outils pour accélérer les mécanismes de fonctionnement et accompagner la gestion, mais, progressivement, ces technologies ont pris une place plus importante et depuis elles s'imposent comme un avantage stratégique et concurrentiel. Selon le MESI et le CEFRIO, les TIC ont le pouvoir de propulser les organisations vers de nouveaux sommets et les aider à créer de la valeur et à accroitre leurs productivités (CEFRIO, 2014 ; MESI, 2016).

2.1.1 Les TIC : définition et caractéristiques

La revue de la littérature sur les TIC expose plusieurs définitions dont deux ont été retenues :

- Zuboff (1998) a défini les TIC comme étant le regroupement de plusieurs techniques comprenant l'électronique, l'informatique, les télécommunications, le génie logiciel et l'analyse des systèmes.
- L'Organisation de coopération et de développement économiques (OCDE) définit les TIC comme étant : le regroupement d'un ensemble d'outils qui permet de visualiser, traiter, stocker ou transporter de l'information par des moyens électroniques (OCDE, 2004). Ces outils sont considérés comme source d'information et de connaissance et fournissent un support aux processus transactionnels et décisionnels dans les organisations (Kefi, Kalika & Reix, 2004).

Ainsi, les TIC sont constituées de l'ensemble des techniques et des dispositifs mis en place pour produire, transformer ou échanger des données et des informations en quantité importante en temps réel ou dans des délais très courts. Globalement, les TIC regroupent les technologies nécessaires

pour manipuler les informations pour en faire des données faciles à gérer et à y accéder à tout moment, les technologies nécessaires pour les communiquer et les technologies nécessaires pour les stocker.

Les définitions des TIC mobilisent des notions comme la donnée, l'information, la connaissance, la technologie de communication, la technologie de l'information (TI). Il est donc important de commencer par les clarifier.

Dans la littérature liée au domaine de l'informatique, la donnée est une représentation d'un symbole qui ne prend sens que lorsqu'elle est interprétée et devient une information (Callon, 1989). L'information produite est considérée comme un message significatif et porteur d'un contenu sémantique plus riche que la donnée qui nécessite un support, un émetteur et un récepteur. L'information fait l'objet de traitement ou de manipulation pour la transformer en connaissance. La connaissance quant à elle est considérée comme l'extension de l'information à laquelle on ajoute de la valeur (Callon, 1989). Une autre définition répandue dans la littérature de la connaissance est développée par Howells (2002) qui la définit comme étant un cadre dynamique dans lequel de l'information peut être stockée, traitée et comprise.

Par quels moyens les données, les informations et les connaissances sont-elles produites, traitées, stockées et communiquées ?

Les TIC qui représentent une convergence de trois types de technologies : la technologie de l'information, la technologie de communication et la technologie de l'infonuagique.

- Les technologies de l'information englobent les dispositifs et les systèmes d'information utilisés pour générer, manipuler et sauvegarder les données et les informations avec comme finalité d'aider à la prise de décision nécessaire au gestionnaire et au développement de la stratégie de l'organisation (Autissier & Delaye, 2008 ; Chandler & Munday, 2012).
- La technologie de communication englobe l'ensemble des outils intervenants dans le transfert et la communication de l'information à l'interne et à l'externe de l'organisation (CEFRIO, 2011). Cette technologie facilite la transmission de l'information quel que soit le volume ou la nature (vidéo, son, texte, etc.) et sans être limité par la distance. La particularité de la technologie de communication est qu'elle assure une circulation fluide de l'information ce qui

permet non seulement d'améliorer la prise de décision, mais aussi de l'accélérer (Courtès-Lapeyrat, 2010 ; CEFRIO, 2011).

- La technologie de l'infonuagique, telle que définie par le National Institute of Standards and Technology (NIST) of United States, est « un modèle permettant l'accès sur demande à un réseau comprenant un bassin partagé de ressources informatiques configurables qui peuvent rapidement être activées et désactivées en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur de services » (National Institute of Standards and Technology [NIST], 2017). Cette technologie attire l'intérêt de plusieurs organisations qui souhaitent alléger le fardeau d'acquisition et de gestion des TIC. Elle permet à l'organisation d'utiliser le logiciel et le matériel d'un tiers, plutôt que de le procurer et le gérer elle-même. Le prestataire du service de l'infonuage fournit des services comme : l'utilisation de serveurs à distance pour entreposer des données numériques, offre des outils qui facilitent le partage de documents et de collaboration, etc.

2.1.2 Les utilisations des TIC dans une organisation

2.1.2.1 Les utilisations des TIC dans la chaîne de valeur d'une organisation

Les TIC sont considérées comme une capacité qui donne aux organisations un avantage concurrentiel (Liang et al, 2010). Elles sont reconnues comme un facteur de bénéfices organisationnels et économiques et les organisations sont incitées à les adopter afin de garantir leurs compétitivités et performances (Deltour & Lethiais, 2014). Dans un tel contexte, l'utilisation des ressources en TIC devient un incontournable pour le développement de l'organisation. Elles permettent à cette dernière de réaliser ses activités, d'atteindre ses objectifs stratégiques, d'améliorer ses performances et ses gains de productivité. Globalement, elles permettent de créer de la valeur.

Dans la théorie des organisations, l'approche systématique développée par Porter (1985) démontre aussi que les TIC constituent un avantage concurrentiel. Porter (1985) explique dans son ouvrage l'avantage concurrentiel que les TIC procurent dans tous les aspects de la chaîne de valeur en supportant toutes les activités de l'organisation pour générer de la valeur.

Les types d'activités qu'on trouve souvent dans les organisations et qui font appel aux utilisations des TIC sont :

- La production.
- La gestion administrative.
- La gestion des ressources humaines.
- La recherche et le développement.
- La chaîne d'approvisionnement.
- La logistique (gestion des stocks, gestion des commandes, etc.).
- Le marketing et la vente.
- Les services.

Dans la chaîne de Porter, les activités sont séparées en deux familles : les activités principales et les activités de soutien. L'appartenance d'une activité à la famille d'activités principales ou de soutien peut varier selon le secteur d'activité de l'organisation (industrie, services, organisme, etc.) et sa mission principale. Porter (1985) précise que les outils technologiques sont utilisés dans l'ensemble des activités de l'organisation pour générer une marge de valeur.

2.2 La prise en compte de la notion de vulnérabilité dans les mécanismes d'analyse

Cette partie porte sur la notion de la vulnérabilité et les trois principaux mécanismes d'analyse les plus utilisés dans les organisations qui prennent en compte les vulnérabilités (International Standardization Organizations [ISO] 22301, 2012 ; ISO 27001, 2013; Business Continuity Institute [BCI], 2013). Tout d'abord, une définition de la notion de la vulnérabilité est présentée. Ensuite, le mécanisme d'analyse utilisé dans la gestion des risques recommandé par la norme internationale ISO 27000 sur le management des risques liés à la sécurité des systèmes d'information (ISO 27000, 2013) est exposé. Puis, les deux mécanismes d'analyse utilisés dans la gestion de la continuité et recommandés dans les guides de bonnes pratiques en matière de la gestion de la continuité des activités développées par le Business Continuity Institute (BCI) et la norme internationale ISO 22301 du système de management de la continuité des activités (ISO 22301, 2012 ; BCI, 2013) sont exposés. La prise en compte de la vulnérabilité qui fait partie des notions clés de cette recherche était parmi les critères de choix de ces trois mécanismes d'analyse.

2.2.1 La notion de vulnérabilité

La notion de vulnérabilité représente une composante importante dans le domaine de la gestion des risques. Plusieurs définitions ont été développées et adaptées aux besoins spécifiques du contexte dans lequel elles sont utilisées. Bien que les définitions de la vulnérabilité soient multiples et sujettes à débat, nous avons retenu celle du CRP jugé significatif pour nos travaux.

2.2.1.1 Les travaux du Centre risque & performance sur la vulnérabilité

Depuis 2008, le CRP, dirigé par Benoît Robert, préconise une approche de gestion des risques centrée sur les conséquences des risques et la vulnérabilité des organisations face à ces derniers (Robert, 2008). Contrairement à l'approche classique probabiliste qui donne une place centrale à la notion d'aléa/menace et sa probabilité d'occurrence, cette approche est intéressante dans la mesure où elle considère non seulement les aléas (menaces), les vulnérabilités et les conséquences potentielles pour définir le risque, mais également l'état de l'organisation (Petit & Robert, 2009).

2.2.1.1.1 Définitions de la vulnérabilité

- Robert (2008) définit la vulnérabilité comme étant « la susceptibilité d'une organisation à subir des défaillances dans le temps ».
- Petit (2009) précise dans ses travaux que la vulnérabilité d'une organisation est déterminée en fonction de son état et de la façon dont un aléa peut agir et engendrer des conséquences (Petit, 2009).
- La définition adaptée par Benon (2017) au besoin des PME en matière des vulnérabilités liées aux utilisations des TIC est déduite de la définition de Robert (2008). Benon (2017) définit la vulnérabilité comme étant « La caractérisation dans le temps de la susceptibilité d'une PME à subir des défaillances par rapport à l'utilisation des TIC et à la cohérence entre les visions organisationnelles et techniques de ces utilisations » (Benon, 2017). Cette définition met l'accent sur la cohérence entre les visions technique et stratégique d'une organisation, la notion de susceptibilité et la notion de temporalité.

Dans l'ensemble, toutes les définitions de la vulnérabilité développées par le CRP ont en commun la perception de la vulnérabilité comme étant la susceptibilité d'une organisation à être exposée aux atteintes des aléas ou menaces et à subir les conséquences potentielles. De plus, la vulnérabilité

d'une organisation dépend de son état de préparation à faire face aux menaces et à minimiser les conséquences potentielles.

2.2.1.1.2 Rapport entre risque, vulnérabilité, menace et impacts

La notion de la vulnérabilité est souvent utilisée dans le même contexte que la notion du risque, des menaces et des impacts. Pour comprendre le lien entre ces quatre notions, il convient de commencer par les définir.

- **La menace :**

La menace telle que définie par la norme ISO 22300 (2012) est « toute cause potentielle d'incidents (indésirables) susceptible de causer des dommages pour un individu, un système ou une organisation ». Une menace exploite une vulnérabilité pour déclencher un événement d'attaque entrainant un risque.

- **La vulnérabilité :**

La notion de vulnérabilité est considérée comme la composante intrinsèque du risque (Cardona, 2004). La vulnérabilité est aussi connue par la qualité de ce qui est susceptible d'être exposé aux menaces. Elle dépend notamment de l'état de l'organisation et de la manière dont une menace pourrait se propager à travers les différents départements et activités de l'organisation pour la rendre inapte à fonctionner d'une manière acceptable.

- **Les impacts :**

Les impacts potentiels renvoient à l'ensemble des dommages qui peuvent toucher directement ou indirectement les missions et les objectifs principaux de l'organisation.

- **Le risque :**

Dans la norme ISO 27000 (2013), le risque est vu comme « l'effet de l'incertitude sur l'atteinte des objectifs » (ISO 27000, 2013). Le risque est souvent caractérisé par référence à des événements et à des conséquences potentielles et est souvent exprimé en fonction de la menace, la vulnérabilité et l'impact [Risque = fonction (menace, vulnérabilité, impacts)].

2.2.2 Le mécanisme d'analyse dans la gestion du risque

La problématique de l'utilisation des TIC, traitée dans ce projet de recherche, explique le choix de l'utilisation de la norme de gestion des risques de la sécurité des systèmes d'information ISO 27000 (2013) comme référence au lieu de la norme générale du management des risques ISO 31000 (2009).

La gestion du risque correspond aux activités coordonnées permettant d'orienter et de contrôler un organisme en matière de risque (ISO 27000, 2016). Elle utilise l'approche préconisée dans la famille des normes ISO/CEI 27001[1] et sert comme une base à l'établissement de la politique de sécurité de l'organisation. Elle dispose d'un processus global qui permet à l'organisation d'identifier, d'analyser et de traiter les risques auxquels elle est soumise, quelles que soient leurs natures, leurs probabilités d'occurrence et leurs conséquences potentielles sur le fonctionnement de l'organisation.

L'objectif de la gestion du risque est d'établir un état de connaissance sur les risques encourus au sein d'une organisation, de déterminer les scénarios les plus probables et de permettre à l'organisation de prendre les décisions les plus adaptées à ses besoins au regard de ses moyens (Mayer & al, 2008). Pour assurer la pertinence des décisions prises, le processus d'analyse doit être établi d'une manière systématique et prendre en compte toutes les menaces, les vulnérabilités et les conséquences potentielles.

---

[1] « ISO/CEI 27001 fait partie de la famille de norme internationale ISO/CEI 27000 qui spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. La présente norme internationale comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation » (ISO/CEI 27001, 2013).

2.2.2.1 L'analyse du risque

L'analyse du risque constitue le cœur de la démarche de gestion du risque et fait partie de la phase d'appréciation dans le processus global de la gestion du risque. Dans la norme ISO 27005 (2013), l'analyse du risque est orientée vers la sécurisation des systèmes d'information.

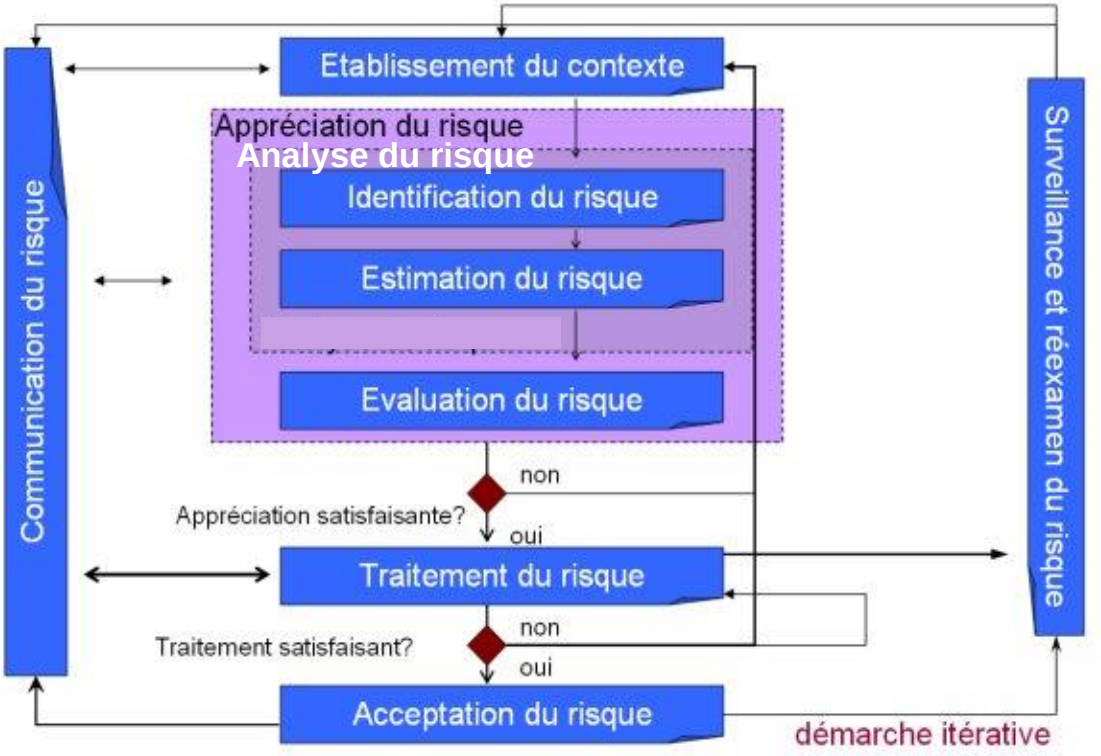

Figure 2.1: Processus de gestion du risque ISO/CEI 27005 (ISO/CEI 27005, 2008).

La figure 2.1 présente les principales étapes comprises dans le processus de gestion du risque :

- Établissement du contexte.
- Appréciation du risque.
- Traitement du risque.
- Acceptation du risque.
- Communication du risque.
- Surveillance et réexamen du risque.

Le processus d'analyse du risque, illustré dans la figure 2.1, est intégré dans l'appréciation du risque et se fait en deux étapes :

- **Étape 1 : Identification du risque**

Dans cette étape, il s'agit d'identifier et de caractériser chaque composante du risque : menace, vulnérabilité, impacts ainsi que les actifs et les mesures de protection existantes. La finalité est de comprendre comment, quand et pourquoi ces risques peuvent arriver, de déterminer les actifs qui seront les plus touchés et les mesures de protection existantes, etc.

- **Étape 2 : Estimation du risque**

Cette étape permet d'estimer les conséquences potentielles ainsi que les probabilités d'occurrence. Les méthodes utilisées pour estimer les conséquences et les probabilités peuvent être quantitatives ou qualitatives (par exemple : une échelle de fort, moyen, faible, etc.). Les valeurs estimées sont ensuite utilisées pour obtenir une estimation des risques auxquels l'organisation fait face. L'analyse de risque permet d'évaluer les risques et de les prioriser ce qui permet de concevoir les plans de traitement et d'assurer l'atteinte des objectifs de sécurité fixés par l'organisation.

2.2.3 Les mécanismes d'analyse dans la gestion de la continuité des activités

La gestion de la continuité des activités est considérée comme un « processus de management holistique qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs » (ISO 22301, 2013). La norme internationale pour les systèmes de management de la continuité des activités ISO 22301 (2013) couvre principalement les domaines suivants :

- La résilience opérationnelle.
- La préparation à des situations d'urgence.
- La gestion des crises.
- La reprise des activités.

Le guide de bonnes pratiques de BCI qui est basé sur les lignes directrices de la norme ISO 22301[2] présente deux mécanismes d'analyse utilisés dans la gestion de la continuité des activités : l'analyse des menaces et le bilan d'impacts d'affaires (BIA). Tel qu'indiqué dans le guide de bonnes pratiques sur la gestion de la continuité du BCI, le BIA et l'analyse des menaces sont utilisés dans l'étape « Analyse » du processus holistique du cycle de vie du management de la continuité d'Activité (MCA) qui vise l'amélioration de la résilience organisationnelle et de la capacité de réponse de l'organisation (BCI, 2013).

Les principales étapes du cycle de vie du MCA sont:

- Le management de la politique et du programme du MCA fait partie des pratiques professionnelles de management qui définit la politique de l'organisation en matière de gestion de la continuité et la façon dont elle va être mise en œuvre et validée (BCI, 2013).
- L'incorporation de la continuité d'activité est aussi une pratique professionnelle de management qui a pour but d'intégrer les principes de la continuité dans la vie quotidienne et la culture de l'organisation.
- L'analyse fait partie des pratiques professionnelles techniques dans le cycle de vie du MCA qui « passe en revue et évalue une organisation en termes d'objectifs, de fonctionnement et de contraintes de l'environnement dans lequel elle opère » (BCI, 2013).
- La conception est la pratique professionnelle technique qui permet d'identifier et de choisir les stratégies de continuités adéquates aux besoins de l'organisation.
- La mise en œuvre est la pratique professionnelle technique qui met en œuvre les stratégies choisies lors de la conception du plan de continuité d'activité (PCA) (BCI, 2013).
- La validation est la pratique professionnelle technique qui permet de valider la conformité du programme de MCA avec les objectifs fixés dans la politique de management de la continuité d'activité (BCI, 2013).

Dans la suite les deux mécanismes préconisés par le BCI pour conduire l'analyse de l'organisation durant le cycle de vie du MCA seront expliqués.

[2] ISO 22301 est la norme du système de management pour la gestion de la continuité des activités.

2.2.3.1 L'analyse des menaces

L'analyse des menaces fait partie des pratiques professionnelles techniques utilisées dans l'étape d'analyse dans le cycle de vie du MCA. L'analyse des menaces fait référence à un « processus d'analyse visant à identifier les concentrations inacceptables des risques sur les activités et les points communs de défaillance » (BCI, 2013). L'approche préconisée dans l'analyse des menaces est semblable à celle utilisée dans l'appréciation du risque de la sécurité d'information. L'identification des menaces qui pourraient causer une perturbation ainsi que l'évaluation de leurs probabilités d'occurrence et leurs impacts permettront de prioriser les menaces selon leur niveau d'impact sur les activités et d'identifier les activités et les sources de vulnérabilité. La finalité de cette analyse est de fournir un appui à la conception des stratégies de continuité visant à réduire les probabilités d'occurrence et à minimiser les impacts sur les activités les plus vulnérables.

2.2.3.2 Le bilan d'impacts d'affaires

Le bilan d'impacts d'affaires (BIA) est le résultat d'un processus d'analyse préconisé par le BCI pour des fins de mise en œuvre des bonnes pratiques de la continuité d'activité. Avec l'analyse des menaces, le BIA arrive à soutenir la conception des stratégies de continuité des activités correspondantes aux besoins établis.

La prise en compte des sources de vulnérabilité identifiées dans l'analyse des menaces permet de faciliter la compréhension des vulnérabilités pouvant influencer les activités critiques de l'organisation. Le BIA vise à spécifier et à identifier les activités qui doivent être redémarrées au plus vite. Globalement, le BIA permet de :

- Documenter les impacts des perturbations dans le temps.
- Mieux comprendre la tolérance de l'organisation aux interruptions et fournir les informations nécessaires à l'élaboration des stratégies de continuité appropriées.
- Dresser un bilan des activités critiques de l'organisation, de leurs dépendances entre elles. Ainsi que la séquence de rétablissement et les moyens sous-jacents (environnement, système d'information (SI), site de secours, site de repli, local, ressources humaines (RH), logistique, etc.) nécessaires à leur reprise.
- Identifier la durée d'interruption maximale acceptée (DIMA).

- De façon à soutenir une reprise rapide des activités, établir une liste des ressources requises : personnes (nombre, expertises, etc.), processus (dépendances internes et externes) et outils (équipements, systèmes informatiques, ressources vitales, etc.).

2.2.3.2.1 Les types de BIA

Le guide de bonnes pratiques du BCI indique qu'il existe quatre types de BIA :

- Le BIA initial est utilisé pour définir le cadre de l'analyse et sert comme intrant pour les BIA stratégique, tactique et opérationnel. À ce point-là, un découpage de l'organisation en activités ou processus est fait et les objectifs de l'analyse sont fixés.
- Le BIA stratégique est utilisé pour identifier les activités les plus critiques notamment celles qui ont un impact sur les objectifs, le fonctionnement de l'organisation ainsi que les contraintes de l'environnement. La priorisation des activités selon leurs criticités, la définition des niveaux de perturbations tolérables ainsi que l'évaluation de la durée d'interruption maximale acceptée (DIMA), l'objectif du temps de restauration (OTR) et l'objectif de restauration des données (ORD) occupent les axes centraux du BIA stratégique.
- Le BIA tactique permet d'identifier les liens de dépendances entre les activités ou processus les plus critiques et d'estimer les impacts potentiels lors des perturbations sur la réputation, la finance, les contrats, règlements, etc.
- Le BIA opérationnel permet de déterminer les ressources exigées pour la reprise des activités les plus critiques. Les exigences en termes de ressources peuvent être pondérées et synchronisées avec la DIMA, l'OTR et l'ORD définis dans le BIA stratégique.

À l'issue du BIA, une vue d'ensemble de l'organisation est établie. Les informations collectées servent de base pour établir des stratégies de continuité et de dresser un bilan des activités prioritaires ainsi que les ressources nécessaires pour la reprise lors d'une perturbation. Il est donc vu comme le point d'appui d'un plan de continuité des activités.

Le BIA est la méthode la plus complète en termes d'analyse. Le guide de bonnes pratiques développé par le BCI fournit les principales étapes à suivre pour conduire un BIA. Il propose les grandes lignes à suivre dans tous les niveaux de l'organisation (stratégique, tactique et opérationnel), toutefois, il n'y a aucune indication sur la manière de le compléter.

Nous pouvons synthétiser les trois mécanismes d'analyse utilisés dans le domaine de la gestion des risques et le domaine de la gestion de la continuité les plus utilisés dans la figure 2.2. Cette dernière permet de présenter les éléments nécessaires à la conception des plans de traitement, des plans de continuité et à la conception des stratégies de la reprise des activités.

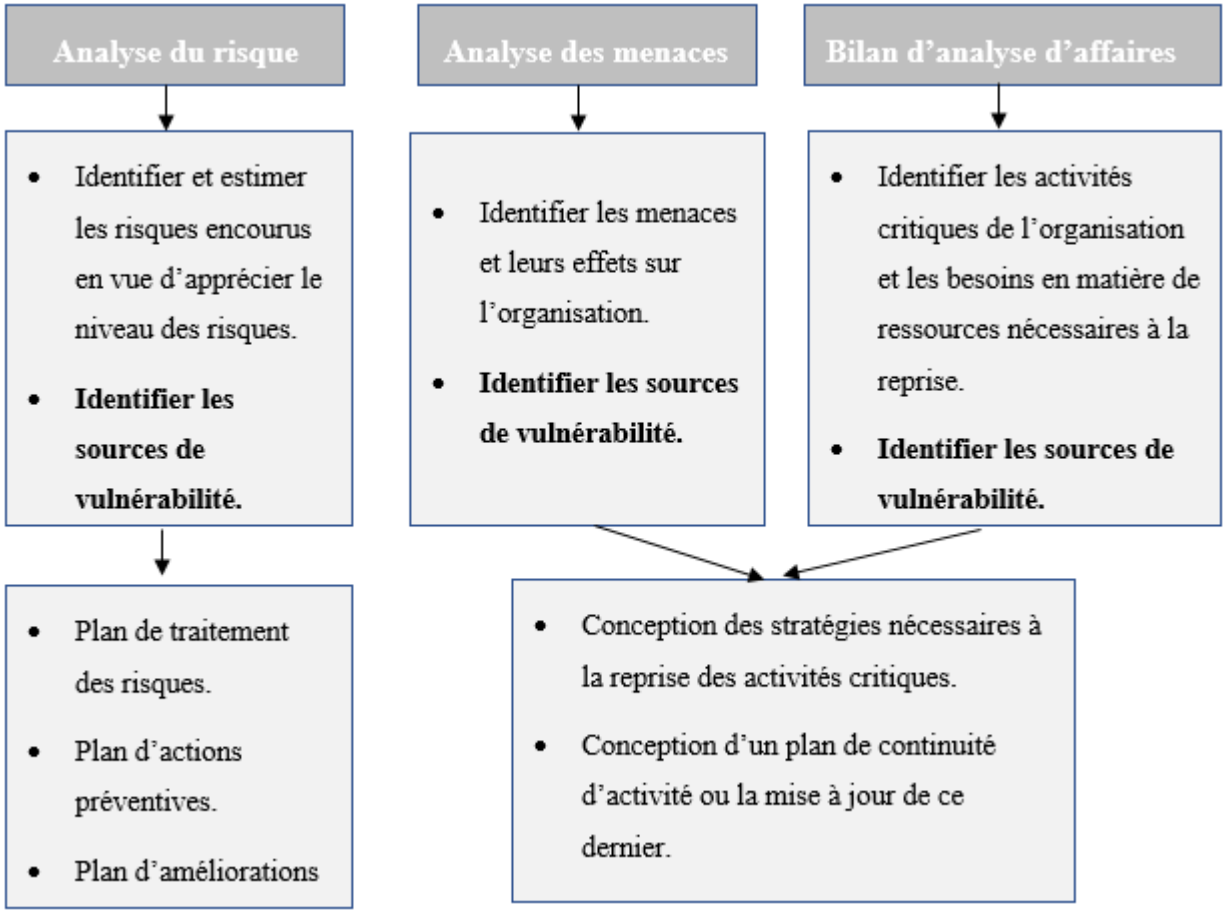

Figure 2.2 : Schéma synthétique des trois mécanismes d'analyse utilisés dans le domaine de la gestion des risques et la gestion de la continuité.

Les mécanismes d'analyse présentés, auparavant, sont considérés comme des démarches générales qui peuvent être adaptées au contexte de l'organisation pour résoudre des problèmes spécifiques. Dans le contexte de ce projet, la problématique traitée porte sur les utilisations des TIC. Donc, il sera intéressant de présenter les méthodes de gestion des risques et des vulnérabilités qui sont plus adaptées à notre contexte de recherche.

2.3 Méthodes de gestion des risques et des vulnérabilités face aux TIC

Plusieurs méthodes de gestion des risques et de vulnérabilités ont été développées pour répondre aux besoins spécifiques des gestionnaires des TI. L'étude approfondie de leurs concepts et processus nous a permis de constater que ces méthodes sont utilisées pour des fins d'analyse ou d'évaluation des risques et/ou des vulnérabilités des systèmes technologiques. La méthode OCTAVE et la méthode MEHARI qui sont présentées par la suite font partie des méthodes les plus utilisées en Amérique du Nord (Club de la sécurité de l'information du Québec, 2013). La méthode OCTAVE est utilisée pour évaluer la vulnérabilité et la méthode MEHARI est utilisée pour analyser les risques des systèmes technologiques.

2.3.1 La méthode OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) est une méthode qualitative d'évaluation des vulnérabilités développée par le Software Engineering Institute (SEI) de l'Université Carnegie Mellon aux USA, à travers son programme Computer Emergency Response Team (CERT) reconnu dans le domaine de la sécurité des systèmes d'information. La méthode est largement utilisée en Amérique du Nord et est conçue pour les organisations de grandes, moyennes et petites tailles. Elle dispose aussi de plusieurs versions : OCTAVE, OCTAVE-S et la dernière version OCTAVE-Allegro (Computer Emergency Response Team (CERT), 2007). En effet :

- La méthode OCTAVE est utilisée dans les grandes organisations et fournit les lignes directrices pour conduire une évaluation des vulnérabilités liées à la sécurité des systèmes d'information à l'intérieur de l'organisation et nécessite des connaissances techniques poussées.
- La Méthode OCTAVE-S a été développée pour les petites organisations. L'équipe d'analystes qui s'occupe de l'évaluation des vulnérabilités doit avoir une excellente connaissance de l'organisation à savoir les exigences de sécurité, les menaces et les pratiques de sécurité utilisées.
- La méthode OCTAVE-Allegro est la dernière version développée pour les petites organisations. Elle permet de réaliser une évaluation rapide des risques touchant les actifs informationnels de l'organisation. La méthode s'appuie sur une approche d'accompagnement structurée, dans la mesure où elle décrit la démarche à suivre ainsi que les outils nécessaires à

l'évaluation des vulnérabilités (questionnaires structurés pour chaque étape). Les détails concernant les étapes d'OCTAVE-Allegro sont développés dans l'annexe A.

2.3.1.1 Les principales phases de la méthode OCTAVE-Allegro

La méthode OCTAVE-Allegro fournit un processus d'évaluation des vulnérabilités, composé de trois phases principales synthétisées dans la figure 2.3 :

Phase 1 : Vue organisationnelle

Dans cette phase les analystes identifient les informations de la direction, de l'équipe opérationnelle et l'équipe de sécurité pour établir un profil des menaces. L'objectif est d'établir les critères d'évaluation des vulnérabilités, de développer un profil des actifs qui décrit les caractéristiques des actifs, leurs propriétaires, leurs valeurs, etc. Les objectifs en matière de sécurité pour chaque actif identifié sont fixés dans cette phase ainsi que les mesures actuelles mises en place pour protéger ces actifs.

Phase 2 : Vue technique

Dans cette phase, les actifs sont priorisés selon leurs criticités (importance, impacts, etc.). Ensuite, un audit des menaces techniques est établi pour identifier les sources de vulnérabilités. Il convient aussi d'identifier dans cette phase les scénarios de menaces les plus probables.

Phase 3 : Développement d'une stratégie de sécurité

Lors de la phase 2, les risques sont identifiés, analysés et évalués sur la base des informations tirées de la phase vue organisationnelle et de la phase vue technique. Ainsi le développement d'une stratégie de la sécurité est fait et le plan d'atténuation est établi.

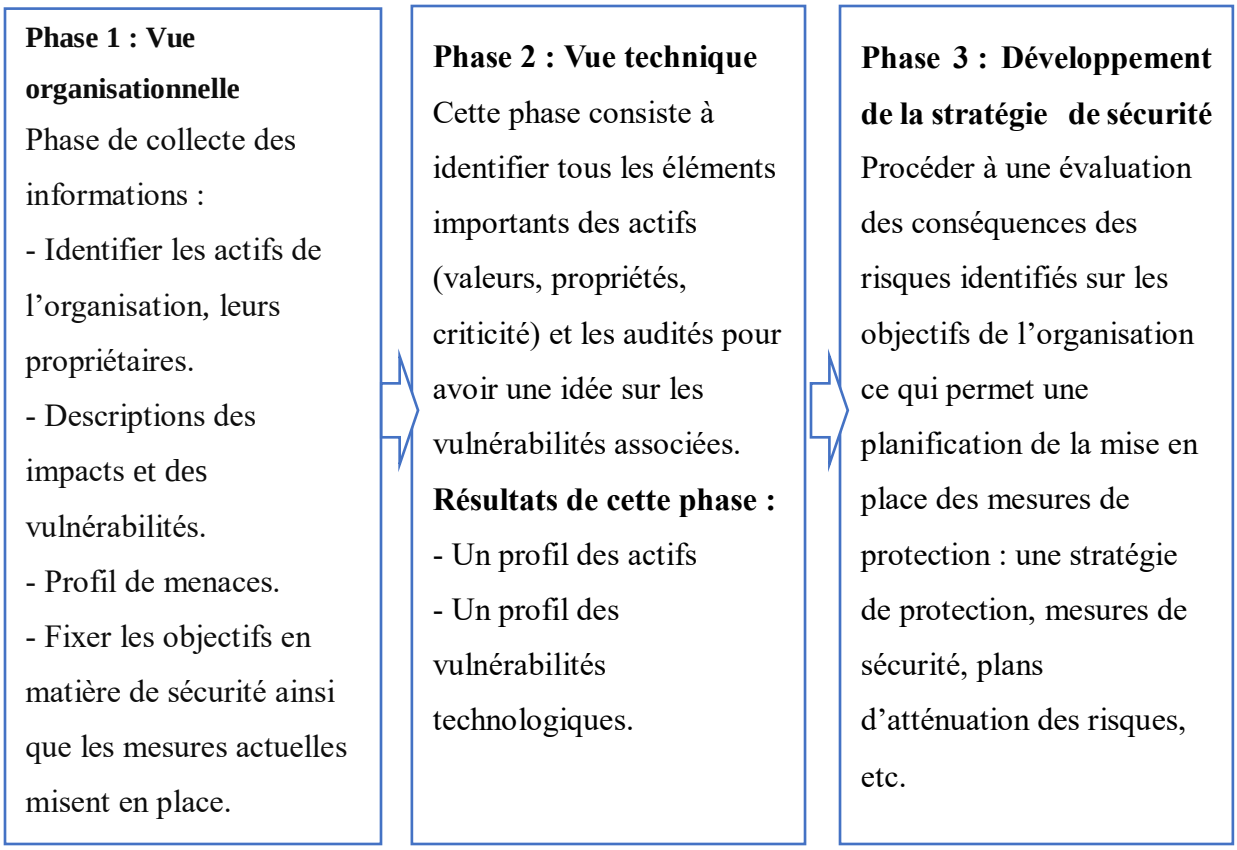

Figure 2.3**:** Synthèse de la méthode OCTAVE-Allegro

2.3.1.2 Apports et limites de la méthode OCTAVE-Allegro

Les apports et les limites de la méthode OCTAVE-Allegro peuvent être résumés en quelques points :

- **Les apports :**

- OCTAVE-Allegro est une méthode bien documentée. Elle se caractérise par la facilité de la mise en place et couvre l'ensemble de l'organisation.
- Les questionnaires utilisés sont ciblés et adaptables à tout type d'organisation.
- Le profil de menaces établi peut être utilisé comme base de formations et des exercices pour améliorer le réflexe des intervenants lors d'une perturbation.
- Le profil de vulnérabilités technologiques peut servir pour cibler les points d'amélioration.

- **Les limites :**

- Le concept sur lequel la méthode OCTAVE-Allegro est basé ressemble à celui du processus de gestion des risques. En effet, l'approche par scénario traite des scénarios les plus susceptibles d'être réalisés, ce qui limite sa portée et amplifie la possibilité de passer à côté les scénarios les moins probables.
- Méthode qui tient compte seulement des actifs informationnels et l'aspect de la sécurité des TIC et donne peu d'importance aux utilisations réelles des TIC.

2.3.2 La méthode MEHARI

MEHARI « Méthode harmonisée d'Analyse des Risques » est une méthodologie française développée par le Club de la sécurité de l'information français (CLUSIF) en 2004 et mise à jour en 2010 (Club de la sécurité de l'information français [CLUSIF], 2010). MEHARI a pour objectif l'évaluation et le management des risques de sécurité qui touchent les systèmes d'information. La méthode offre la possibilité de gérer les risques liés aux scénarios grâce à des formules et des outils qui permettent de qualifier et quantifier tous les éléments de risque (CLUSIF, 2010).

2.3.2.1 Les principales phases de la méthode MEHARI

La méthode MEHARI comprend trois phases (CLUSIF, 2010) :

Phase 1 : La phase préparatoire

Cette phase consiste à définir le contexte et le champ d'application, d'identifier et d'analyser les enjeux de sécurité, des menaces et des vulnérabilités attachées aux actifs (l'entité, le site, les locaux, les applicatifs, les services offerts par les systèmes et l'infrastructure, les développements et la maintenance des logiciels, les réseaux et les télécoms). De plus, l'audit des vulnérabilités des services de sécurité permet de déterminer les points faibles et l'efficacité des mesures de sécurité en place. Cette phase facilite la réalisation d'un plan d'action et permet de générer le plan stratégique de sécurité. Ce dernier permet de fixer les objectifs de sécurité pour chaque actif identifié et de définir la politique de sécurité ainsi que la charte d'utilisation des systèmes d'information pour ses utilisateurs.

Phase 2 : Analyse des risques

Dans cette phase, l'analyste du risque doit permettre de détecter les scénarios de risque qui peuvent remettre en cause les objectifs de sécurité de l'organisation. Une analyse et une évaluation des risques (probabilité, impact) sont réalisées en vue de choisir les mesures de traitement. Le résultat de cette phase est la conception du plan opérationnel de sécurité qui définit les mesures de sécurité à mettre en œuvre.

Phase 3 : La planification de mise à niveau de la sécurité des systèmes d'information

Dans cette phase, les scénarios de risque choisis sont analysés pour planifier les options de traitement. Le résultat de cette phase est la conception du plan opérationnel d'entreprise qui assure le suivi et l'élaboration d'indicateurs sur les risques identifiés et le choix des scénarios contre lesquels il faut se prémunir.

En résumé, la méthode MEHARI offre aux gestionnaires de TI une démarche qui répond aux besoins de la sécurité des systèmes d'information de l'organisation. Les audits des vulnérabilités qu'elle propose permettent la création de plans d'action concrets (plan de sécurité stratégique, plan de sécurité opérationnel et le plan opérationnel d'entreprise). Cette méthode permet donc de construire une politique solide de sécurité destinée à pallier les vulnérabilités constatées lors des audits ainsi que de piloter la sécurité des systèmes d'information en utilisant les outils qu'elle propose aux organisations voulant gérer les risques de sécurité des TI. Globalement, la méthode est conçue pour le besoin d'un gestionnaire de TI et pour les grandes organisations qui ont les moyens et les expertises en TI.

2.3.3 Les pratiques de gestion dans les PME

L'utilisation des pratiques de gestion est une question d'efficacité et de survie pour les organisations, quelle que soit sa taille. Pour les PME, les pratiques de gestion sont incorporées selon la vision de son dirigeant qui assume dans la majorité des cas le rôle du gestionnaire.

Julien (1988) précise dans ces travaux que les particularités d'une PME expliquent les pratiques de gestion dans ce type d'organisation. En effet, les particularités d'une PME sont :

- Une PME est limitée par la taille, la structure de l'organisation est aléatoire, les tâches sont moins spécialisées et les employés assument plusieurs tâches et responsabilités.

- La gestion d'une PME a tendance à être centrée sur la vision du gestionnaire. Il est responsable de l'atteinte des objectifs, de la prise de décision et de la circulation de l'information critique.
- Pour les TIC utilisées dans les PME, il est constaté qu'il y a une dépendance quasi-totale aux fournisseurs pour l'acquisition, le maintien et le support technique de ces technologies.

La présentation des particularités des PME va permettre de contextualiser le rôle que les TIC jouent dans le fonctionnement des PME et les vulnérabilités découlant de leurs utilisations.

La relation à l'informatique n'est pas évidente pour les PME (Deltour & Lethiais, 2014). Les PME déploient souvent un « sentiment d'impuissance face aux TIC » (Deltour & Lethiais, 2014). La complexité de ces technologies et le manque de compétences spécialisées renforcent ce sentiment d'impuissance.

L'étude des particularités des PME montre qu'il y a un besoin plus grandissant dans ce type d'organisation en matière d'analyse des vulnérabilités liées aux utilisations des TIC. Le type d'analyse proposé dans les travaux de recherche présentés dans ce mémoire s'applique particulièrement bien avec le contexte des organisations du type PME. Le but est d'alléger le fardeau du gestionnaire qui n'a pas nécessairement les connaissances techniques assez poussées pour effectuer des analyses techniques comme celles proposées dans MEHARI ou OCTAVE-Allegro.

CHAPITRE 3 PROBLÉMATIQUE DE LA RECHERCHE

3.1 Contextualisation du projet

Actuellement, il est possible d'observer une croissance accélérée de l'acquisition des TIC dans les PME et la volonté de ces dernières de faire partie de la quatrième révolution industrielle qui promet plus de performances (OCDE, 2014). Dans ce contexte, le MESI s'est mobilisé en lançant « l'initiative Industrie 4.0 » en 2017 qui s'inscrit dans le Plan d'action en économie numérique (MESI, 2017) qui a pour objectif d'informer et sensibiliser les PME aux gains associés à l'appropriation de ces technologies, aux changements apportés aux modèles d'affaires, à la chaîne de valeurs et aux modes de gestions lors du passage à la nouvelle ère (MESI, 2017).

Le CRP de sa part, se focalisant sur la résilience des organisations, profite de cette opportunité pour démarrer avec des PME partenaires, un projet phare sur leur résilience qui couvre : l'aspect des changements climatiques, la prise en compte des interdépendances dans les plans de continuité et les technologies de l'information. Ce projet de recherche vise à développer des outils adaptés aux spécificités des PME et aux besoins de ces gestionnaires.

Le projet de recherche actuel vient compléter les travaux de recherche initiés par Benon (2017) sur les vulnérabilités liées aux utilisations des TIC.

3.2 Définition du problème

Le besoin grandissant d'appréhender les vulnérabilités qui accompagnent l'utilisation des TIC demande d'aider les gestionnaires à effectuer des analyses systématiques qui vont servir de base pour mieux planifier, organiser et cibler les mesures de protection à mettre en place.

Les constats issus de la revue de la littérature peuvent être synthétisés en trois points :

- Il existe trois mécanismes largement utilisés en Amérique du Nord pour effectuer les analyses, soit l'analyse des risques (ISO 27005, 2011), le bilan d'impacts d'affaires (ISO 22301 ; BCI, 2013) et l'analyse des menaces (ISO 22301 ; BCI, 2013). Toutes les analyses prennent en compte les vulnérabilités des systèmes technologiques, toutefois peu d'attention est portée aux utilisations de ces systèmes dans la réalisation de la mission de l'organisation. Aussi le mécanisme d'analyse d'affaires présenté dans le guide de bonnes pratiques du BCI couvre seulement les grands axes d'analyse, sans traiter du comment le BIA est complété.

- La méthode de gestion des vulnérabilités OCTAVE-Allegro (2007), et la méthode d'analyses des risques technologiques MEHARI (2010) sont basées sur une approche par scénario et/ou probabiliste et traitent des aspects techniques ou organisationnels séparément et pas vraiment des utilisations effectives des TIC.
- Les particularités des PME, présentées précédemment, montrent qu'elles ont un besoin grandissant pour acquérir des outils organisationnels qui vont permettre aux gestionnaires des PME de mieux comprendre et d'appréhender les vulnérabilités accompagnant les utilisations des TIC. Le problème majeur dans le contexte des PME est le manque d'expertises techniques nécessaires pour en faire des analyses techniques détaillées.

Dans ce contexte, le projet du CRP sur la résilience des PME est réalisé en deux phases dont les travaux de recherche du présent mémoire s'inscrivent dans la phase 2.

La phase 1 consiste à établir un portrait des vulnérabilités liées aux utilisations des TIC. Cette phase a été couverte par le projet réalisé par Benon (2017). Elle vise à proposer une nouvelle approche d'étude des vulnérabilités technologiques qui se focalise sur l'utilisation réelle de ces technologies. Le portrait des vulnérabilités établi a permis aux gestionnaires des PME d'avoir une vision qui englobe l'aspect organisationnel et technique et utilise une approche basée sur les contraintes de l'organisation.

La phase 2 consiste à proposer des analyses-diagnostics des vulnérabilités liées aux utilisations des TIC. Les résultats des travaux de la phase 2 sont présentés dans ce mémoire. Ils vont permettre de compléter le profil des vulnérabilités établi dans la phase 1, en utilisant la même approche par contraintes.

Des analyses-diagnostics doivent être développées. Elles porteront principalement sur les interdépendances entre les contraintes de l'organisation, les utilisations des TIC et les dépendances avec fournisseurs de ces technologies. La finalité est d'initier le dialogue entre le gestionnaire et le gestionnaire TI et de les soutenir dans les prises de décisions stratégiques.

L'approche par contrainte développée par le CRP a permis de proposer une nouvelle démarche de découpage de l'organisation qui a été utilisée pour élaborer un premier portrait des vulnérabilités liées aux utilisations des TIC. Ce contexte de recherche permet de poser la question de recherche suivante :

Comment peut-on amener un gestionnaire à analyser les vulnérabilités liées aux utilisations des TIC dans son organisation ?

3.3 Objectifs de recherche et résultats attendus

3.3.1 Objectifs généraux

Les deux objectifs généraux de cette recherche sont :

1) Caractériser les vulnérabilités résultant des utilisations des TIC.
2) Comprendre les dépendances avec les fournisseurs des TIC et les vulnérabilités associées à l'externalisation des TIC.

3.3.2 Objectifs spécifiques

Pour atteindre les objectifs généraux fixés au préalable, quatre objectifs spécifiques ont été déterminés :

1) Développer des analyses-diagnostics des vulnérabilités en rapport avec les utilisations des TIC.
2) Prendre en compte les stratégies de maintien, de rétablissement, de reprise et de sécurité à l'interne.
3) Prendre en compte les dépendances avec les fournisseurs des TIC.
4) Proposer un outil d'aide à la prise de décision concernant l'acquisition, le changement ou l'abandon d'une technologie.

3.3.3 Résultats attendus

Les résultats attendus de recherche peuvent être résumés en quatre points :

- Proposer un profil des vulnérabilités liées aux utilisations des TIC.
- Examiner l'état de préparation de l'organisation : les mesures de protection, les stratégies de maintien, de rétablissement, de reprise et de sécurité existantes à l'interne et celles dont la mise en œuvre est en cours.
- Caractériser les fournisseurs de TIC et les liens de dépendance.

- Proposer un outil d'analyse-diagnostic pour la prise de décision concernant l'acquisition, le changement ou l'abandon d'une technologie.

3.4 Méthodologie de recherche

La méthodologie suivie dans ce projet de recherche est la méthodologie de recherche-action. Elle consiste en une stratégie de changement planifié s'exerçant au cœur d'un processus de résolution de problèmes (Savoie-Zajc et al, 2001). En effet, la stratégie de recherche-action vise principalement à proposer une démarche de résolution des situations jugées problématiques et à apporter des réponses à des besoins exprimés de la part des organisations ou des chercheurs. La méthodologie se distingue des autres méthodologies de recherche de la façon dont elle opère : les chercheurs et les acteurs sont partenaires dans toutes les étapes de la recherche et la sollicitation de la résolution des problématiques peut être exprimée de la part des chercheurs ou des acteurs partenaires.

La problématique traitée dans le cadre de ce projet s'inscrit bien avec la méthodologie de recherche-action. En effet, le besoin exprimé de la part des PME concernant les utilisations des TIC et porté à l'attention du CRP a donné le jour au démarrage du projet qui porte sur l'étude et l'analyse des vulnérabilités liées aux utilisations des TIC.

Les projets portant sur les TIC s'inscrivent dans le cadre du projet analyses-diagnostics de la résilience des PME qui a été démarré en 2016. Ce dernier est subventionné par le Centre de recherche en sciences naturelles et en génie du Canada (CRSNG) pour trois ans. Les partenaires dans ce projet sont :

- La direction régionale de la Montérégie du MESI du Québec.
- LogiAg Inc. : Une PME offrant des services de conseils en agro environnement (plans de fertilisation, plans de drainage, etc.).
- Les Serres Lefort : une PME qui se spécialise dans la production des légumes sous les serres.
- Corflex : Une PME experte en optimisation d'espace.
- Nétur Inc. : Une PME experte en usinage de pièces aéronautiques et en solutions d'assemblage des pièces d'avion.

Les rencontres avec les gestionnaires (dirigeants) et les gestionnaires TI de ces PME ont permis de déterminer des besoins concrets chez chacun de nos partenaires et de définir les grands axes des analyses-diagnostics présentés dans le chapitre suivant.

Le processus de la méthode recherche-action suivi pour mener cette recherche est le même utilisé dans les travaux de Marty (2014), Micouleau (2016), Benon (2017) et Plamondon-Tremblay (2018). En effet, le processus de la recherche-action contient quatre phases. La première phase consiste à définir et à formuler le problème par le chercheur. La deuxième phase consiste à développer une solution au problème défini. Cette phase est effectuée par le chercheur et les gestionnaires. La troisième phase est effectuée par le chercheur qui propose une solution au problème défini. La quatrième phase consiste à valider et à tester la solution proposée par le chercheur et les gestionnaires.

Pour mieux positionner ce projet de recherche, il convient de rappeler que les travaux réalisés dans ce projet font suite aux travaux de Benon (2017) qui ont permis d'établir un portrait des vulnérabilités liées aux utilisations des TIC et de développer l'approche par contraintes. La phase 1 du processus de la recherche-action qui consiste à définir le problème a donc été réalisée par Benon (2017).

Ce mémoire couvre la phase 2 et 3. La phase 2 qui consiste à développer une solution au problème défini, a été effectuée en collaboration avec les gestionnaires et les gestionnaires TI des PME partenaires dont deux des trois gestionnaires assument à la fois le rôle du gestionnaire et le rôle du gestionnaire TI. Trois ateliers de travail ont été organisés avec les gestionnaires de trois PME partenaires pour discuter les solutions possibles. L'annexe B et l'annexe C présentent les fiches de rencontre qui ont été utilisées pour cadrer les discussions durant les ateliers de travail. La phase 3 du même processus est couverte par les résultats présentés dans ce mémoire couvrent la phase trois du processus de la méthode recherche-action. L'outil d'analyse-diagnostic proposé représente une solution au problème défini. Des travaux ultérieurs devront couvrir la phase 4 du processus pour valider et tester la solution proposée.

CHAPITRE 4 ANALYSES-DIAGNOSTICS DES VULNÉRABILITÉS LIÉES AUX UTILISATIONS DES TIC

L'analyse-diagnostic des vulnérabilités liées aux utilisations des TIC consiste à caractériser les vulnérabilités provenant des environnements interne et externe de l'organisation. La finalité de ce type d'analyse est d'identifier les forces et faiblesses de l'organisation, de la repositionner dans son environnement (technologique, économique, légale, etc.) et d'acquérir les connaissances destinées à alimenter une réflexion stratégique du gestionnaire sur les utilisations des TIC et les vulnérabilités qui les accompagnent.

En bref, les analyses-diagnostics consistent à :

1) Identifier les facteurs internes et externes susceptibles d'influencer le respect des contraintes en effectuant une analyse du positionnement en termes de vulnérabilités découlant des environnements interne et externe, des ressources en TIC et des capacités de l'organisation.
2) Permettre d'identifier si des prises de décision concernant un changement technologique récent ou futur vont faire émerger des vulnérabilités ou des opportunités pour l'organisation.

La démarche d'analyse-diagnostic des vulnérabilités liées aux utilisations des TIC qui est proposée dans ce projet vise à fournir aux gestionnaires des PME un outil d'analyse-diagnostic adapté aux particularités et aux besoins de leurs organisations. Le but est d'accompagner les gestionnaires des PME qui éprouvent des difficultés en matière de gestion des vulnérabilités technologiques et d'encourager le dialogue entre les gestionnaires et les gestionnaires de TI.

La démarche contient deux grandes étapes : la première étape vise à établir un portrait de l'organisation dans lequel les contraintes de l'organisation et les ressources en TIC utilisées pour les satisfaire sont identifiées. Le diagnostic des contraintes permet d'identifier les contraintes critiques qui ont des impacts importants sur les objectifs et la mission de l'organisation. Dans la seconde étape, les analyses-diagnostics des vulnérabilités liées aux utilisations des TIC seront réalisées.

4.1 Portrait de l'organisation

Le portrait de l'organisation est établi pour faciliter les analyses-diagnostics des vulnérabilités liées à l'utilisation des TIC. Il contient deux éléments importants pour les présents travaux de recherche : les contraintes appliquées à l'organisation et les ressources en TIC nécessaires pour les satisfaire.

1) **Les contraintes** représentent un ensemble de conditions appliquées à l'organisation par son environnement et qui peuvent avoir des impacts majeurs sur la réalisation de sa mission.
2) **Les technologies de l'information et de communication** regroupent l'ensemble des technologies qui interviennent dans la transformation, le stockage, le traitement et la diffusion des informations ; elles assemblent quatre composantes : le matériel (équipements), les logiciels, la communication (internet, télécommunication) et les systèmes de sauvegarde des données.

Avant de procéder à la caractérisation des contraintes appliquées à l'organisation et à la caractérisation des TIC utilisées, il faut noter que le portrait de l'organisation nécessite la collaboration des gestionnaires et des gestionnaires TI. Le gestionnaire (dirigeant-propriétaire) possède une vision d'ensemble est au centre de la prise de décision. Ainsi, il est pertinent d'accorder la tâche de la caractérisation des contraintes au gestionnaire et la tâche de la caractérisation des TIC au gestionnaire TI.

4.1.1 Les contraintes

Comme précisé auparavant, les contraintes ont un lien direct avec les objectifs et la mission de l'organisation. Le non-respect des contraintes peut engendrer des impacts significatifs sur l'organisation et la rendre plus vulnérable. La caractérisation des contraintes, leurs natures (criticités), leurs marges de manœuvre et leurs temporalités sont effectuées par le gestionnaire de l'organisation qui a les acquis nécessaires et la position hiérarchique adéquate. Cette caractérisation facilite la compréhension du fonctionnement de l'organisation et des sources de vulnérabilités.

4.1.1.1 Caractérisation des contraintes

Les exemples de contraintes présentées proviennent des discussions avec les gestionnaires des trois PME partenaires dans ce projet de recherche. La fiche de rencontre 1 et 2 présentée dans l'annexe B contient les éléments discutés lors des deux premiers ateliers de travail. Avant que les ateliers de

travail prennent place, la fiche présentée à l'annexe B a été communiquée aux gestionnaires pour préparer les points à discuter. Tout d'abord, il a été demandé aux gestionnaires de caractériser les contraintes auxquelles leurs organisations doivent répondre et de commencer à réfléchir aux différents outils technologiques liés aux technologies de l'information et de communication (TIC) utilisées afin de satisfaire les contraintes. L'objectif était d'amener les gestionnaires à caractériser les vulnérabilités associées à l'utilisation des systèmes technologiques.

Les résultats des deux premiers ateliers de travail ont été utilisés pour alimenter les travaux de recherche présentés dans ce mémoire.

Selon Benon (2017), les contraintes appliquées à ces organisations peuvent être regroupées dans six grandes catégories : organisationnelles, techniques, légales, contractuelles, sécuritaires, économiques. En effet :

- ***Les contraintes organisationnelles*** proviennent des règles de gestion et politiques que l'organisation a choisi d'adopter pour accomplir ses missions.
  Exemple : Contrôle de la température ou de l'humidité dans les locaux industriels.
- ***Les contraintes techniques*** relèvent du domaine technique des activités de l'organisation. Elles peuvent porter sur les spécifications techniques et les contraintes opérationnelles des équipements de l'organisation ou sur certaines étapes clés du processus industriel.
  Exemple : Effectuer des tests et des simulations sur les équipements pour assurer le maintien du fonctionnement des installations et contrôler les paramètres techniques ou de configuration d'une ligne de production.
- ***Les contraintes légales ou réglementaires*** indiquent les requis légaux, règlementaires ou normatifs que l'organisation s'engage à respecter dans le cadre de ces activités.
  Exemple : Préparer un rapport annuel en lien avec des réglementations gouvernementales sur la traçabilité de certaines activités industrielles.
- ***Les contraintes contractuelles*** proviennent d'un engagement passé entre l'organisation et ses parties prenantes (fournisseurs, clients, etc.) par le biais d'un contrat ou d'une convention reconnue et acceptée par les parties concernées.

Exemple : Les fournisseurs exigent certaines conditions dans les contrats signés avec l'organisation par exemple : l'interdiction d'apporter des modifications aux équipements ou aux systèmes fournis sans un accord préalable.

- ***Les contraintes sécuritaires*** sont liées aux mesures nécessaires pour maintenir un environnement de travail sécuritaire pour le personnel et les biens/actifs.
  Exemple : Sécurisation des systèmes industriels.

- ***Les contraintes* économiques** englobent les requis économiques que l'organisation doit gérer pour assurer sa pérennité financière.

  ***Exemple* :** La gestion des comptes courants.

4.1.1.2 La nature des contraintes

La nature des contraintes est déterminée par le gestionnaire qui a les acquis nécessaires pour estimer leurs criticités pour l'organisation. Elle est déterminée en regard de l'importance du respect des contraintes dans une période spécifique ou pas. La prise en compte de la nature des contraintes dans le portrait de l'organisation permet de prévenir les impacts potentiels sur l'organisation. On distingue deux types de contraintes :

- Une contrainte est ***nécessaire*** lorsque son respect est crucial pour le fonctionnement des processus stratégiques et/ou opérationnels de l'organisation. Le non-respect de ces contraintes entraîne des impacts importants sur les objectifs et la mission de l'organisation. Dans le cadre de ce projet, les contraintes qui ont été qualifiées « nécessaires » ont un lien direct avec les activités principales des entreprises partenaires.

  Exemple : Préparer un rapport annuel en lien avec des réglementations gouvernementales sur la traçabilité de certaines activités industrielles.

- Une contrainte est ***souhaitable*** lorsqu'elle est facultative ou optionnelle. Le non-respect de cette contrainte n'entraîne pas des impacts négatifs sur le fonctionnement de l'organisation.

  Exemple : L'organisation choisit de suivre les directives de la norme de continuité des activités en partie ou au complet sans être dans l'obligation de se certifier ou de les suivre à la ligne.

4.1.1.3 Notion de temporalité

La définition retenue de la vulnérabilité développée par le CRP met l'accent sur la notion de temporalité, d'où la pertinence de l'utilisation de ce critère pour caractériser les contraintes appliquées à l'organisation et lors des analyses-diagnostics des vulnérabilités. La notion de temporalité est déterminée par le gestionnaire et dépend notamment du fonctionnement et des modalités d'exécution des contraintes. La récurrence des contraintes dans le temps peut être continue ou calendaire (périodique) :

- ***Continue :*** est utilisée pour caractériser les contraintes qui s'appliquent à l'organisation en tout temps.
- ***Calendaire (périodique) :*** est utilisée pour les contraintes qui ne s'appliquent que dans des périodes spécifiées.

4.1.1.4 Marge de manœuvre

La marge de manœuvre représente le temps entre la prise en compte d'une perturbation et le moment où les contraintes de l'organisation commencent à être affectées significativement. Elle fait aussi référence à la durée estimée pour que le gestionnaire puisse activer le plan d'action utilisé pour minimiser les impacts de la perturbation. Le gestionnaire est capable d'estimer la marge de manœuvre en se basant entre autres sur la connaissance de l'organisation (les contraintes, leurs criticités et leurs temporalités, les TIC utilisées). Dans le contexte de ce projet, la marge de manœuvre doit prendre en compte le temps nécessaire à la reprise et au rétablissement des ressources en TIC utilisées pour satisfaire les contraintes appliquées à l'organisation. Il est important de préciser que le temps de reprise est proportionnel à la sévérité des perturbations.

Le tableau 4.1 a été conçu pour qu'un gestionnaire puisse caractériser les contraintes de son organisation. Il contient le résumé des exemples de contraintes identifiées lors des discussions avec les gestionnaires des PME partenaires. Pour la nature des contraintes, un « oui » a été utilisé pour déterminer si une contrainte est obligatoire ou souhaitable. Durant les rencontres avec les PME partenaires, la notion de temporalité s'est dégagée comme un élément important pour la caractérisation des contraintes. Il a été donc important de faire la distinction entre les contraintes appliquées en tout temps et celles qui sont calendaires. Enfin, les marges de manœuvre ont été établies par le gestionnaire qui a estimé le temps nécessaire à la reprise en cas de perturbation en

se basant sur les connaissances organisationnelles et les expériences antérieures. Des exemples de ces temporalités et marges de manœuvre sont donnés dans le tableau 4.1. Il faut préciser que les exemples présentés sont dérivés des ateliers de travail qui ont eu lieu avec les gestionnaires et l'équipe de recherche du CRP.

Tableau 4.1 : Exemples de contraintes appliquées à une organisation, leurs natures, leurs temporalités et marges de manœuvre.

Catégorie de contraintes	**Exemples de contraintes**	**Nature des contraintes**		**Temporalité des contraintes**		**Marge de manœuvre**
		Obligatoire	**Souhaitable**	**Continue**	**Calendaire**	
Techniques	Tests des installations et contrôle des paramètres d'une ligne de production.		Oui		Chaque 3 mois	4 à 5 jours
Organisationnelles	Contrôle de la température ou de l'humidité dans les locaux industriels.	Oui		Tout le temps		48 heures
Contractuelles	Clauses de contrat avec les fournisseurs.	Oui			Période spécifique	2 jours
Légales	Rapport annuel au gouvernement.	Oui			2 à 3 mois par année	1 jour
Économiques	La gestion des comptes courants	Oui		Tout le temps		6 jours
Sécuritaires	Sécurisation des systèmes industriels.		Oui	Tout le temps		8 heures

Le tableau 4.1 constitue la première étape dans la réalisation du portrait de l'organisation dans la mesure où il permet de dresser un portrait des contraintes auxquelles l'organisation doit répondre. L'identification de la nature des contraintes par les gestionnaires a permis de soulever les contraintes critiques au fonctionnement de leurs organisations. Pareillement, l'identification de la temporalité des contraintes et les marges de manœuvre associées permet de déterminer les

contraintes temporelles auxquelles l'organisation est soumise et les périodes de stress de l'organisation.

4.1.2 Les technologies de l'information et de communication

Le portrait de l'organisation couvre deux éléments principaux : les contraintes et les technologies utilisées pour les satisfaire. Après la caractérisation des contraintes auxquelles l'organisation doit répondre par le gestionnaire, il s'avère pertinent de procéder à la caractérisation des TIC utilisées et des perturbations possibles.

4.1.2.1 Caractérisation des technologies de l'information et de communication

Les TIC regroupent quatre composantes principales : le matériel, le logiciel, la communication et les données. Dans ce qui suit, une caractérisation des TIC, leurs utilisations pour satisfaire les contraintes et les perturbations possibles dues à des défaillances des TIC doivent être effectuées par le gestionnaire TI ou l'équipe du personnel technique.

- ***Le matériel*** est constitué de tout ce qui est physique. Il regroupe l'ensemble des infrastructures bureautiques, électriques, électroniques, dispositifs informatiques et périphériques qui entrent dans la constitution des TIC (Industrie Canada, 2014).

  Exemple : Les composants électroniques (carte mère, processeur, etc.), les équipements audio et vidéo, le matériel informatique (serveurs, PC et périphériques, équipements de transmission de données) et les équipements de télécommunication (équipement de réseaux, commutateur, routeur, etc.).

- ***Le logiciel*** fait allusion à l'ensemble des applications informatiques qui contiennent des instructions permettant de faire le traitement, la diffusion et le stockage de l'information.

  Exemple : Les logiciels de base (Microsoft Office), les logiciels de gestion (programme de gestion de production), les logiciels de simulation et de modélisation, les applications web, etc.

- ***La communication*** permet l'envoi et l'échange des informations entre les différents appareils informatiques à l'interne et à l'externe grâce au réseau.

  Exemple : Service de télécommunication, service de transmissions des données par un réseau internet ou réseau sans fil, fibre optique pour la connexion haut débit, etc**.**

- ***Les données*** sont définies comme l'ensemble des indications enregistrées en machine pour permettre l'analyse et la recherche automatique des informations.

  Exemple : Les données stockées dans les banques de données, dans les serveurs (interne ou infonuagique).

4.1.2.2 Caractérisation des perturbations possibles

Les perturbations associées à l'utilisation des TIC sont dues à l'apparition d'une défaillance d'une ou de plusieurs composantes technologiques. Dans la norme ISO 27001(2013) qui expose les exigences en matière du management de la sécurité des systèmes d'information, trois critères de classification de l'information ont été utilisés : la disponibilité, l'intégrité et la confidentialité. Ces mêmes trois critères vont être utilisés pour caractériser les perturbations touchant les systèmes technologiques et impactant les contraintes de l'organisation.

- ***La disponibilité*** est une notion qui renvoie à la propriété d'être accessible et utilisable sur demande par une entité autorisée (ISO 27000, 2016). La disponibilité s'applique aux quatre composantes principales des TIC. Pour les contraintes qui font appel à l'utilisation des TIC, l'accès à ces systèmes technologiques dans un délai acceptable est important et l'impossibilité d'utiliser ces systèmes peut engendrer des impacts majeurs.

- **L'intégrité** concerne plutôt trois composantes de TIC, soit les données, les logiciels et la communication. La pertinence et la précision des données communiquées et les logiciels utilisés pour les produire sont très importants pour le fonctionnement de l'organisation. Dans l'ISO 27000 (2016), l'intégrité est considérée comme le principe permettant la sauvegarde de l'exactitude et de l'exhaustivité des données et de la façon dont il est traité.

- **La confidentialité** concerne deux composantes de TIC : la communication et les données. L'intérêt de considérer ce critère consiste dans le fait que les données stockées dans les serveurs peuvent nécessiter un certain niveau de confidentialité par exemple : les informations professionnelles (liées au secret industriel par exemple) ou personnelles des employés. Dans la norme ISO 27001 (2016), la confidentialité est considérée comme étant une condition permettant à ce que les données ne soient pas divulguées ou communiquées à des personnes ou entités qui ne possèdent pas les autorisations appropriées.

Le tableau 4.2 représente un récapitulatif des quatre composantes principales de TIC avec une caractérisation des perturbations possibles. Il est constaté que pour le matériel, la disponibilité des équipements et infrastructures bureautiques est cruciale. Pour le logiciel, en plus de la disponibilité du logiciel, il faut qu'il soit intègre vu qu'il permet la manipulation des données. Pour la communication et les données, la disponibilité, l'intégrité et la confidentialité sont très importantes. Des perturbations interfèrent la disponibilité, l'intégrité ou la confidentialité des TIC pouvant entraîner la non-satisfaction des contraintes de l'organisation. Un oui ou non sont utilisés pour indiquer si les composantes de TIC sont concernées par les perturbations possibles ou pas.

Tableau 4.2 : Récapitulatif des quatre composantes de TIC et des perturbations possibles

Composantes de TIC	**Perturbations possibles**		
	Disponibilité	**Intégrité**	**Confidentialité**
Matériel	Oui	Non	Non
Logiciel	Oui	Oui	Non
Communication	Oui	Oui	Oui
Donnée	Oui	Oui	Oui

4.1.3 Exemple d'un portrait d'une organisation de type PME

Les informations retenues lors des discussions avec les gestionnaires des PME partenaires ont permis d'établir un exemple de portrait d'une PME.

Premièrement, un inventaire des contraintes appliquées à la PME et les ressources en TIC utilisées pour les satisfaire a été établi. Pour chacune des contraintes, les gestionnaires nous ont spécifié la nature des contraintes (basées sur l'estimation de leur importance), leurs temporalités et les outils technologiques nécessaires pour les satisfaire.

Deuxièmement, les outils technologiques utilisés pour satisfaire les contraintes et les types de perturbations possibles sont identifiés par le gestionnaire TI. Pour éviter l'encombrement du portrait, il a été préférable d'indiquer la seule composante de TIC considérée comme la plus critique pour chaque outil technologique utilisé, soit le matériel, le logiciel, la communication ou les données. Il est alors possible de caractériser les perturbations possibles provenant des défaillances techniques.

Donc l'élaboration d'un portrait de l'organisation nécessite la collaboration entre le gestionnaire et le gestionnaire TI. Le tableau 4.3 présente un portrait d'une PME et est le résultat du croisement du tableau 4.1 et du tableau 4.2.

Globalement, le tableau 4.3 est constitué de cinq blocs :

- L'inventaire des contraintes : en utilisant l'approche par contrainte développée par le CRP, l'organisation est découpée en six grandes catégories de contraintes. Dans ce bloc, il est nécessaire que le gestionnaire (dirigeant de l'organisation) puisse identifier l'ensemble des contraintes appliquées à l'organisation et de les classer par catégories. L'inventaire des contraintes a été établi durant les trois ateliers de travail.
- L'estimation de l'importance des contraintes permet de déterminer la nature des contraintes selon leurs criticités pour l'atteinte des objectifs de l'organisation. L'importance des contraintes a été déterminée par les gestionnaires des PME. Aucune échelle qualitative ou quantitative n'a été utilisée pour faire cette estimation. Comme précisé, auparavant, les contraintes nécessaires sont les contraintes qui sont en lien direct avec la mission de l'organisation ou les contraintes qui peuvent générer des impacts inacceptables sur l'organisation si elles ne sont pas satisfaites. Dans le cas échéant, les contraintes sont considérées comme souhaitables.
- Les modalités de fonctionnement ou d'exécution des contraintes dépendent de la notion temporelle. Les contraintes qui sont présentes tout le temps sont qualifiées de « continues » et les contraintes qui s'imposent dans des périodes spécifiques sont qualifiées de « calendaires ». La temporalité des contraintes est déterminée par le gestionnaire.
- La dépendance à l'utilisation des TIC est déterminée à l'aide du gestionnaire TI et du personnel technique. Dans ce bloc, les outils technologiques utilisés pour satisfaire chacune des contraintes sont précisés. Ensuite, il est demandé au gestionnaire TI et au personnel de préciser la composante la plus importante de TIC. Pour déterminer la composante critique du TIC, le gestionnaire TI ou le personnel technique sont mieux qualifiés (expertises techniques) pour remplir ce bloc du tableau. Un signe « X » est accordé dans la case correspondante et dans la colonne (matériel, logiciel, communication ou donnée) pour indiquer la composante critique.
- Les perturbations possibles : comme précisé, précédemment, dans la section qui porte sur la caractérisation des perturbations possibles, les perturbations sont dues à des défaillances techniques d'une ou de plusieurs composantes de TIC qui viennent défaillir la disponibilité,

l'intégrité ou la confidentialité des TIC et, en conséquence, préviennent la satisfaction des contraintes. Cette partie est effectuée par le gestionnaire TI. En se basant sur les connaissances techniques. Un signe « X » est utilisé à chaque fois pour indiquer les perturbations possibles.

Encore une fois, un portrait de l'organisation est établi en se basant sur les acquis du gestionnaire, et ceux du gestionnaire TI et/ou personnel technique. Dans le contexte de ce projet, la fiche présentée dans l'annexe B a servi comme guide pour collecter les informations nécessaires pour établir le portrait de l'organisation.

Le portrait de la PME illustré dans le tableau 4.3 contient l'ensemble des contraintes qui ont été identifiées lors des ateliers de travail avec les trois PME partenaires. L'utilisation de toutes les contraintes identifiées est simplement pour monter un exemple illustrant plusieurs contraintes et pour garder l'anonymat des informations collectées.

Pour éviter l'encombrement du texte, deux exemples explicatifs seront présentés. Prenons l'exemple du contrôle de la température qui appartient à la catégorie de contraintes organisationnelles. Cette contrainte est cruciale pour une des PME partenaires et est présente en tout temps est donc elle nécessaire et continue. Le contrôle de la température ou de l'humidité dans les locaux industriels se fait par un logiciel spécialisé qui régularise la température selon le besoin et donc la composante la plus critique de l'outil technologique utilisé est le logiciel qui doit être intègre et disponible 24 heures sur 7 jours.

Un autre exemple est la gestion des comptes courants qui est une contrainte contractuelle et économique. Chez une des PME partenaires, la gestion des comptes courants représente la contrainte la plus critique vu que le fonctionnement de cette organisation dépend des ressources économiques récupérées lors de la gestion des comptes courants pour s'approvisionner de la matière première qui est l'aluminium. L'outil technologique utilisée est un ERP. La donnée est identifiée comme la composante des TIC qui est la plus critique et donc leur disponibilité, intégrité et confidentialité sont indispensables.

Tableau 4.3: Exemple d'un portrait d'une PME.

1. Inventaire des contraintes de l'organisation		2. Estimation de l'importance de ces contraintes		3. Modalité de fonctionnement des contraintes		4. Dépendances à l'utilisation des TIC					5. Perturbations possibles		
Catégories / Exemples de contraintes		**Nature des contraintes**		**Notion de temporalité**		**Outils technologiques utilisés**	**Les composantes des TIC**				**Type de défaillance**		
		Nécessaire	**Souhaitable**	**Continue**	**Calendaire**		**Matériel**	**Logiciel**	**Com**	**Donnée**	**D**	**I**	**C**
Techniques	Tests des installations et contrôle des paramètres d'une ligne de production		Oui		Chaque 3 mois	SCADA	X	X			X	X	
Organisationnelles	Contrôle de la température ou de l'humidité dans les locaux industriels.	Oui		Tout le temps		Logiciel spécialisé		X			X	X	
Contractuelles	Gestion des contrats avec les fournisseurs	Oui			Période spécifique	Ms office			X	X	X	X	X
Légales	Rapport annuel au gouvernement	Oui			2 à 3 mois par année	Logiciel spécialisé			X	X	X	X	X
Économiques	Gestion des comptes courants	Oui		Tout le temps		ERP		X			X	X	
Sécuritaires	Sécurisation des systèmes industriels	Oui		Tout le temps		Logiciel spécialisé		X			X	X	
----	----	----	----	----	----	----	----	----	----	----	--	--	--

Les abréviations utilisées dans le tableau 4.3 sont respectivement :

- **Com :** Communication.
- **D** : Disponibilité.
- **I** : Intégrité.
- **C** : Confidentialité**.**
- **SCADA** : système d'acquisition et de gestion des données.
- **ERP** : Entreprise ressource planning.

Le portrait de l'organisation doit permettre au gestionnaire de mieux connaître son organisation et de s'approcher des aspects techniques des TIC. La collaboration entre le gestionnaire et le gestionnaire TI doit permettre la fin du travail en silo et d'avoir une meilleure compréhension des défis que chacun des gestionnaires essaie de relever de son côté.

4.2 Analyses-diagnostics des vulnérabilités liées aux utilisations des TIC

« Les analyses-diagnostics consistent à caractériser les environnements interne et externe d'une organisation pour en identifier ses forces, ses faiblesses, ses opportunités et ses menaces » (Mercator, 2014). Dans le contexte de ce projet, les analyses- diagnostics des vulnérabilités liées aux utilisations des TIC vont permettre d'identifier et d'analyser les vulnérabilités provenant de l'environnement interne et les vulnérabilités provenant de l'environnement externe.

1) Effectuer une analyse-diagnostic des vulnérabilités internes :
   - Vulnérabilités résultantes des interdépendances entre les systèmes technologiques et les contraintes de l'organisation.
   - Vulnérabilités en lien avec l'état de préparation de l'organisation
2) Effectuer une analyse-diagnostic des vulnérabilités externes : Vulnérabilités résultantes des dépendances avec les fournisseurs des TIC.

4.2.1 Profil des vulnérabilités internes

Le portrait de l'organisation établi au préalable (tableau 4.3) permet de déterminer la correspondance entre les contraintes de l'organisation et les applications et systèmes informatiques

utilisés pour les satisfaire. Les TIC utilisées pour assurer le respect des contraintes sont considérées comme des sources de vulnérabilités. En effet, les interdépendances entre les systèmes technologiques et les contraintes de l'organisation impliquent que l'indisponibilité des TIC affecte directement les contraintes organisationnelles et temporelles (marge de manœuvre, délai de livraison, etc.) et oblige le recours à des procédures manuelles pour satisfaire les contraintes.

Le tableau 4.4 présente un exemple d'un profil de vulnérabilité tiré de la compilation du portrait de l'organisation présenté dans le tableau 4.3. Les vulnérabilités découlant de l'environnement interne prennent en compte les contraintes de l'organisation, les utilisations des TIC et les perturbations possibles. Les mêmes exemples de contraintes utilisés dans les tableaux précédents ont été maintenus.

Les vulnérabilités sont déterminées à partir des contraintes appliquées à l'organisation et les liens de dépendance aux utilisations des TIC. L'identification des outils technologiques utilisés pour satisfaire chacune des contraintes, les composantes critiques de ces outils ainsi que les perturbations possibles vont permettre de déterminer les éléments de TIC les plus vulnérables et de générer une prise en conscience chez le gestionnaire et le gestionnaire TI des vulnérabilités internes à l'organisation.

Reprenons l'exemple du contrôle de la température ou de l'humidité dans les locaux industriels et de la gestion des comptes courants encore une fois.

Pour le contrôle de la température ou de l'humidité dans les locaux industriels, l'organisation utilise un logiciel spécialisé pour régulariser la température ou l'humidité selon le besoin. L'organisation est vulnérable face à l'utilisation de ce logiciel spécialisé. Une défaillance entraînant l'indisponibilité du logiciel ou un problème d'intégrité oblige l'organisation à fonctionner en mode manuel et éventuellement un arrêt de fonctionnement après 48 heures.

Pour la gestion des comptes courants l'utilisation d'un ERP pour collecter les données nécessaires à la gestion des comptes courants rend l'organisation vulnérable aux pertes de données stockées sur les serveurs et aux contraintes temporelles propres à la contrainte. L'ERP est susceptible de subir des défaillances qui pourraient défaillir la disponibilité, l'intégrité ou la confidentialité des données utilisées pour gérer les comptes courants. Le manque de liquidité (ressources financières) résultant du retard de la gestion des comptes courants pourra affecter l'approvisionnement de la matière première, ralentir la production et portera atteinte aux objectifs de l'organisation.

Tableau 4.4 : Exemple d'un profil des vulnérabilités à l'interne

Vulnérabilités provenant de l'environnement interne				
Catégorie de contraintes	**Exemples de contraintes**	**Utilisation des TIC**		
		Outils technologiques utilisés	**Composante critique de TIC**	**Perturbations possibles**
Techniques	Tests des installations et contrôle des paramètres d'une ligne de production.	SCADA	Équipements + logiciel	Disponibilité Intégrité
Organisationnelles	Contrôle de la température ou de l'humidité dans les locaux industriels	Logiciel spécialisé	Logiciel	Disponibilité Intégrité
Contractuelles	Clauses de contrat avec les fournisseurs.	Ms office	Donnée + Communication	Disponibilité Intégrité Confidentialité
Légales	Rapport annuel au gouvernement.	Logiciel spécialisé	Donnée	Disponibilité Intégrité Confidentialité
Économiques	Gestion des comptes courants.	ERP	Logiciel	Disponibilité Intégrité
Sécuritaires	Sécurisation des systèmes industriels.	Logiciel spécialisé	Logiciel	Disponibilité Intégrité Confidentialité

4.2.2 Analyse du profil de vulnérabilités internes

Dans le contexte des interdépendances entre les systèmes technologiques et les contraintes organisationnelles et temporelles (marge de manœuvre) de l'organisation, la gestion des vulnérabilités technologiques devient plus complexe pour le gestionnaire. Prenons les exemples présentés dans le profil de vulnérabilité. Les contraintes techniques appliquées à une PME sont : les tests techniques des installations et le contrôle des paramètres de configuration de la ligne de production.

Les éléments les plus critiques des TIC pour ces types de contraintes sont : les équipements et les logiciels spécialisés. Dans de nombreux cas, les mises à jour des logiciels ne pourraient être faites que pendant les phases de maintenance des équipements et, parfois, leur application peut entraîner la nécessité de reconfigurer les paramètres de la ligne de production. Pour les tests techniques des installations, l'utilisation d'un logiciel de simulation est nécessaire pour effectuer les tests et vérifier l'état de fonctionnement des installations. Dans ce cas, la priorité est donnée à l'intégrité et à la disponibilité des installations et des logiciels utilisés dans les tests de simulation et le contrôle de la ligne de production.

L'exposition des équipements ou des logiciels qui soutiennent les activités critiques à des défaillances techniques deviennent une source de vulnérabilité pour l'ensemble de l'organisation. En effet, une indisponibilité des équipements ou du logiciel de simulation augmente la vulnérabilité de l'organisation et empêche le respect des contraintes techniques. Pareil pour l'intégrité des logiciels utilisés dans les tests de simulation ou dans la configuration des paramètres d'une ligne de production. Parmi les vulnérabilités découlant des problèmes d'intégrité des systèmes technologiques, on a : 1) Les mises à jour automatiques des logiciels peuvent incompatibles avec les anciennes installations. 2) L'utilisation d'un logiciel non intègre augmente le risque d'avoir des résultats erronés voire même l'arrêt du fonctionnement de la ligne de production.

Pour les contraintes qui nécessitent les données et les enregistrements critiques. Maintenir l'intégrité, la disponibilité et la confidentialité des données stockées dans les serveurs ou en ligne et des systèmes de traitement de ces données est crucial. La sauvegarde des documents technologiques doit être faite et testée régulièrement. Dans les PME, les sauvegardes sont souvent partielles ou disponibles chez le fournisseur et lorsque des sauvegardes existent, le bon fonctionnement des procédures de restauration en cas d'incident est rarement testé.

En résumé, la caractérisation des vulnérabilités provenant de l'environnement interne permet d'identifier les points les vulnérables de l'organisation. L'analyse diagnostic des vulnérabilités identifiées permet d'amener le gestionnaire à une réflexion sur comment il peut améliorer la pertinence des mesures mises en place pour assurer la veille sur les vulnérabilités technologiques, d'adapter les mesures de protection aux besoins de l'organisation et d'appréhender les vulnérabilités internes provenant des utilisations des TIC.

4.2.3 Analyse-diagnostic de l'état de préparation

La vulnérabilité d'une organisation dépend de son état de préparation à faire face aux menaces qui exploitent les maillons faibles des infrastructures technologiques pour déclencher des perturbations et par conséquent, générer le non-respect des contraintes. En effet, l'utilisation des TIC pour satisfaire les contraintes accroît la vulnérabilité des organisations principalement les PME. C'est pourquoi le gestionnaire d'une PME doit plus que jamais adopter des stratégies proactives pour préparer l'organisation à faire face aux vulnérabilités provenant des utilisations des TIC.

4.2.3.1 État de préparation de l'organisation

La préparation est considérée comme une étape au cours de laquelle les décisions sont prises concernant les choix des stratégies de maintien, de reprise, de rétablissement et de sécurité à mettre en place. Le gestionnaire qui prend les décisions concernant ce sujet est amené à collaborer avec le gestionnaire TI ou le personnel technique pour identifier les stratégies les plus appropriées aux besoins de l'organisation. Les buts de la préparation sont :

1) Renforcer la capacité (plans, procédures, ressources et mesures alternatives) de l'organisation à faire face à des perturbations découlant des défaillances des systèmes technologiques et appréhender les vulnérabilités internes qui accompagnent les utilisations des TIC.
2) Développer une capacité à l'interne en se fondant sur les priorités de l'organisation, l'analyse des besoins en matière de maintien, de reprise et de rétablissement des systèmes technologiques utilisés et les exigences en matière de sécurité.
3) Intégrer les dépendances avec les fournisseurs des TIC dans les mesures de planification (plan de relève informatique, plan de continuité d'activité, marge de manœuvre, etc.).

4.2.3.2 La prise de décision concernant les choix des stratégies

Dans les PME, la prise de décision concernant les choix des stratégies à adopter à l'interne est habituellement effectuée par le gestionnaire. En développant des stratégies à l'interne, le gestionnaire travaille en collaboration avec le gestionnaire TI ou le personnel technique pour chercher à identifier et à maîtriser les principales sources de vulnérabilités résultantes des environnements interne et externe.

À la suite des ateliers de travail avec les gestionnaires et les gestionnaires TI des partenaires, nous avons identifié quatre catégories de stratégies qui pourraient les amener à mieux anticiper les vulnérabilités qui accompagnent l'utilisation des TIC et à réagir en conséquence afin d'assurer le maintien, la sécurité, la reprise et le rétablissement des activités lors d'une perturbation.

Les stratégies que le gestionnaire peut adopter pour consolider l'état de préparation de son organisation sont :

- **La stratégie de sécurité**

Elle correspond à l'ensemble des règles de sécurité que l'on désire mettre en place dans une organisation, ainsi que le niveau de celle-ci. Elle peut contenir des stratégies de gestion des connexions et de gestion des identifications aux comptes utilisateurs (contrôle des mots de passe).

Exemples :

- Accès sécurisé à l'interne (délégation de droits sur les systèmes et les données).
- Accès externe par VPN.

- **La stratégie de maintien**

Elle englobe l'ensemble des mesures, des procédures et des ressources visant le maintien et la protection des actifs en TIC utilisées pour satisfaire les contraintes de l'organisation. Cette stratégie vise à anticiper les défaillances des TIC et à mettre en place des actions pour maintenir un niveau de fonctionnement acceptable.

Exemples :

- Redondance des équipements (serveurs, router, commutateur, stockage, pare-feu).
- Réplication des serveurs.
- Diversification des outils technologiques utilisés.

- **La stratégie de rétablissement**

Elle permet d'adapter l'ensemble des mesures et procédures planifiées à l'avance pour assurer le retour à un état de fonctionnement acceptable le plus vite possible lors d'une perturbation. Cette stratégie nécessite la disponibilité des moyens et des ressources pour se rétablir. À la différence de la stratégie de maintien, la stratégie de rétablissement nécessite généralement une plus grande part

d'adaptation puisque la mise en place des mesures planifiées ne couvre pas toutes les situations de perturbation.

Exemples :

- Stratégie de sauvegarde des données**.**
- Planification des mesures alternatives (faire appel à un fournisseur de support technique ou autres).

- **La stratégie de reprise**

Elle consiste à mettre en place un plan de relève informatique qui permettra de gérer les perturbations qui peuvent produire un arrêt du fonctionnement des TIC et un plan de reprise ou de continuité d'activité qui permet d'assurer la reprise des activités et le respect des contraintes de l'organisation.

Exemples :

- Un plan de sauvegarde des données sensibles devrait être mis en place afin de pouvoir restaurer les systèmes en cas de perte ou de destruction.
- Acquisition d'un régulateur de tension UPS qui assure une autonomie de 15 à 20 min.

Pour faire le diagnostic de l'état de préparation de l'organisation, le gestionnaire est amené à remplir le tableau 4.5, les exemples cités donnent une idée sur les ressources et les mesures de protection que l'organisation doit mettre en place pour appréhender les vulnérabilités.

Le tableau 4.5 présente un récapitulatif des stratégies qu'un gestionnaire peut adopter pour consolider l'état de préparation dans son organisation. Les exemples présentés dans le tableau 4.5 sont issus des discussions avec les gestionnaires des PME partenaires dans ce projet de recherche.

Tableau 4.5 : Exemple récapitulatif des stratégies mises en place pour renforcer l'état de préparation de l'organisation

État de préparation de l'organisation			
Stratégie de Maintien à l'interne	**Stratégie de Rétablissement à l'interne**	**Stratégie de Reprise à l'interne**	**Stratégie de Sécurité à l'interne**
- Redondance des équipements (serveurs, router, commutateur, stockage, pare-feu) - Réplication des serveurs.	- Stratégie de sauvegarde des données.	- Plan de sauvegarde des données sensibles. - Acquisition d'un régulateur de tension UPS qui assure une autonomie de 15 à 20 min.	- Accès sécurisé à l'interne (délégation de droits sur les systèmes et les données). - Accès externe par VPN.

Dans cette phase de l'analyse-diagnostic, il convient d'examiner les stratégies à l'interne et de voir à quel point elles sont efficaces. Permettent-elles d'assurer le respect des contraintes de l'organisation ? Faut-il adopter d'autres stratégies pour maintenir un niveau de fonctionnement acceptable en cas de perturbations ? Est-ce qu'il y a d'autres mesures de protection qu'on peut mettre en place pour réduire les vulnérabilités associées aux utilisations des TIC ?

Le profil de vulnérabilité et le portrait de l'état de préparation permettent au gestionnaire d'établir un ordre de priorité pour les stratégies futures à adopter. De dégager les forces et les faiblesses des mesures de protection à l'interne et d'examiner la cohérence entre les stratégies et les mesures de protection à l'interne avec les besoins en matière de gestion des vulnérabilités technologiques.

4.2.4 Analyse-diagnostic des vulnérabilités externes

La complexité des problèmes techniques et les vulnérabilités associées aux utilisations des TIC incitent souvent le gestionnaire d'une PME à opter pour l'externalisation de ces services. Le transfert d'une ou de plusieurs fonctions technologiques vers un fournisseur externe ou un prestataire de service est considéré comme une démarche profitable et une option qui allège le fardeau de la gestion et de la maintenance des ressources en TIC. Cependant, lorsque les technologies proviennent d'un ou de plusieurs fournisseurs externes, il est nécessaire de faire des choix judicieux, car les vulnérabilités résultantes des dépendances avec les fournisseurs externes

ne sont plus contrôlées. Dans les contrats signés entre une PME et ses fournisseurs, elle délègue la responsabilité de la gestion des risques par l'intermédiaire des clauses spécifiques souvent nommées « clauses de transfert des risques ». Dans ce cas, l'organisation accepte le fait qu'elle a créé de nouvelles vulnérabilités provenant de l'environnement externe (fournisseurs).

4.2.4.1 Caractérisation des fournisseurs

Les fournisseurs sont caractérisés par les services qu'ils fournissent. Une organisation peut avoir plusieurs fournisseurs de services ou un seul fournisseur qui fournit plus qu'un service. Les types de fournisseurs de services que nous avons pu identifier lors du troisième atelier de travail avec les partenaires sont :

- Le fournisseur du service du matériel est celui qui se charge de la fabrication et/ou la distribution des dispositifs informatiques, électroniques, électriques et des infrastructures bureautiques comme les ordinateurs, imprimante, scanner, etc.
- Le fournisseur du service du logiciel est celui qui assure la conception, le développement, la maintenance et la commercialisation des produits logiciels comme les logiciels spécialisés, le progiciel de gestion des ressources de l'entreprise ERP, les applications web, etc.
- Le fournisseur du service de communication propose à ses clients des services qui répondent à leurs besoins en matière de communication. Ceci, inclus les services de connectivité et des équipements de réseau (internet, télécommunication, réseau sans fil, fibre optique, etc.).
- Le fournisseur du service des systèmes de sauvegarde des données est celui qui offre des services d'hébergement et de sauvegarde des données en ligne ou dans les serveurs.
- Le fournisseur du service du support technique est celui qui fournit de l'assistance et le support pour des problèmes techniques touchant le matériel, le logiciel, la communication et les systèmes de sauvegarde.

Après la caractérisation des fournisseurs du service de TIC, un inventaire de ces fournisseurs est établi à l'aide du gestionnaire TI.

Le tableau 4.6 permettant de caractériser les fournisseurs de TIC est tiré du tableau 4.3 qui représente le portrait de l'organisation. Pour chaque composante de TIC, l'organisation fait appel

à un ou plusieurs fournisseurs du service de TIC (matériel, logiciel, communication et donnée). Bien évidemment, un ou plusieurs fournisseurs du service de support techniques sont à considérer.

Le tableau 4.6 doit permettre de caractériser les fournisseurs du service de TIC. Il contient trois colonnes. La première colonne regroupe tous les fournisseurs de service que nous avons identifiés précédemment. La deuxième colonne présentes des exemples explicatifs pour diriger le choix des fournisseurs des technologies. La troisième colonne est utilisée pour préciser si l'organisation fait appel aux services d'un fournisseur en répondant par « oui ou non ? » et ensuite le nommer en répondant à la question « nommez-les ? ».

Tableau 4.6 : Caractérisation des fournisseurs possibles des TIC

Caractérisation des fournisseurs de service	**Exemples explicatifs**	**Identification des fournisseurs**
Fournisseurs du service du matériel	Les dispositifs informatiques et les équipements	- Oui/ non ? - Nommez-les
	Infrastructures bureautiques	
Fournisseurs du service du logiciel	- Logiciel spécialisé. SCADA : Systèmes d'acquisition et de contrôle des données. - ERP	- Oui/ non ? - Nommez-les
	Applications web : site web, commerce en ligne	
Fournisseurs du service des systèmes de la communication	Réseau Internet, sans fil	- Oui/ non ? - Nommez-les
	Fibre optique	
	Service téléphonique	
Fournisseurs du service des systèmes de sauvegarde des données	Cloud	- Oui/ non ? - Nommez-les
	Serveur	
Fournisseurs du service du support technique	Support technique des équipements	- Oui/ non ? - Nommez-les
	Support technique d'un ou de plusieurs logiciels	
	Support technique pour les systèmes de sauvegarde	

Le remplissage du tableau 4.6 par le gestionnaire va permettre de déterminer le nombre de fournisseurs auxquels l'organisation est dépendante et de voir s'il y a un ou plusieurs fournisseurs

qui proposent plus qu'un service. La prise en compte des dépendances avec les fournisseurs du service de TIC dans la caractérisation des vulnérabilités liées aux utilisations des TIC fait partie des objectifs spécifiques à ce projet de recherche. La caractérisation et l'identification des fournisseurs de services de TIC doivent permettre aux gestionnaires de remettre en cause les prises de décision concernant le choix de ces fournisseurs et le choix des stratégies mises en place à l'interne. L'analyse du contenu du tableau 4.6 permet de déterminer les fournisseurs susceptibles à affecter la mission de l'organisation (matériel, logiciel, support, etc.). Plus l'organisation est dépendante à un seul fournisseur plus elle devient vulnérable.

La finalité est d'amener le gestionnaire et le gestionnaire TI à comprendre les vulnérabilités provenant des dépendances avec ses fournisseurs et de se questionner sur la capacité de l'organisation à limiter les sources de vulnérabilité provenant de l'environnement externe et la capacité de fonctionner si le fournisseur n'arrive pas à lui offrir le service attendu.

4.2.4.2 Quels sont les critères de choix des fournisseurs des TIC ?

La prise de décision concernant la sélection d'un fournisseur est une décision stratégique qui a un impact important sur la mission de l'organisation et ses objectifs. Cette décision vise à créer et à maintenir un réseau de fournisseurs des TIC fiable et efficace. Les capacités du fournisseur à fournir un service ou produit de qualité avec un coût concurrentiel ne sont plus les seuls critères déterminants pour sélectionner un fournisseur.

Lors des discussions avec les gestionnaires des PME partenaires dans ce projet, il a été conclu que la similarité des offres sur le marché du rapport coût/qualité n'est pas le critère le plus déterminant. À part les critères du coût et de la qualité, les gestionnaires se basent sur d'autres critères pour déterminer les fournisseurs les plus appropriés aux besoins de son organisation. La fiche de rencontre présentée dans l'annexe C nous a permis de guider les discussions sur les critères de choix des fournisseurs des TIC.

Les trois critères retenus lors des ateliers de travail avec les gestionnaires des PME sont :

1) **Le temps de réponse** est un critère utilisé pour mesurer la performance du fournisseur. Il représente le temps entre l'émission de la demande et la réalisation de l'action demandée. Le fournisseur promet d'offrir le soutien nécessaire rapidement à l'issue de la requête de son client. Le temps de résolution du problème est d'habitude basé sur la complexité de la requête.

2) **La disponibilité** est un critère très important dans la sélection du fournisseur du Cloud. Le fournisseur offre une disponibilité du système sur une période de temps. Par exemple, l'application ou les données vont être disponibles à 98% du temps 7 jours par semaine, 19 heures par jour.

3) **La marge de manœuvre du fournisseur** : la cohérence entre la marge de manœuvre du fournisseur et celle de l'organisation est un critère déterminant dans le choix des fournisseurs.

Exemple : un gestionnaire estime que la marge de manœuvre pour restaurer les données perdues lors d'une faille de sécurité est environ de 24 heures maximum. Si la marge de manœuvre du fournisseur du système de sauvegarde des données est incohérente avec celle de l'organisation alors il vaut mieux choisir un autre fournisseur qui répond à ce critère ou trouver un moyen d'ajuster la marge de manœuvre de l'organisation.

4.2.5 Exemples d'applications

4.2.5.1 La prise de décision concernant un changement technologique

Un changement technologique comprend l'action d'acquérir, d'abandonner ou de changer une technologie. La prise de décision concernant ce sujet doit respecter les objectifs stratégiques de l'organisation et satisfaire les contraintes de cette dernière. Au moment de la prise de décision concernant un changement technologique, la considération de ces quatre perspectives est essentielle : le changement technologique, le changement organisationnel, le changement de stratégie et le changement de fournisseurs des TIC. Ceci veut dire qu'une telle décision requiert une perception des changements organisationnel et technique qui accompagneront le changement, l'acquisition ou l'abandon d'une technologie et les vulnérabilités éventuelles.

Dans la suite le tableau 4.7 est utilisé pour clarifier un peu plus les changements techniques, organisationnels, de stratégies et des liens avec les fournisseurs lors d'un changement technologique.

- La première colonne doit permettre d'indiquer la technologie à abandonner, à changer ou à acquérir et la composante de TIC la plus critique que le gestionnaire ou le gestionnaire TI prévoit de changer. Les éléments indiqués dans cette colonne sont tirés du tableau 4.4.
- La deuxième colonne doit faire apparaître les changements organisationnels dus à un changement technologique et de voir si le changement va permettre de respecter les contraintes

organisationnelles et temporelles auxquelles l'organisation doit répondre et marge de manœuvre. Les éléments indiqués dans cette colonne sont tirés du tableau 4.4.

- La troisième colonne doit permettre de contempler les stratégies déjà mises en place ou les stratégies futures. En répondant à la question suivante : quelles sont les stratégies à mettre en place pour protéger l'organisation contre les vulnérabilités qui accompagnent les changements technologiques ? Les éléments indiqués dans cette colonne sont tirés du tableau 4.5.
- La quatrième colonne doit préciser si un changement de fournisseur est nécessaire ou pas. Si oui, le gestionnaire doit considérer les termes des contrats (clauses) signés avec ses fournisseurs. Les éléments indiqués dans cette colonne sont tirés du tableau 4.6.

L'ensemble des questions posées peut être récapitulé dans le tableau suivant :

Tableau 4.7: Les changements techniques, organisationnels, de stratégies et des liens avec les fournisseurs lors d'un changement technologique

Changement technologique	**Changement organisationnel**	**Changement de stratégies**	**Changement des liens avec les fournisseurs**
- Outils technologiques concernés ? - Composante critique de TIC?	- Impacts sur le respect des contraintes ? - Respect des contraintes temporelles ? - Respect des marges de manœuvre?	Quelles sont les stratégies à mettre en place pour protéger l'organisation contre les vulnérabilités qui accompagnent les changements technologiques ?	- Changement de fournisseur à déterminer. - Clauses de contrat ?

Le tableau 4.7 doit être rempli par le gestionnaire de l'organisation et le gestionnaire de TI. La réponse aux questions rapportées dans ce type de tableau doit permettre aux gestionnaires d'avoir une vision globale sur les enjeux à considérer lors de la prise de décision concernant un changement technologique. En plus de la prise en conscience des changements technologique, organisationnels, de stratégies et des liens avec les fournisseurs par les gestionnaires, les acquis ressortis de ce tableau doivent faciliter la connaissance des vulnérabilités technologies provenant de l'environnement

interne (dépendances aux utilisations des TIC, état de préparation) et de l'environnement externe (dépendances avec les fournisseurs du service de TIC).

4.2.5.2 Exemples explicatifs

Exemple 1 : ajout des fonctionnalités à un ERP

L'ERP est un progiciel permettant la gestion de toutes les ressources et les informations/données de l'organisation et contribuant d'une manière positive au fonctionnement des organisations qui l'adopte. En ajoutant de nouvelles fonctionnalités à ce progiciel, les gestionnaires doivent prendre conscience des changements (technologiques, organisationnels, de stratégie et de fournisseurs) éventuels et des vulnérabilités technologiques résultants. En effet, les modifications des caractéristiques d'un ERP affectent directement les données produites par cette technologie et par conséquent le respect des contraintes organisationnelles et temporelles (marge de manœuvre, date buttoir, etc.).

Le portrait de vulnérabilité de la PME présenté précédemment démontre que les données représentent la composante de TIC la plus critique pour plusieurs contraintes ; légales, contractuelles et économiques. L'identification des contraintes qui pourraient être influencées par l'ajout des fonctionnalités d'un ERP doit permettre aux gestionnaires d'avoir un aperçu sur les effets d'un changement des fonctionnalités d'un ERP.

Dans la suite, il convient d'identifier les changements technique, organisationnel, de stratégie et des liens avec les fournisseurs.

L'ajout des fonctionnalités à un ERP implique un changement technologique au niveau de la manipulation des données. Il doit permettre de satisfaire des contraintes existantes ou des contraintes nouvellement appliquées à l'organisation est donc il permet de respecter les contraintes organisationnelles et temporelles ainsi que les marges de manœuvre. Le changement de stratégies touche notamment les stratégies qui ont été mises en place pour assurer la disponibilité, l'intégrité et la confidentialité des données générées par l'ERP. Le tableau 4.8 en présente des exemples comme la stratégie de sauvegarde des données qu'il faut peut-être revoir et la stratégie à mettre en place pour assurer la compatibilité équipements avec les fonctionnalités de l'ERP à changer. Enfin, pour le changement touchant les liens avec les fournisseurs des services de TIC, le fournisseur de service de TIC ne changera pas. Cependant, il faudra prévoir une négociation des termes des

contrats avec les fournisseurs du service de support technique et celui du service de sauvegarde des données.

Tableau 4.8 : Exemple explicatif des changements technologique, organisationnel, de stratégies et des liens avec les fournisseurs au cas d'un ajout de fonctionnalités à un ERP.

Changement technologique	**Changement organisationnel**	**Changement de stratégies**	**Changement des liens avec les fournisseurs**
- Ajouter des fonctionnalités à l'ERP. - Les données sont touchées par ce changement.	- Les contraintes organisationnelles et temporelles sont respectées. - Les marges de manœuvre sont aussi respectées.	- Stratégie de sauvegarde des données (back-up). - Stratégie à mettre en place pour assurer la compatibilité des équipements avec les fonctionnalités de l'ERP à changer.	- Le fournisseur du service de l'ERP ne changera pas. Cependant, le fournisseur du service du support technique et les fournisseurs du service de sauvegarde de données doivent être avisé par le changement. + Négocier les termes des contrats signés avec eux.

Exemple 2 : changement d'un logiciel spécialisé dans le contrôle de la température ou de l'humidité dans les locaux industriels

Le changement d'un logiciel spécialisé dans le contrôle de la température ou de l'humidité dans les locaux industriels peut entraîner des changements majeurs à tous les niveaux de l'organisation. Des complications sont à prévoir au niveau de la compatibilité des équipements avec les caractéristiques du nouveau logiciel acquis. Ce qui pourra porter atteinte au respect des contraintes organisationnelles et temporelles. Le respect des marges de manœuvre est à déterminer. Pour le changement touchant les stratégies de protection et de redondance des équipements et des licences de l'ancien logiciel, il faut prévoir de nouvelles stratégies à mettre en place pour assurer le maintien, le rétablissement et la sécurité du nouveau logiciel acquis. Concernant le changement des liens

avec les fournisseurs des services de TIC, le fournisseur du service du logiciel changera si l'organisation fait appel à un nouveau fournisseur. Semblablement, le fournisseur du service de support technique pourra changer s'il n'est plus en mesure de fournir le service du support technique. Le tableau 4.9 présente un récapitulatif de cet exemple.

Tableau 4.9 : Récapitulatif des changements technologique, organisationnel, de stratégies et des liens avec les fournisseurs lors d'un changement d'un logiciel spécialisé.

Changement technologique	**Changement organisationnel**	**Changement de stratégies**	**Changement des liens avec les fournisseurs**
- Changer le logiciel spécialisé qui contrôle la température ou l'humidité dans les locaux industriels. - La composante critique de TIC est le logiciel.	- Impacts sur le respect de contraintes à déterminer par le gestionnaire. - Le respect des marges de manœuvre est à déterminer.	- Changer la stratégie de redondance des équipements et des licences du logiciel. - Mettre en place une stratégie pour assurer la compatibilité des équipements avec le nouveau logiciel acquis.	- Changement du fournisseur du service du logiciel si le gestionnaire se décide sur un nouveau fournisseur. - Changer le fournisseur du service de support technique si l'ancien ne peut pas continuer à fournir ce service.

À travers les deux exemples exposés ci-dessus, les gestionnaires ont une vision globale sur les éléments touchés par une décision impliquant un changement technologique. Ils peuvent aussi prévoir les conséquences de leurs choix et les vulnérabilités technologiques éventuelles.

CHAPITRE 5 DISCUSSION & CONCLUSION

Ce chapitre présente dans un premier lieu une discussion générale dans laquelle la portée, les limites ainsi que les pistes d'améliorations futures de ces travaux de recherche seront présentées. Et dans un second lieu, une conclusion générale pour clôturer ce mémoire.

5.1 Discussion

Deux méthodes de gestion des vulnérabilités des systèmes d'information, dont MEHARI et OCTAVE-Allegro ont été présentées auparavant dans la revue de la littérature. Les points communs entre ces deux méthodes sont qu'elles ont été conçues pour les gestionnaires techniques de TI et qu'elles sont centrées sur les vulnérabilités des systèmes technologiques afin d'identifier des mesures de sécurité spécifiques.

L'avancée de cette recherche consiste dans le fait d'intégrer l'utilisation des technologies comme un moyen de satisfaire les contraintes organisationnelles et temporelles auxquelles l'organisation doit répondre. Le point central de cette recherche est la caractérisation et l'analyse des vulnérabilités internes et externes liées aux utilisations des TIC. Contrairement à la méthode MEHARI et la méthode OCTAVE-Allegro qui s'adressent aux gestionnaires de TI, la démarche proposée dans ce mémoire s'adresse aux gestionnaires des organisations de types PME souhaitant améliorer la capacité de leurs organisations à faire face aux vulnérabilités technologiques sans forcément maîtriser tous les détails techniques. À partir du portrait de l'organisation, du profil de vulnérabilités internes, de l'état de préparation et la compréhension des dépendances avec les fournisseurs des services de TIC et les vulnérabilités associées à l'externalisation des TIC, cette nouvelle approche couvre des aspects importants à considérer dans la gestion des vulnérabilités technologiques.

L'utilisation de la méthodologie de la recherche-action a permis de répondre à un besoin réel exprimé de la part des gestionnaires des PME partenaires dans ce projet de recherche. Les grands axes des analyses-diagnostics ont été déterminés lors des discussions avec les gestionnaires des trois PME partenaires. Les critères de choix des fournisseurs des services de TIC et les stratégies à mettre en place pour consolider l'état de la préparation des organisations ont été déduits des échanges avec les gestionnaires et les gestionnaires de TI que nous avons rencontrés.

5.1.1 Retour sur les objectifs

Pour ce projet de recherche, deux objectifs généraux ont été définis. Le premier objectif est de caractériser les vulnérabilités liées aux utilisations des TIC. La caractérisation des vulnérabilités a été faite à partir du portrait de l'organisation, du profil des vulnérabilités internes et du portrait de l'état de préparation face aux vulnérabilités technologiques. En effet, le portrait de l'organisation a permis d'acquérir les connaissances nécessaires à l'élaboration du profil de vulnérabilités technique et organisationnelle provenant de l'environnement interne. Le portrait de l'état de préparation a permis de mettre en regard les stratégies de protection existantes et d'encourager les gestionnaires à se questionner sur la pertinence de leurs choix de stratégies.

Le deuxième objectif était de comprendre les liens de dépendances aux fournisseurs des services de TIC et les vulnérabilités associées à l'externalisation. En effet, la prise en compte des dépendances avec les fournisseurs des services de TIC dans les analyses diagnostiques a permis de mettre la lumière sur les vulnérabilités provenant de l'environnement externe de l'organisation et de prévoir des mesures de protection alternatives pour mieux protéger ses intérêts stratégiques et respecter ses contraintes. Pour ce faire, il a été nécessaire de caractériser les fournisseurs des TIC et d'orienter les choix de ces fournisseurs en utilisant des critères plus parlants comme la disponibilité, le temps de réponse et la marge de manœuvre.

5.1.2 Les apports et les limites de cette recherche

La démarche développée propose des outils simplifiés pour équiper les gestionnaires souhaitant mener des analyses-diagnostics des vulnérabilités technologiques. Le portrait de l'organisation permet d'établir un état de connaissance de l'organisation. Le profil de vulnérabilité a fait ressortir les vulnérabilités techniques et organisationnelles. La prise en conscience de ces vulnérabilités va permettre aux gestionnaires de consolider leur état de préparation. En effet, le portrait de l'état de préparation qui expose l'ensemble des stratégies que l'organisation à adopter pour assurer le maintien, la reprise, le rétablissement et la sécurité des systèmes technologiques va permettre d'unir les efforts du gestionnaire et du gestionnaire TI dans leur quête d'appréhender les vulnérabilités technologiques. Finalement, il a été intéressant d'amener le gestionnaire d'une PME à une réflexion sur les enjeux associés aux prises de décision concernant l'acquisition, l'adoption ou le changement d'une technologie.

En ce qui concerne les limites de recherche, les travaux de recherche n'ont pas été complètement validés par les PME partenaires. Donc, il est important de les tester pour confirmer la pertinence de l'approche suivie pour amener le gestionnaire à réaliser les analyses-diagnostics proposées. Il y a aussi un manque en termes de recommandation pour mieux gérer les vulnérabilités externes provenant des dépendances avec les fournisseurs des services de TIC.

En plus, la démarche a été développée pour répondre aux besoins des organisations de type PME qui sont limitées par leur taille et leur niveau de maturité numérique ce qui fait que l'applicabilité de cette démarche convient à un contexte particulier. Néanmoins, cette démarche peut raffiner pour servir dans d'autres contextes que celui des organisations de petite et moyenne taille.

5.1.3 Perspectives de la recherche

Les analyses-diagnostics constituent un premier pas vers l'accompagnement des gestionnaires des PME dans leurs transitions vers la quatrième révolution ou l'industrie 4.0. Malgré les avantages que cette révolution industrielle apporte, il est nécessaire de penser aux limitations techniques (sécurité, interconnectivité entre les systèmes cyber-physiques) et aux changements technologiques, organisationnels et stratégiques qui les accompagnent.

La démarche développée dans ce projet peut servir comme point de départ pour évaluer la résilience ou plus précisément, la cyber-résilience des organisations face aux vulnérabilités technologiques. La cyber-résilience est en effet « la capacité à se préparer et s'adapter à des conditions en perpétuelle évolution ainsi qu'à récupérer rapidement ses capacités suite à des attaques délibérées, des accidents, des catastrophes naturelles ou encore des incidents dans le cadre de l'utilisation de moyens informatiques et de communication » (Bonneaud, 2015). Il sera intéressant de réaliser une analyse de cohérence entre les stratégies en place et les vulnérabilités ressorties lors des analyses-diagnostics et de tracer une feuille de route pour assurer l'adaptation aux changements apportés par la transformation au numérique.

Il serait intéressant d'accompagner des PME qui ont déjà un certain niveau de maturité organisationnelle pour atteindre un niveau de maturité numérique acceptable et de les préparer à devenir cyber-résilientes. Cette maturité pourra orienter les choix concernant la prise des décisions relative au changement d'une technologie et les stratégies à adopter pour renforcer l'état de la préparation de l'organisation.

5.2 Conclusion

Selon le MESI, les PME québécoises investissent entre 7% et 9% de leurs chiffres d'affaires pour intégrer les nouvelles technologies et d'avancer dans l'ère d'industrie 4.0 (MESI, 2017). Il est donc de rigueur que ces organisations s'attendent à un retour d'investissement. En profitant des avantages concurrentiels, de performance et de gains en termes de temps et de productivités, les organisations arrivent à rentabiliser leurs investissements. Toutefois, cette révolution industrielle apporte avec elle sa part de vulnérabilités et des enjeux. L'enjeu majeur est d'assurer la transition fluide et de préparer les organisations à faire face aux deux grands défis, dont l'interconnectivité entre les systèmes cyber-physiques et la sécurité de ces systèmes. En outre, les organisations qui font appel à l'utilisation des TIC arrivent à respecter plusieurs contraintes qui ont été appliquées par leurs environnements.

Ce projet de recherche a été réalisé en collaboration avec les PME de la région du Montréal dans le but d'améliorer la résilience des PME face aux utilisations des TIC. Pour ce faire, il a été convenu de commencer tout d'abord par caractériser les vulnérabilités techniques et organisationnelles et ensuite de procéder à des analyses-diagnostics.

Les vulnérabilités internes à l'organisation ont été identifiées à partir du portrait de l'organisation qui a représenté la phase d'acquisition des connaissances, du portrait de l'état de préparation. Les vulnérabilités externes ont été identifiées à partir de la mise en regard des liens de dépendance avec les fournisseurs des services de TIC.

Le projet de la résilience des PME face aux utilisations des TIC constitue un premier pas pour amener les gestionnaires à mieux appréhender les vulnérabilités technologiques et les accompagner dans les prises de décision concernant les changements de technologique et les enjeux découlant de ce changement. Des travaux futurs pourraient apporter plus de pistes de bonification et des outils organisationnels plus raffinés permettant d'évaluer les vulnérabilités technologiques et d'aider les organisations à devenir plus cyber-résilientes.

BIBLIOGRAPHIE

Autissier, D., & Delaye, V. (2008). Mesurer la performance du système d'information. Tiré de https://www.eyrolles.com/Chapitres/9782212541168/Chap3_Autissier.pdf

Benon, A. (2017). *Portrait des vulnérabilités face aux utilisations des technologies de l'information et de communication.* (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

Bonneaud, A. (2015). Cyber-sécurité vs cyber-résilience [Billet de blogue]. Tiré de http://www.ab-consulting.fr/blog/non-classe/cyber-securite-vs-cyber-resilience

Business Continuity Institute. (2013). *The BCI good practice guidelines*. United Kingdom: Business Continuity Institute.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). Introducing OCTAVE-Allegro: Improving the information security risk assessment process (Rapport no TR-012). Tiré de https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Capgemini Consulting. (2013). Impacts des nouvelles technologies de l'information et de la communication sur la qualité de vie et la santé au travail. Tiré de https://www.capgemini.com/consulting-fr/resources/ntic-sante-qualite-de-vie-au-travail/

Centre facilitant la recherche et l'innovation dans les organisations. (2011). Les usagers du Web 2.0 dans les organisations. Tiré de https://cefrio.qc.ca/media/uploader/Livre_blanc_Web2.pdf

Chandler, D., & Munday, R. (2016). *Dictionary of Media and Communication*. Oxford University Press. Tiré de http://www.oxfordreference.com/view/10.1093/acref/9780191800986.001.0001/acref-9780191800986

Club de La Sécurité de l'Information Français. (2010). MEHARI 2010: Overview. Tiré de https://clusif.fr/publications/mehari-2010-overview-2/

Courtès-Lapeyrat, C. (2010). Quand les technologies de l'information et de la communication bouleversant la communication interne de l'entreprise et deviennent un outil de gestion

des ressources humaines. Tiré de https://creg.ac-versailles.fr/quand-les-technologies-de-l-information-et-de-la-communication-bouleversent-la

Deltour, F., Farajallah, M., & Lethiais, V. (2014). L'équipement des PME en systèmes ERP : une adoption guidée par les priorités stratégiques? Management international, 18(2), 155-168. doi:10.7202/1024200ar

Deltour, F., & Lethiais, V. (2014). Innovation et performance des PME : une approche par la contribution des technologies de l'information. Tiré de http://www.strategie-aims.com/events/conferences/24-xxiiieme-conference-de-l-aims/communications/3103-innovation-et-performance-des-pme-une-approche-par-la-contribution-des-technologies-de-linformation/download

Dubé, J. (2017). *L'entreprise 4.0 et la révolution numérique au Québec* [Présentation PowerPoint]. Tiré de http://jiq.actionti.com/wp-content/uploads/2017/11/1JIQ_Conference_Jacqueline_Dube_vfinale.pdf

Elidrissi, D., & Elidrissi, A. (2010). Contribution des systèmes d'information à la performance des organisations : le cas des banques. La Revue des Sciences de Gestion 2010/1 (n°241), p. 55-61. doi 10.3917/rsg.241.0055

Gouvernement du Canada. (2014). Archivé - L'innovation grâce aux technologies numériques. Tiré de https://www.ic.gc.ca/eic/site/028.nsf/fra/00037.html

Gouvernement du Québec. (2016). Stratégie numérique du Québec - Objectif numérique #StratNumQC. Tiré de https://www.economie.gouv.qc.ca/fileadmin/contenu/documents_soutien/strategies/economie_numerique/strategie_numerique_mandat.pdf

Gouvernement du Québec. (2017). Pratique recommandée en sécurité de l'information : Guide de sensibilisation à la sécurité de l'information. Tiré de https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/sensibilisation_securite_information.pdf

Howells, J. (2004). Sourcing external technology: a decision support framework for firms. *International Journal of Technology Management*, 27 (2-3), p. 143-154. doi :10.1504/IJTM.2004.003949

International Organization for Standardization (ISO). (2009). *Management du risque - Principes et lignes directrices*. Norme ISO-31000. Genève: ISO.

International Standardization Organizations (ISO). (2012). *Sécurité sociétale-Systèmes de management de la continuité d'activité*. Norme ISO-22301. Genève: ISO.

International Standardization Organizations (ISO). (2013). *Information technology - Security techniques- Information security management systems - Requirements*. Norme ISO-27001. Switzerland: ISO.

International Standardization Organizations (ISO). (2016). *Information technology - Security techniques- Information security management systems- Overview and vocabulary*. Norme ISO-27000. Switzerland: ISO.

International Standardization Organizations (ISO). *Gestion des risques liés à la sécurité de l'information. Apprendre à gérer les risques de son système d'information*. Norme ISO-27005. Genève: ISO.

Julien, P-A., & Marchesnay, M. (1988). La petite entreprise : Principes d'économie et de gestion. Paris, France: Vuibert.

Lefebvre, G. (2017). *La révolution numérique: Nos organisations sont-elles prêtes?* [Présentation PowerPoint]. Tiré de https://medias.irsst.qc.ca/videos/1711_au_co_HD_CEFRIO_fr_pdf.pdf

Liang, J. (2010). A resource-based perspective on information technology and firm performance: A meta-analysis. *Industrial Management & Data Systems*, Vol. 110 Issue: 8, pp.1138-1158. doi :10.1108/02635571011077807

Marty, M. (2014). *Analyses-diagnostics du potentiel de résilience d'une organisation.* (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

Mayer, R. (2008). *Learning and Instruction (2nd ed.)*. New Jersey, United States: Pearson.

Mell, P., & Granc, T., (2011). The NIST definition of cloud computing. Tiré de https://csrc.nist.gov/publications/detail/sp/800-145/final

Mercator. (2014). Mercator (11 éd.). Tiré de http://www.mercator-publicitor.fr/lexiquemarketing-definition-analyse-diagnostic

Micouleau, D. (2016). *Potentiel de résilience d'une organisation – Application à des Services Municipaux*. (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

Ministère des Finances et de l'Économie (MFEQ). (2012). Plan d'action en économie numérique : Pour l'excellence numérique des entreprises et des organisations québécoises. Tiré de https://www.economie.gouv.qc.ca/fileadmin/contenu/documents_soutien/strategies/economie_numerique/paen.pdf

Ministère d'économie, de la science et de l'innovation du Québec. (2017). Industrie 4.0 : Les défis de la quatrième révolution industrielle. Tiré de *https://www.economie.gouv.qc.ca/bibliotheques/outils/gestion-dune-entreprise/industrie-40/industrie-40-les-defis-de-la-quatrieme-revolution-industrielle/*

Monino, J. (2013). Les TIC un outil indispensable pour une démarche d'intelligence économique. doi: 10.3917/maorg.018.0173

Organization for Economic Cooperation and Development (OCDE). (2004). Perspectives des technologies de l'information de l'OCDE. Tiré de https://www.oecd.org/fr/sti/ieconomie/37620150.pdf

Organization for Economic Cooperation and Development (OCDE). (2014). Examen de l'OCDE des politiques d'innovation. Tiré de https://www.oecd.org/fr/sti/inno/innovation-france-ocde.pdf

Petit, F. (2009). *Concept d'analyse de la vulnérabilité des infrastructures essentielles - Prise en compte de la cybernétique*. (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

Plamondon-Tremblay, T. (2018). *La prise en compte de l'analyse des dépendances aux ressources dans la planification de la continuité des opérations*. (Mémoire de maîtrise, Polytechnique Montréal, Montréal, Québec).

Porter, M. (2003). *L'avantage concurrentiel : Comment devancer ses concurrents et maintenir son avance*. France : Dunod.

Porter, M. (1985). The Competitive Advantage: Creating and Sustaining Superior Performance. New York: Free Press.

Robert, B., & Morabito, L. (2009). Réduire la vulnérabilité des infrastructures essentielles-Guide méthodologique. Paris, France : Éditions TEC&DOC.

Savoie-Zajc, L., & Guillemette, S. (2001). La recherche-action et ses rapports de coconstruction de savoirs et de formation dans une perspective de professionnalisation entre acteurs praticiens et chercheurs. doi:10.18162/fp.2012.7

ANNEXE A- LA MÉTHODE OCTAVE-ALLEGRO

Les 8 étapes de la méthode OCTAVE-Allegro décrites dans le rapport technique de CERT sont les suivantes :

Étape 1 : Établir les critères qualitatifs d'évaluation des risques

L'objectif est d'établir les critères de mesure des risques et d'identifier les principaux éléments de l'organisation concernée (réputation et confiance des clients, finances, productivité, sûreté et santé, législatif, etc.).

Étape 2 : Établir un profil des actifs informationnels

Cette étape consiste à identifier l'ensemble des actifs informationnels nécessaires à l'établissement du profil des actifs informationnels et leurs fréquences d'utilisation.

Pour ce faire, il nécessaire de répondre à des questions comme : quels sont les actifs qui ont le plus de valeur pour l'organisation ? Les actifs qui sont utilisés tous les jours dans l'accomplissement des diverses tâches de l'organisation ? Les actifs dont la perte empêcherait l'organisation d'atteindre ses objectifs ?

Étape 3 : Identifier les intervenants et les contenants

Pour chaque actif identifié dans le profil des actifs informationnels, il est nécessaire les lieux et les façons dont ces actifs sont conservés, les éléments technologiques impliqués (les serveurs d'applications web ou de bases de données, réseaux internes, Internet, stations de travail, etc.) ainsi que les utilisateurs.

Étape 4 : Identifier les domaines de préoccupation

Dresser une liste des situations pouvant affecter les actifs informationnels de l'organisation et à partir de la description de la situation choisie, un scénario possible peut être établi et détaillé en spécifiant les éléments suivants (acteurs, moyens, motifs, résultats et impacts sur les exigences de sécurité, etc.). Le but de cette étape est de développer un réflexe chez l'équipe d'analystes et les aider à se préparer et réagir face à une situation de crise et non pas imaginer tous les scénarios possibles.

Étape 5. Identifier les scénarios de menaces

Les domaines de préoccupation sont étendus en scénarios de menaces qui détaillent de plus en plus les propriétés des menaces sur les actifs informationnels de l'organisation. Les informations ressorties seront utilisées pour l'établissement des scénarios de menaces.

Étape 6. Identifier les risques

Déterminer les conséquences pour chaque scénario de menace identifié. Une échelle de faible, moyen et fort pour déterminer les conséquences touchant la réputation de l'organisation, la finance, la production, la santé & sécurité dans le travail, etc. Les valeurs 1, 2 et 3 sont attachées respectivement à l'échelle de faible, moyen et fort pour calculer le score des conséquences dues à une faille de sécurité informatique.

Étape 7. Analyser les risques

Attribuer une valeur qualitative pour décrire l'impact d'une menace sur l'organisation en fonction des objectifs de l'organisation.

Étape 8. Choisir une approche face aux risques

Choisir comment réagir face aux risques, c'est-à-dire choisir le type de traitement et évaluer le risque résiduel. En effet, l'organisation a trois options pour traiter les risques identifiés :

1) Accepter les risques.
2) Atténuer les risques en mettant en place des mécanismes de protection pour réduire les impacts et appréhender les vulnérabilités.
3) Transférer les risques à une assurance ou à des prestataires de service.

ANNEXE B - LA FICHE DE LA RENCONTRE 1 ET 2

Objectif pré-rencontre : Caractériser les contraintes de l'organisation et commencer à réfléchir aux différents outils technologiques liés aux technologies de l'information et de communication (TIC) utilisées afin de satisfaire les contraintes.

Objectif de l'atelier du travail : À partir des contraintes de l'organisation, faire le lien avec l'utilisation de TIC et caractériser la vulnérabilité associée à ces systèmes.

Identification des contraintes

Qu'est-ce qu'une contrainte : Il s'agit d'une condition à satisfaire afin d'atteindre les objectifs de l'organisation

Nous avons identifié six types de contraintes :

1. Contractuelles : proviennent d'un engagement passé entre l'organisation et un acteur extérieur via un contrat reconnu et accepté par les deux parties.
2. Légales : requis légaux que l'organisation doit respecter de par la nature de ces activités.
3. Organisationnelles : issues de règles ou politiques de gestion internes.
4. Techniques : relèvent du domaine technique des activités de l'organisation. Elles peuvent porter sur les équipements de l'organisation ou sur certaines étapes clés du processus industriel, etc.
5. Économiques : requis économiques afin d'assurer la pérennité financière de l'organisation.
6. Sécuritaires : conditions pour maintenir un environnement de travail sécuritaire pour le personnel, mais aussi pour la protection des biens et des actifs.

Avant la rencontre, il faut identifier diverses contraintes et lors de la rencontre, nous ferons avec vous le lien entre ces contraintes et :

- L'identification des conséquences pouvant en résulter.
- Les marges de manœuvre.
- L'utilisation des TIC qui en découle.
- Les perturbations pouvant toucher les TIC qui interviennent dans la satisfaction des contraintes appliquées à l'organisation.

ANNEXE C- LA FICHE DE LA RENCONTRE 3

Objet de la rencontre 3 : À partir des contraintes de l'organisation, faire le lien avec l'utilisation de TIC et comprendre les processus décisionnels quant aux choix des fournisseurs externes des TIC et des vulnérabilités que cela entraine pour l'organisation.

Une contrainte est une condition à satisfaire afin d'atteindre les objectifs de l'organisation. Six types de contraintes ont été identifiées :

7. Contractuelles : proviennent d'un engagement passé entre l'organisation et un acteur extérieur via un contrat reconnu et accepté par les deux parties.
8. Légales : requis légaux que l'organisation doit respecter de par la nature de ces activités.
9. Organisationnelles : issues de règles ou politiques de gestion internes.
10. Techniques : relèvent du domaine technique des activités de l'organisation. Elles peuvent porter sur les équipements de l'organisation ou sur certaines étapes clés du processus industriel, etc.
11. Économiques : requis économiques afin d'assurer la pérennité financière de l'organisation.
12. Sécuritaires : conditions pour maintenir un environnement de travail sécuritaire pour le personnel, mais aussi pour la protection des biens et des actifs.

Lors de la rencontre, nous ferons le lien entre ces contraintes, l'utilisation des TIC, les dépendances avec des fournisseurs informatiques et les mesures de protection mises en place.