Un modèle de réseau bayésien pour la gestion des risques dans la gouvernance d'un centre de services informatiques

par

Cristian Chirca

essai présenté au CeFTI
en vue de l'obtention du grade de maître en génie logiciel
(maîtrise en génie logiciel incluant un cheminement de type cours en génie logiciel)

FACULTÉ DES SCIENCES
UNIVERSITÉ DE SHERBROOKE

Longueuil, Québec, Canada, mai 2014

Sommaire

Le centre de services informatiques est le point central de contact entre les utilisateurs des systèmes informatiques et le département d'informatique d'une organisation. Le bon fonctionnement du centre de services est essentiel non seulement pour le département d'informatique, mais aussi pour l'entreprise en général. N'importe quelle déviation d'une activité normale pourrait générer des effets indésirables. L'implémentation d'un système efficace de la gestion des risques est essentielle pour le bon fonctionnement du centre de services.

L'essai aborde la question de la gestion des risques dans un centre de services au moyen d'un outil formel : les réseaux bayésiens. Un modèle de réseau bayésien a été réalisé en utilisant des informations acquises par des sondages et entrevues avec divers experts. La validation du modèle est faite en utilisant des données statistiques et un logiciel dédié à la gestion des risques.

Remerciements

Je veux remercier à mon épouse Elena et à mon fils David pour leur compréhension et support sans lesquels la réalisation de cet essai n'était pas possible.

Je veux remercier à mes directeurs, M. Valéry Bevo et M. Pierre-Martin Tardif, qui ont eu beaucoup de patience et m'ont offert le meilleur encadrement possible.

J'aimerais aussi remercier à M. Claude Cardinal qui m'a donné de très bons conseils et m'a appuyé pendant mes études et la rédaction de mon essai.

Table de matières

Introduction 1

Chapitre 1 - Le centre de services 3

1.1 Le centre de services dans ITIL 4

1.1.1 Centre de services local ou réparti 5

1.1.2 Centre de services centralisé 6

1.1.3 Centre de services virtuel 7

1.2 Outils 8

Chapitre 2 - La gestion des risques 11

2.1 Risk IT 12

2.1.2 Domaines du Risk IT 15

2.2 Méthodes utilisées pour la gestion du risque dans le cadre d'un centre de services 20

Chapitre 3 - Le modèle de réseau bayésien 22

3.1 Les réseaux bayésiens 22

3.1.1 Définition 23

3.1.2 Construction 24

3.2 Problématique 25

3.3 Méthodologie 26

3.3.1 Cadre théorique 27

3.3.2 Processus de développement 28

3.4 Construction du modèle de réseau bayésien 31

3.4.1 Identifier les risques 31

3.4.2 Classifier les risques 32

3.4.3 Le modèle graphique 39
3.4.4 Choisir les risques 41
3.4.5 Le modèle de réseau bayésien 43
3.4.6 Validation du modèle 51
Conclusions 56
Liste des références 58
Annexe 1 60
Formulaire sondages français 60
Annexe 2 63
Formulaire sondages anglais 63

Liste des tableaux

2.1 Avantages comparatifs des réseaux bayésiens 21

3.1 Score des risques 42

3.2 probabilités marginales pour le soutien de la haute direction 45

3.3 Exemples valeurs nœud Budget insuffisant 46

3.4 Exemple "what-if" 52

3.5 Exemple a posteriori 54

Liste de figures

1.1 Centre de services décentralisé 6
1.2 Centre de services centralisé 7
1.3 Centre de services virtuel 8
2.1 Vue d'ensemble de la cascade d'objectifs de COBIT 5 12
2.2 Le Référentiel Risk IT 16
3.1 Étapes de construction d'un réseau bayésien 25
3.2 Modèle graphique 40
3.3 Résultats sondage Internet 43
3.4 Modèle de réseau bayésien 44
3.5 Le modèle de réseau bayésien dans AgenaRisk 51
3.6 Temps moyen pour fermer des incidents (extrait du logiciel Track-It!) 55

Liste des abréviations, symboles et sigles

ITIL	Information Technology Infrastructure Library
ISACA	Information Systems Audit and Control Association
TI	Technologies de l'information
ITSSMIT	Service Support Management
ICP	Indicateurs clés de performance
SLA	Service Level Agreement
ITSSM	IT Service Support Management

Introduction

Le rôle joué par l'informatique dans l'activité d'une entreprise a connu une croissance exponentielle dans les dernières décennies. Le bon fonctionnement de la majorité des entreprises ne peut pas se dérouler sans l'utilisation des systèmes informatiques : courriel, services d'impression, logiciels de gestion.

Les entreprises utilisent d'autres systèmes informatiques pour gagner de la visibilité et attirer de potentiels clients : sites web, moteurs de recherche, publicité électronique. Les activités financières sont accomplies en utilisant des systèmes informatiques : activité bancaire, déclaration de taxes, paiement de rétribution et factures. Les projets de design ou conception complexes sont basés sur des logiciels et systèmes informatiques très puissants. Les formations, communications et réunions se font de plus en plus dans un milieu virtuel à l'aide des systèmes informatiques.

Les utilisateurs de ces systèmes ont acquis des connaissances pour l'utilisation de ces ressources mais ils ne sont pas nécessairement des experts informatiques. Lorsqu'ils ont un problème qui dépasse leurs compétences, ils demandent l'aide aux spécialistes. Sauf que ces spécialistes ont chacun leur aire d'expertise : applications, réseautique, communication ou système d'exploitation. Pour aider les utilisateurs, les entreprises ont mis en place une structure qui offre un seul point de contact pour les utilisateurs qui ont besoin d'aide relativement à un problème informatique : le centre de services informatiques.

Les gestionnaires du centre de services doivent s'assurer qu'ils sont capables d'offrir le support requis par les utilisateurs d'une façon efficace dans des délais raisonnables. Toutes les syncopes dans le bon fonctionnement du centre de services sont reflétées sur la qualité du service offert à l'utilisateur et peuvent causer de pertes importantes à l'entreprise. Pour éviter ces syncopes, les gestionnaires mettent en place un système pour la gestion du risque.

Le but de cet essai est de trouver une méthode formelle pour la gestion des risques dans la gouvernance d'un centre de services. Dans une première étape, un cadre est défini pour le centre de services et pour la gestion du risque.

ITIL est un choix naturel pour encadrer le centre de services. ITIL est une collection de bonnes pratiques qui cible la gestion des services informatiques. Dans la perspective ITIL, le centre de services informatiques est le point central de contact entre les utilisateurs du système informatique et le département informatique d'une organisation. ITIL définit les responsabilités du centre de services et les processus dans lesquels il est impliqué par ses activités. Il définit aussi les différents types de centre de services. Cette structure permet une meilleure identification des risques potentiels, des mesures de mitigation et des personnes ou entités responsables.

Pour la gestion du risque, le référentiel Risk IT est choisi. Risk IT, rattaché directement au cadre COBIT, offre l'avantage de traiter spécifiquement les risques reliés à l'informatique et offre une vision complète des domaines, des processus et des activités pour l'évaluation, le traitement et la gestion du risque.

Une fois le cadre théorique établi, une méthode formelle est choisie, méthode qui peut s'intégrer facilement dans les activités ITIL et Risk IT. L'utilisation de réseaux bayésiens dans la gestion des risques est une approche de choix pour d'autres domaines d'activité tels que financier ou médical. L'essai veut établir si cette méthode est pertinente et offrir un modèle pour la gestion du risque dans le cadre de la gouvernance d'un centre de services informatiques.

Des entrevues avec des experts sont réalisées, deux sondages pour l'identification et la classification des risques collectent des données qui sont utilisées pour réaliser un modèle de réseau bayésien. Ce modèle est validé dans un logiciel spécialisé et quelques exemples sont utilisés pour valider le fonctionnement du modèle.

Chapitre 1

Le centre de services

Si jusqu'à la fin du siècle XX la société était connue comme une société industrielle, dans les dernières décades, la société a évolué vers une société de l'information. Le rôle joué par l'information est dans une croissance continue et il est reflété en particulier par le développement du secteur de l'informatique, de la communication et des services associés. L'importance de l'information dans tous les aspects de la société actuelle est devenue une préoccupation à tous les niveaux. L'Organisation des Nations Unies a organisé deux sommets mondiaux sur la société de l'information suivis par de forums annuels sur ce sujet [1]. L'Union internationale des télécommunications mentionne dans un rapport [2] qu'en 2013, plus de 41 % des maisons dans le monde détenaient un ordinateur connecté à l'Internet par comparaison à l'année 2005 quand ce pourcentage était de 18,4. Pour les pays développés, ce pourcentage était beaucoup plus élevé : 77,7 % en 2013.

Les organisations doivent s'adapter à cette nouvelle société où l'information fait partie de leur patrimoine. La façon dans laquelle les entreprises accèdent, analysent et utilisent l'information peut offrir un avantage stratégique face à la compétition. Dans leurs études sur l'utilisation de l'information, IBM mentionne que dans le monde sont produits chaque jour 2.5 exabytes de données [3] et présente des études des cas ou l'analyse des données à amener des améliorations significatives dans divers domaines [4]:

- Santé : réduction de 20 % en ce qui concerne la mortalité des patients
- Opérateurs de télécommunications : réduction de 92 % du temps pris pour traiter les données
- Utilités : 99 % d'amélioration de la précision de l'emplacement des ressources de production d'électricité

Pour accueillir, analyser et utiliser ces données, les entreprises ont mis en place un système informatique plus ou moins complexe. Ce système peut être utilisé dans tout le processus d'une entreprise : de l'acquisition et production, en passant par la comptabilité et jusqu'au marketing et la vente. Le système peut constituer un des principaux outils de contact entre l'entreprise, ses fournisseurs et clients. Les entreprises veulent s'assurer que leurs employés, partenaires et clients ont toujours accès au système. Malheureusement de problèmes ou des anomalies peuvent apparaitre et les utilisateurs du système ont besoin de contacter quelqu'un qui peut les aider.

1.1 Le centre de services dans ITIL

Dans la perspective ITIL, le centre de services informatiques est le point central de contact entre les utilisateurs du système informatique et le département informatique d'une organisation. Les utilisateurs contactent le centre de services pour se faire aider par de personnes qualifiées pour résoudre leurs problèmes, sans être obligés à chercher une personne spécifique capable de traiter leur problème. [5, p. 121]

Le centre de services peut avoir plusieurs responsabilités :

- Recevoir, enregistrer et traiter tous les appels : rapports des erreurs, demandes des services, demandes de changement
- Faire le diagnostic initial, offrir une solution rapide et escalader le problème à un niveau supérieur qui peut fournir un meilleur diagnostic et résolution
- Faire le suivi pour tous les appels tout au long jusqu'à la validation et la fermeture d'incident, en s'assurant que le niveau de services soit respecté
- Coordonner les activités d'escalade et informer régulièrement les utilisateurs sur l'état de leur demande
- Fournir l'information aux utilisateurs : procédures, changements prévus, services offerts, erreurs existantes, services de maintenance

- Surveillance de l'infrastructure: systèmes d'alertes et notifications, mises à jour, copies de sauvegarde

Les principaux processus ITIL dont le centre de services est impliqué par ses activités sont :

- la gestion des incidents
- la gestion de mises en production
- la gestion des niveaux de services
- la gestion des configurations
- la gestion de changements

Différents aspects déterminent le type et la structure du centre de services. La structure de l'entreprise peut être mono-site ou repartie sur plusieurs sites qui peuvent être localisés proche ou dans différents régions ou même pays et continents. En ce qui concerne les utilisateurs, leur nombre, leur niveau de connaissances, leurs particularités linguistiques et culturelles influencent la structure du centre de services. Les niveaux de services attendus, les types et nombre d'applications utilisées, les décalages horaires, les technologies disponibles ont une influence majeure sur la structure, le type et la localisation du centre.

ITIL identifie [5, p. 123] trois types courants de centres de services : local ou réparti, centralisé et virtuel

1.1.1 Centre de services local ou réparti

Il est basé sur le principe que chaque site (si plusieurs) ou chaque unité fonctionnelle de l'entreprise dispose de son propre centre de services. Dans ce cas le principal avantage est la proximité des utilisateurs et la facilité de répondre rapidement et efficacement à leurs demandes. Toutefois la coordination centrale, la standardisation du processus, la maintenance d'une base de connaissances commune sont plus difficiles à réaliser.

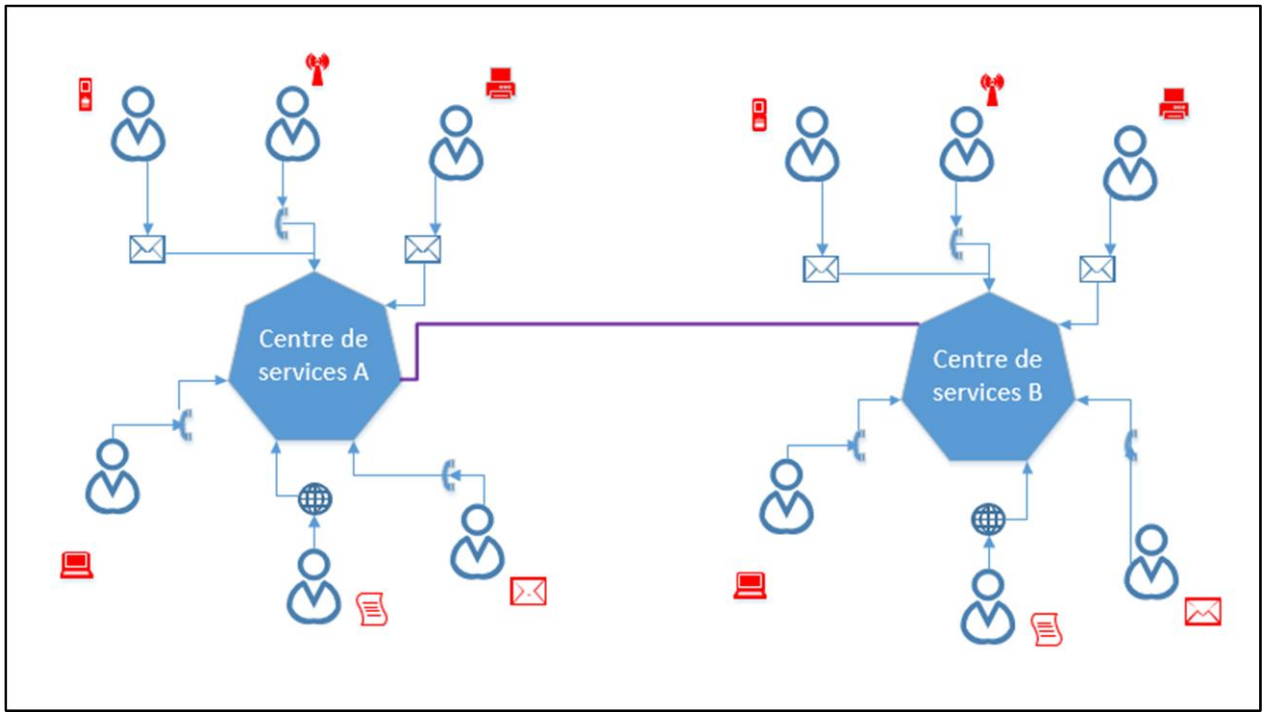

Figure 1.1 Centre de services décentralisé

1.1.2 Centre de services centralisé

Dans ce cas, un seul centre de services répond à toutes les entités de l'entreprise permettant une meilleure gestion des ressources et un meilleur contrôle des processus. Au contraire, des problèmes liés aux spécifiques locaux de chaque entité, des problèmes de langues et des fuseaux horaires peuvent constituer un problème.

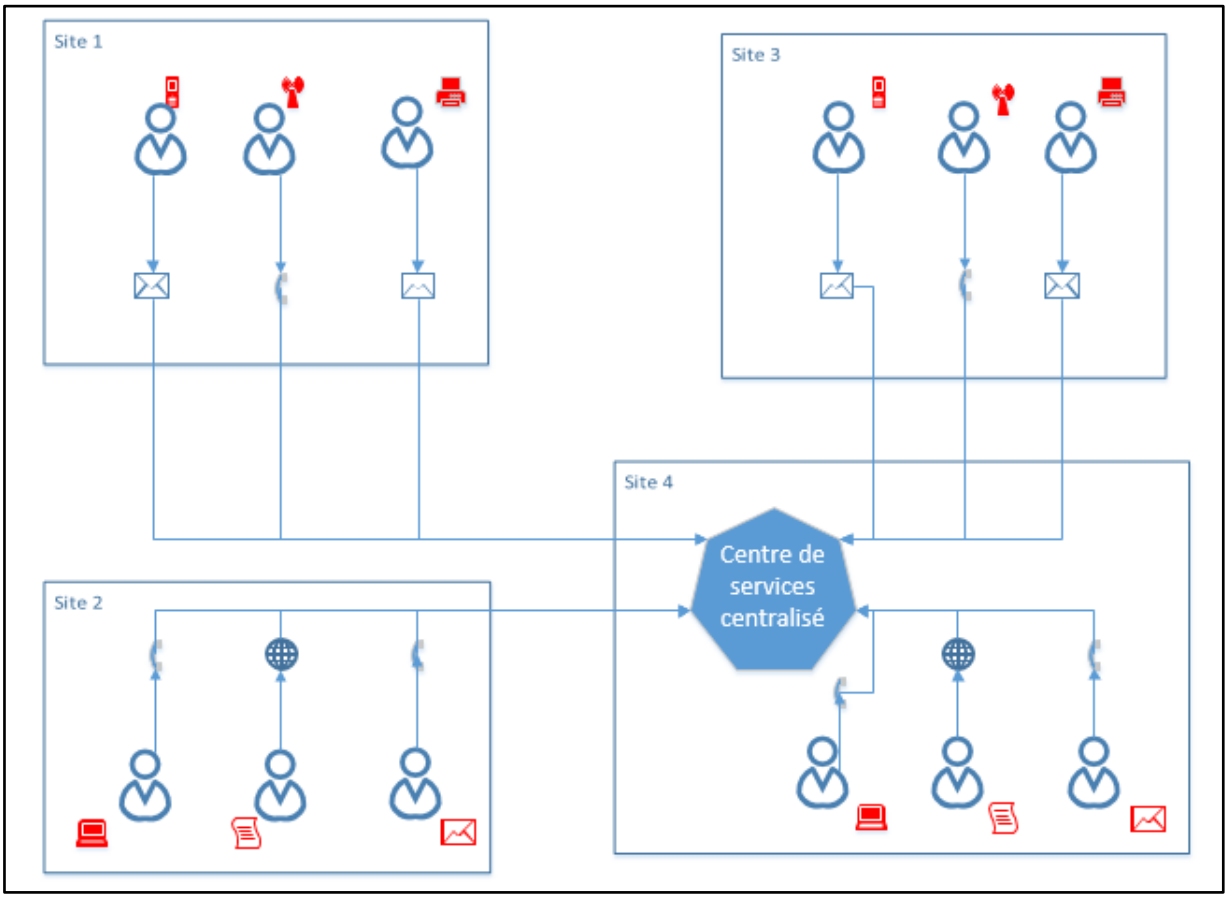

Figure 1.2 Centre de services centralisé

1.1.3 Centre de services virtuel

Il s'agit d'un modèle qui est une combinaison des deux types de structures précédents, composé d'un ou plusieurs centres de type local qui réagit comme un centre de type central. Dans ce cas l'emplacement géographique n'est plus important. Ce modèle permet d'offrir un support complexe et il est utilisé pour des structures qui sont distribuées sur multiples fuseaux horaires et un service 24/7. Ce modèle est mis en place dans le cas où les services sont externalisés. Avec l'avancement technologique, un seul point de contact sert pour plusieurs centres de services d'une façon transparente pour les utilisateurs. Des problèmes culturels et

linguistiques ainsi qu'une difficulté à offrir l'assistance sur place sont en général les principaux enjeux pour ce modèle.

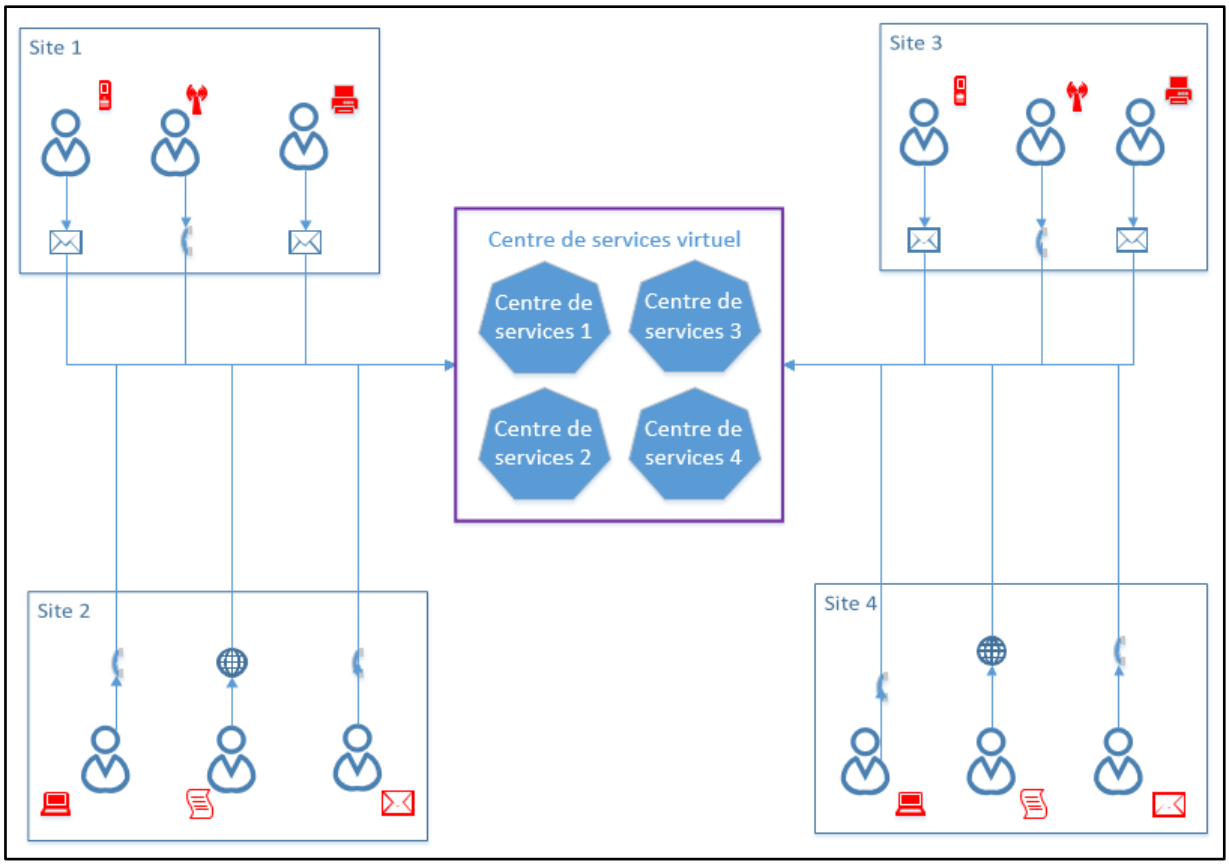

Figure 1.3 Centre de services virtuel

1.2 Outils

Avec l'avancement technologique, les centres de services ont une multitude d'outils à leur disposition pour faciliter la gestion des services :

- Logiciels dédiés à l'activité des centres des services
- Outils d'intégration avec la gestion de services et la gestion de système

- Outils en libre service qui permettent aux utilisateurs de trouver des solutions à leurs problèmes ou de rapporter les problèmes de façon efficace
- Systèmes de réponse vocale interactifs
- Services de courriel avec capacité de filtrage et classification
- Systèmes de téléphonie intelligente avec techniques intégrés d'identification et routage d'appels
- Outils de gestion avec modules automatisés d'alertes et notifications
- Vaste plateforme de communication téléphonique et réseau
- Access à une multitude des bases de connaissances
- Outils de diagnostic et connexion à distance

Il existe plusieurs outils de mesure et contrôle de l'efficacité du centre de services. La satisfaction du client est le premier critère et des mesures telles que le délai de réponses aux appels et courriels, les délais de restauration du service, le temps écoulé avant qu'une solution soit fournie ou que le problème soit escaladé se retrouvent dans des rapports qui peuvent être consultés par les gestionnaires. Les sondages sont de méthodes d'évaluation pour les indicateurs qui ne sont pas directement mesurables comme la courtoisie ou les conseils offerts pour éviter d'une façon proactive la réapparition des problèmes.

En outre de l'aspect technique du centre de services, les entreprises doivent considérer les avantages stratégiques qu'un centre de services peut fournir : augmentation de la productivité, création de la valeur ajoutée, réduction des coûts, amélioration de la qualité du service aux utilisateurs ou l'amélioration de la perception des services informatiques de l'entreprise par les utilisateurs.

Tenant compte de l'importance du centre de services informatiques non seulement pour le département informatique, mais pour l'entreprise en général, n'importe quelle déviation d'une activité normale peut générer des effets dommageables. L'implémentation d'un système

efficace de la gestion des risques devient une exigence incontournable pour les gestionnaires du centre de services. Cela est reflété dans ITIL, où, avec chaque nouvelle version, le rôle accordé à la gestion du risque devient de plus en plus important [16]. Même si la gestion de risque est traitée à travers les livres ITIL, il n'existe pas un processus dédié au risque avec des activités clairement définies. Ce problème est examiné dans le chapitre suivant.

Chapitre 2

La gestion des risques

Pour chaque entreprise qui tente d'avoir un niveau de maturité élevé dans leur processus de gestion, la gestion des risques est toujours un des domaines les plus difficiles à gérer. Dans un sondage publié par William Ibbs and Young H. Kwak [6, p. 441], la gestion des risques a été le domaine avec le plus bas taux de maturité sur une base de 1 à 5 : 2.75. De plus elle était le seul domaine avec une maturité plus petite que trois pour tous les quatre types d'entreprises analysés : constructions, télécommunications, système informatique et développement de logiciels et manufacturiers de haute technologie.

Thomas Coleman considère que *« in reality, risk management is as much the art of managing people, processes, and institutions as it is the science of measuring and quantifying risk »*[1]. Plusieurs normes et cadres existent pour faciliter et guider la gestion des risques :

- ISO 31000 : 2009
- OCEG 1.0 : 2009
- BS 31100 : 2008
- COSO : 2004
- FERMA : 2002

Ces référentiels sont conçus pour la gestion du risque de l'entreprise et ils ne sont pas dédiés à la gestion du risque TI.

[1] En réalité, la gestion de risque est autant l'art de gérer les gens, les processus et les institutions, de même qu'elle est la science à mesurer et de quantifier le risque. (traduction libre)

2.1 Risk IT

Un référentiel conçu pour aider les gestionnaires dans la gouvernance des TI de l'entreprise, COBIT a été développé par ISACA, une association indépendante et leader en matière de la connaissance, de la gestion et de la gouvernance des TI.

Dans la version 5 de COBIT, parmi les trois principaux objectifs de la gouvernance se trouve l'optimisation des risques qui couvre tous les processus et les fonctions au sein de l'entreprise pour maintenir les risques reliés aux TI à un niveau acceptable par rapport à la réalisation des bénéfices et l'utilisation des ressources de l'entreprise.

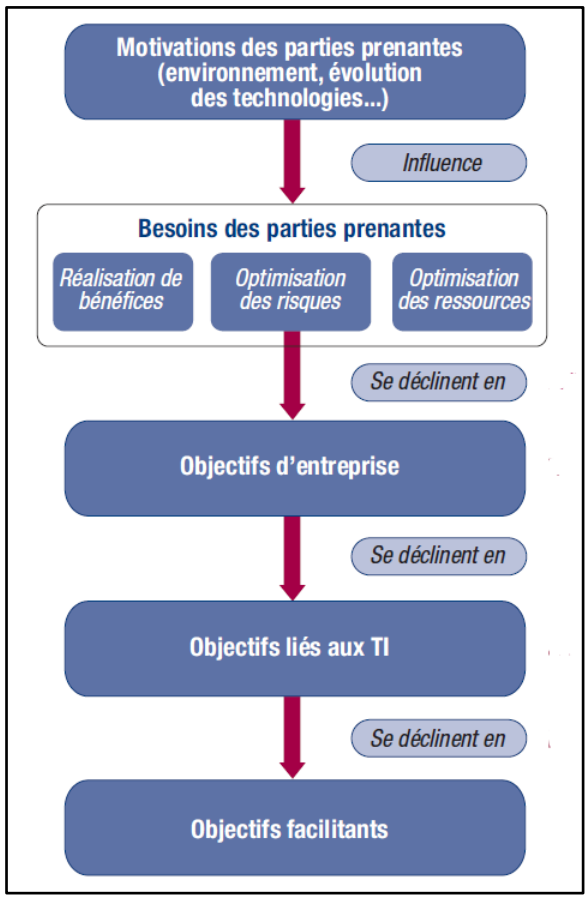

Figure 2.1 Vue d'ensemble de la cascade d'objectifs de COBIT 5

Source : [7, p. 20]

Dérivé du COBIT, ISACA a développé un référentiel dédié à la gestion des risques : Risk IT. Risk IT complète COBIT, mettant ensemble dans un référentiel les meilleures pratiques qui permettent aux entreprises d'identifier et gérer le risque. Risk IT permet aux entreprises de créer une image exacte des risques TI actuels et futurs et de réaliser un profil complet qui éventuellement va les aider à mieux utiliser leurs ressources. Une fois le profil réalisé, des responsabilités sont définies et acceptées, ensuite les risques TI sont englobés dans la structure générale de risque et conformité de l'entreprise. Risk IT offre des solutions pour capitaliser l'investissement fait dans le système de contrôle, en augmentant la qualité et l'efficacité des processus d'affaires par une meilleure gestion des risques TI. Il permet aussi d'améliorer la communication entre les divers départements et unités de l'entreprise en utilisant un langage commun et une guidance d'un but à l'autre qui va plus loin que les mesures pures techniques [8, p. 12].

2.1.1 Principes

Risk IT est basé sur six principes [8, p. 13] :

1. Toujours être connecté aux objectifs de l'entreprise

   Le risque relié au TI est traité comme un risque d'affaire, il doit être analysé en fonction de son impact sur le processus d'affaires et la réalisation des objectifs des entreprises. La gestion des risques TI est un émulateur d'affaires assurant que les valeurs actuelles sont protégées et permettant l'apparition de nouvelles opportunités.
   Les gestionnaires du centre de services doivent être au courant des objectifs de l'entreprise et aligner leur gestion des risques en conséquence.

2. Aligner la gestion des risques TI avec la gestion globale des risques de l'entreprise

   Les objectifs de l'entreprise et le niveau d'acceptabilité des risques sont bien définis et le

processus de décision prend en considération les conséquences et les opportunités offertes par le risque TI. La vision globale sur le risque est consolidée à travers l'entreprise.

La gestion des risques pour le centre de services est flexible et elle s'adapte à la politique de gestion des risques de l'entreprise. Les gestionnaires du centre de services sont informés sur la gestion globale du risque de l'entreprise et ils adaptent la gestion des risques du centre de services en conséquence.

3. Balancer les coûts et les bénéfices de la gestion des risques TI.

   Une analyse coûts-bénéfices est faite et des mesures de contrôle sont mises en place pour assurer le contrôle de plusieurs risques qui sont hiérarchisés et traités d'une manière plus efficace.

   Les gestionnaires du centre de services évaluent les coûts et les bénéfices associés aux risques identifiés dans le contexte global de l'entreprise

4. Promouvoir une communication ouverte et honnête du risque associé au TI.

   Des informations claires, opportunes sont offertes en termes compréhensibles et elles servent dans la prise de toutes les décisions concernant le risque.

   Une communication transparente et bidirectionnelle entre les gestionnaires du centre de services et ceux du département informatique et même de la direction de l'entreprise est mise en place en permanence.

5. Établir la ligne de conduite de haut niveau et responsabiliser les employés pour attendre les niveaux d'acceptabilité désirés.

   La haute direction supporte la gestion des risques TI et elle est impliquée dans la prise des décisions importantes. Des personnes spécifiques sont nommées responsables pour assurer la bonne fonctionnalité de la mise en place et du processus de contrôle, des politiques et procédures claires sont poussées avec le support de la direction.

   Les décisions prises par la haute direction de l'entreprise sont agrégées et mises en place de façon efficace dans le cadre du centre de services.

6. La gestion des risques doit se faire de façon continue sur une base quotidienne.

   Par sa nature le risque évolue de façon très dynamique, chaque changement pouvant entrainer de nouveaux risques ou opportunités, d'où le besoin d'évaluer ou réévaluer le risque d'une façon continue. Les changements majeurs sont énoncés aussi tôt que possible pour permettre une analyse complète et approfondie. Les responsables sont bien connus, les processus, les risques associés et les impacts sont identifiés. Des déclencheurs pour la révision de processus sont mis en place.

   Le centre des services est un milieu dynamique et la bonne fonctionnalité du centre est reflétée dans la disponibilité des ressources pour les utilisateurs du système informatique, d'où la nécessité d'assurer une gestion des risques continue qui peut aider à la découverte et la résolution des problèmes potentiels.

2.1.2 Domaines du Risk IT

Le référentiel Risk IT est basé sur trois domaines [8, p. 15]: la gouvernance, l'évaluation et la réponse au risque. Chaque domaine est divisé en processus et chaque processus a plusieurs activités associées. Les gestionnaires du centre de services participent dans la gouvernance des risques en concordance avec les principes mentionnés antérieurement. Ils suivent le référentiel Risk IT et mettent en pratique le processus et les activités, non seulement pour assurer une meilleure gestion des risques associés au centre de services, mais aussi pour aligner le processus de la gestion avec le processus global de gestion des risques et le modèle d'affaires de l'entreprise.

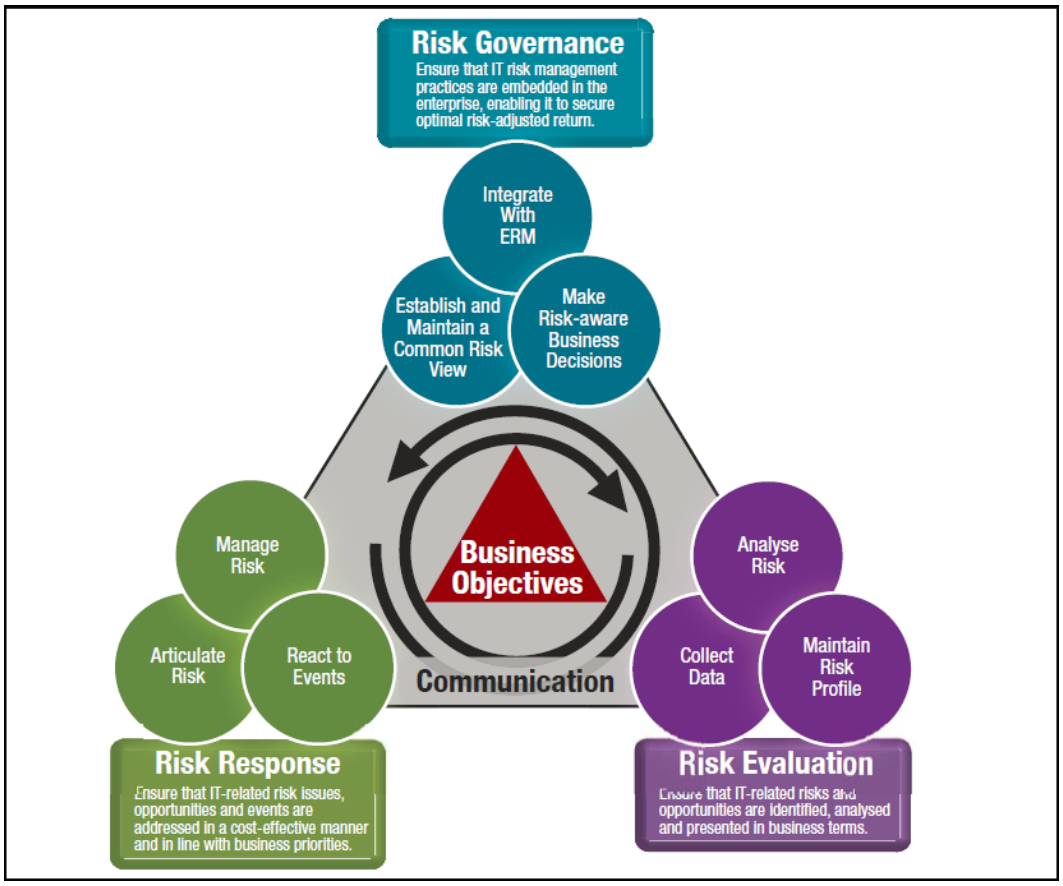

Figure 2.2 Le Référentiel Risk IT

Source : [8, p.15]

La gouvernance du risque est le domaine qui s'assure que les pratiques utilisées dans la gestion du risque TI soient intégrées dans la gouvernance de l'entreprise. Les processus et les activités pour ce domaine sont:

1. Établir et maintenir une vision commune : les activités de la gestion des risques sont alignées avec la capacité de l'entreprise de supporter les pertes associées au TI et la tolérance de la direction de l'entreprise par rapport à cela. Les activités de ce processus sont :
    - Évaluer le risque TI de l'entreprise

- Proposer des seuils de tolérance du risque TI
- Approuver les seuils de tolérance
- Aligner la politique des risques TI
- Promouvoir une culture d'entreprise avisée sur le risque TI
- Encourager une communication efficiente du risque TI

2. Intégrer avec la gestion des risques de l'entreprise : la gestion des risques TI est alignée à la gestion des risques de l'entreprise pour les décisions stratégiques. Plusieurs activités sont définies :
    - Établir est maintenir des personnes responsables pour la gestion des risques TI
    - Coordonner la gestion des risques TI avec la gestion des risques de l'entreprise
    - Adapter les pratiques associées au risque TI avec celle du risque de l'entreprise
    - Assurer les ressources nécessaires pour la gestion des risques TI
    - Fournir une garantie par une autorité indépendante pour la gestion des risques TI
3. Prendre de décisions d'affaires en conscientisant le risque
    - Gagner la confiance de la direction pour les méthodes d'analyse du risque TI
    - Approuver l'analyse du risque TI
    - Intégrer les considérations sur le risque TI dans la prise de décisions stratégiques de l'entreprise
    - Accepter le risque TI
    - Prioriser les activités de réponse au risque TI

La métrique du domaine de la gouvernance des risques est la mesure dans laquelle l'utilisation stratégique des TI dans la mobilisation des ressources de l'entreprise réduit le risque global de l'entreprise. Une autre mesure est représentée par le pourcentage des personnes qualifiées dans la gestion des risques qui occupe de positions de gestionnaire du risque.

L'évaluation du risque est le domaine qui définit les processus et les activités pour s'assurer que les risques reliés à l'informatique soient identifiés, analysés et présentés en terme d'affaire. Trois processus composent ce domaine :

1. Colliger les données: identifier les données pour assurer une identification, analyse et communication efficiente. Les activités suivantes sont reliées à ce processus :
    - Établir et maintenir un modèle pour la collecte de données
    - Colliger des données concernant l'environnement d'activité
    - Colliger des données sur les évènements associés au risque
    - Identifier les facteurs de risque
2. Analyser les risques : développer d'informations utiles pour soutenir les décisions relatives au risque qui prennent en compte la relevance des facteurs de risque pour l'entreprise. Quatre activités sont mentionnées :
    - Définir la portée pour l'analyse de risque;
    - Estimer le risque TI;
    - Identifier des options de réponse au risque et
    - Effectuer une vérification parallèle de l'analyse de risque.
3. Maintenir le profil de risque : maintenir un inventaire mis à jour et complet des risques connus incluant des détails, spécifications, ressources et mesures de contrôle en référence avec le processus d'affaires. Plusieurs activités sont associées à ce processus :
    - Cartographier les ressources TI au processus d'affaires
    - Déterminer le niveau d'importance de ressource TI pour l'entreprise
    - Comprendre les capacités TI
    - Mettre à jour les éléments des scénarios de risque
    - Maintenir un registre des risques
    - Développer d'indicateurs de risque

La mesure du domaine de l'évaluation du risque est l'impact cumulatif pour l'entreprise causé par des incidents et événements qui ne sont pas anticipés par le processus d'évaluation du risque.

Le traitement du risque est le domaine qui offre des modalités pour traiter les problèmes, les opportunités et les événements reliés au risque TI en concordance avec les priorités d'affaires. Les processus associés à ce domaine sont :

1. Exprimer le risque : s'assurer que les informations sur l'état réel des expositions au risque et des opportunités sont mises à la disposition des personnes concernées en temps opportun pour obtenir une repose adéquate. Les activités de ce processus sont :
    - Communiquer les résultats de l'analyse du risque TI
    - Rapporter les activités de la gestion des risques TI et l'état de conformité
    - Interpréter les résultats de l'évaluation indépendante
    - Identifier les opportunités reliées au TI
2. Gérer les risques : assurer que les mesures pour garder les opportunités stratégiques et pour la réduction du risque sont gérées en tant qu'un portefeuille. Les activités sont :
    - Contrôler l'inventaire
    - Surveiller l'alignement opérationnel avec les seuils de tolérance au risque
    - Répondre aux expositions au risque et aux opportunités découvertes
    - Implémenter de contrôles
    - Rapporter les avancements du plan d'action du risque TI
3. Réagir aux événements : assurer que des mesures pour capter les opportunités immédiates ou pour limiter les pertes générées par des activités TI soient activées efficacement. Les quatre activités associées sont :
    - Maintenir un plan de réponse en cas d'incidents
    - Surveiller le risque TI
    - Initier la réponse aux incidents

- Communiquer les leçons apprises d'évènements reliés au risque

La mesure du domaine de traitement du risque est l'impact cumulatif pour l'entreprise causé par des incidents et événements qui sont anticipés par le processus d'évaluation du risque, mais pour lesquels il n'existe pas encore de mesures de mitigation ou un plan d'action.

2.2 Méthodes utilisées pour la gestion du risque dans le cadre d'un centre de services

Un des trois domaines sur lesquels est basé le référentiel Risk IT est l'évaluation des risques, basée sur l'habilité à mesurer et quantifier le risque. Plusieurs méthodes et modèles sont utilisés : réseau de neurones, système expert, méthode Delphi, arbres de décision, la régression linéaire, arbre de défaillances, matrices de probabilité et impact ou les réseaux bayésiens, chacune de ces techniques a ses propres avantages et désavantages, en considérant plusieurs aspects : l'expertise disponible, les coûts d'implémentation, les données disponibles, l'environnement ou les délais.

Patrick Naïm réalise une comparaison de divers modèles [9, p. 197]. Dans le tableau suivant, cinq modèles sont comparés : analyse de données, réseaux neuronaux, arbres de décision, systèmes experts et réseaux bayésiens. Pour chaque modèle, un signe de plus est marqué si la caractéristique constitue un avantage pour le modèle, une étoile (⋆) est placée dans la case de la meilleure technique du point de vue de la caractéristique considérée. L'utilisation des réseaux bayésiens est considérée la meilleure méthode pour la majorité des caractéristiques analysées.

Pendant des entrevues avec plusieurs gestionnaires des centres de services, l'analyse de données et les opinions des experts sont les méthodes utilisées le plus souvent dans la gestion du risque d'un centre de services.

Tableau 2.1 Avantages comparatifs des réseaux bayésiens

Connaissances	*Analyse de données*	*Réseaux neuronaux*	*Arbres de décision*	*Systèmes experts*	*Réseaux bayésiens*
ACQUISITION					
Expertise seulement				★	
Données seulement	+	★	+		+
Mixte	+	+	+		★
Incrémental		+			★
Généralisation	+	★	+		+
Données incomplètes		+			★
REPRÉSENTATION					
Incertitude				+	★
Lisibilité	+		+	+	★
Facilité		+	★		
Homogénéité					★
UTILISATION					
Requêtes élaborées	+			+	★
Utilité économique	+	+			★
Performances	+	★			

Source : [9, p. 197].

L'analyse de données est une méthode utilisée par le centre de services parce qu'elle est basée sur de données existantes, significatives. Toutefois les données ne sont pas toujours faciles à obtenir, et sont en format hétérogène qui rend leur utilisation plus difficile.

L'opinion des experts est une autre méthode de choix pour les centres de services, car les experts peuvent interpréter toutes les données existantes et les confronter avec les normes de l'industrie. Le désavantage de cette méthode est que les experts ne sont pas toujours disponibles et ça prend du temps avant qu'ils se familiarisent avec les particularités de chaque centre de services.

Les réseaux bayésiens offrent l'avantage qu'ils peuvent utiliser des données partielles et incomplètes et qu'ils sont faciles à adapter à un environnement spécifique en utilisant l'apprentissage.

Chapitre 3

Le modèle de réseau bayésien

Les réseaux bayésiens, tels que présentés dans la dernière section du chapitre précédent, sont une des meilleures options pour la gestion des risques. En fait, ils sont déjà utilisés dans la gestion des risques dans divers domaines [14, p. 1] : légal, médical, sécurité, financier, fiabilité.

Dans ce chapitre, un modèle de réseau bayésien pour la gestion des risques sera présenté dans le contexte d'un centre de services informatiques.

3.1 Les réseaux bayésiens

Les réseaux bayésiens sont de graphes acycliques orientés où les variables sont représentées par des nœuds et les relations de dépendance ou de corrélation entre les variables sont représentées par des arcs directionnels.

Chaque variable est représentée par un tableau de probabilités qui sont déterminées en utilisant le théorème de Bayes [10, p.12]:

$$P(H|E) = \frac{P(E|H) * P(H)}{P(E)}$$

Si l'hypothèse H est basée sur des données observées et E est l'évidence (la preuve), alors P(H) est une probabilité a priori de l'hypothèse, en fait le degré initial de confiance dans l'hypothèse. P(E|H) est la vraisemblance des données observées, donc la mesure dans laquelle l'évidence a été observée quand l'hypothèse était vraie. P(H|E) est la probabilité a posteriori de l'hypothèse étant donné l'évidence.

Le théorème de Bayes offre l'adaptabilité et la flexibilité qui permettent à l'utilisateur de réviser et changer les estimations et les prédictions si de nouvelles données pertinentes sont accueillies.

Les réseaux bayésiens sont la représentation de la dépendance entre un ensemble de variables. Un arc entre deux variables, disons de V à, W, dénote qu'il existe une relation de dépendance directe du V sur W et dans ce cas V est un parent de W. Les tableaux de probabilités associés aux nœuds sont la distribution de probabilités du nœud en considérant tous les parents de celui-là.

3.1.1 Définition

Dawn Holmes et Lakhmi Jain définissent formellement le réseau bayésien [11, p. 2] :

Soit S un ensemble fini de sommets et A un ensemble des arcs entre ces sommets sans boucles de rétroaction, les sommets et les arcs forment un graph acyclique orienté G = { S , A }. Un ensemble d'événements est représenté par les sommets de G et donc aussi par S. Soit chaque événement ait un ensemble fini de résultats mutuellement exclusifs, ou E_i est une variable qui peut prendre n'importe quelles issues e_i^j de l'évènement i ou j=1,…,n. Soit P une distribution de probabilités sur les combinaisons d'événements. Soit C l'ensemble des contraintes suivantes:

- une distribution de probabilités somme à l'unité
- pour chaque événement i et un ensemble de parents M_i il y a probabilités conditionnelles associées $P(E_i \mid \bigcap_{j \in M_i} E_j)$ pour chaque issue possible qui peut être assignée à E_i et E_j
- Ces relations d'indépendance impliquées par d-séparation dans le graphe acyclique orienté. Alors N = (G, P, C) est un réseau causal si P doit satisfaire C.

Parmi les avantages et bénéfices obtenus par l'utilisation des réseaux bayésiens se retrouvent :

- Peuvent utiliser de données partielles ou incomplètes;

- Permettent l'étude des relations causales et l'influence directe d'une variable sur l'autre;
- Combinent l'estimation d'experts et les données statistiques pour mieux évaluer la casualité permettant de mettre ensemble toutes les sources de données disponibles, subjectives aux objectives;
- Couvrent le raisonnement cause à effet de façon transparente et documentée
- Permettent l'analyse de type « what if »;
- Permettent l'acquisition, la représentation et l'utilisation de connaissance;
- Dans les dernières années, il y a une abondance d'outils et de logiciels qui permettent de saisir et traiter les réseaux bayésiens. Quelques exemples : Bayes server, Hugin, BayesNet, MSBNx.

Parmi les limitations des réseaux bayésiens se retrouvent :

- Complexité élevée d'intégration dans un cadre basé seulement sur l'opinion des experts;
- Graphes et les algorithmes de calcul peuvent être lourds dans les réseaux complexes;
- Difficultés à travailler avec les variables continues.

3.1.2 Construction

Plusieurs étapes sont à considérer dans la construction d'un réseau bayésien :

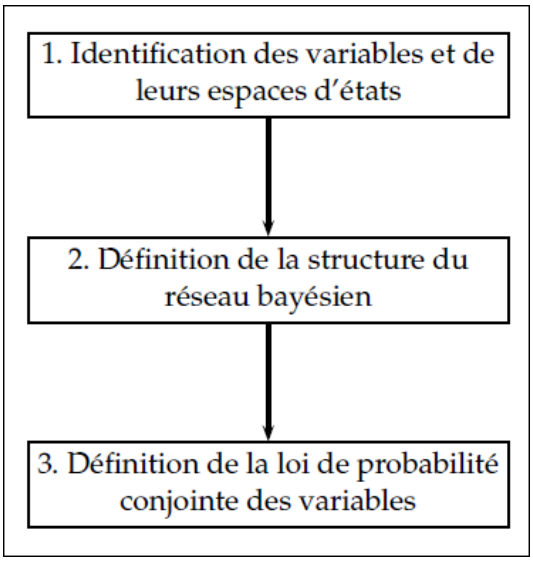

Figure 3.1 Étapes de construction d'un réseau bayésien

Source : [9, p.209]

La première étape est l'identification de variables et pour chaque variable l'ensemble de ses valeurs possibles, pour cette étape l'intervention des experts du système est toujours nécessaire.

La deuxième étape est la définition de la structure du réseau bayésien, trouver les liens d'influence entre les variables tout en s'assurant qu'il n'y a pas de boucle ou cycle. Patrick Naim mentionne que [9, p.210]: « *quelles que soient les dépendances stochastiques entre des variables, il existe toujours une représentation par réseau bayésien* »

La dernière étape vise la création des tableaux de probabilités pour les variables, soit de variables sans parentes pour lesquelles des probabilités marginales doivent être définies, soit de variables qui ont de variables partantes et, dans ce cas, de probabilités conditionnelles sont définies.

3.2 Problématique

La gestion des risques permet non seulement d'éviter ou minimiser les pertes dans le cas d'apparition d'évènements imprévus, mais aussi de saisir des opportunités d'affaires qui amènent de la valeur ajoutée.

La gestion des risques est devenue un sujet d'inquiétude encore plus élevée avec la crise économique de 2008, pour laquelle la plupart des spécialistes ont indiqué comme causes principales l'évaluation erronée et la gestion défectueuse des risques.

Le secteur TI n'a pas fait exception et la gestion des risques étais acquiescée de plus en plus dans les projets et les activités TI. Les entreprises doivent s'offrir des preuves de conformité de leurs processus. Des lois et normes sont devenues obligatoires et la gestion du risque fait partie du processus de conformité pour des entreprises. Elles doivent se conformer à CMMI ou SOX par exemple. Le centre de services informatiques est un des départements visés par les audits, car, par ces fonctions, le centre de services gère des activités reliées à la sécurité et l'intégrité des données telles que: la création et modification de comptes, les droits d'accès, les listes de distribution, les sauvegardes et transferts de données ou les mises à jour.

L'essai veut identifier les risques associés à un centre de services informatiques et trouver une méthode formelle qui peut aider dans la gestion et la mitigation de ces risques.

3.3 Méthodologie

Pour réaliser le modèle, un cadre théorique est défini. Ce cadre est la base pour les étapes requises dans le développement du modèle et il s'appuie sur des collections de bonnes pratiques autant pour le centre des services que pour la gestion du risque. Le développement du modèle est fait en utilisant des données collectées par revues de la littérature, entrevues avec des experts et des sondages.

3.3.1 Cadre théorique

Le cadre théorique présenté dans les premiers chapitres a permis de définir un centre de services dans la perspective ITIL, la présentation du cadre Risk IT développé par ISACA et la présentation succincte des réseaux bayésiens.

Centre de services ITIL

Le cadre ITIL a été choisi car il est le cadre le plus reconnu pour la gestion de services TI. Il est basé sur de meilleures pratiques et combine l'opinion des experts et la contribution de ces utilisateurs. ITIL est un cadre actif et évolutif qui couvre tous les aspects de la gestion d'un centre de services. En effet, il y a un chapitre dédié à la gestion de centre de services.
La définition et les responsabilités du centre de services ont été présentées, suivies par une classification et quelques outils pertinents.

Risk IT

Le référentiel Risk IT a été choisi pour sa facilité et la structure bien définie pour la gestion des risques. Avec ses domaines, processus et activités, Risk IT est généralement reconnu dans la littérature de spécialité comme un outil complet et efficace.
Le fait que Risk IT offre un cadre indépendant dédié à la gestion des risques, plus encore dans la gestion des risques TI, a imposé Risk IT comme un choix très pertinent pour la gestion des risques.
Lors de la rédaction de cet essai la réalisation d'essai, ISACA a publié une nouvelle version du cadre Cobit, COBIT 5 et un guide séparé pour le risque : *COBIT 5 for risk*. Cette version définit le risque informatique comme une partie intégrante des risques de l'entreprise, plus

exact le risque d'entreprise lié à l'utilisation, la possession, l'exploitation et l'adoption de l'informatique au cadre de l'entreprise.
Parce que les activités de *COBIT 5 for risk* sont en quasi-majorité les mêmes que celles du Risk IT, l'auteur a continué de se baser sur ce dernier référentiel.

Réseaux bayésiens

En cherchant une méthode formelle pour la gestion, l'utilisation des réseaux bayésiens est venue un choix naturel. Les réseaux bayésiens offrent un cadre formel, mais aussi la facilité d'apprentissage et l'adaptation aux nouvelles données ou requêtes.
Dans la littérature il existe de nombreux exemples qui présentent l'utilisation des réseaux bayésiens dans la gestion des risques dans divers secteurs tels que : financier, médical ou légal. Les réseaux bayésiens sont aussi utilisés dans le développement de logiciel, plus précisément dans les applications antivirus. Plusieurs logiciels conçus pour la représentation de réseaux bayésiens existent et cela constitue un autre avantage.

3.3.2 Processus de développement

En utilisant les notions théoriques présentées dans les chapitres précédents, la création du modèle a été réalisée en suivant les étapes :

- Identifier les risques
- Classifier les risques
- Réaliser le modèle graphique
- Choisir les risques qui seront utilisés dans le cadre du réseau bayésien
- Définir le réseau bayésien
- Valider le modèle

Identifier les risques

Pour l'identification de risques potentiels reliés au centre de services, plusieurs méthodes ont été utilisées :

- Revue de la littérature: en parcourant la littérature, une liste initiale de risques a été créée;
- Entrevues avec des experts : pendant la participation aux plusieurs séminaires et webinaires organisés par BMC, plusieurs experts ont été interrogés de façon informelle. BMC et une compagnie qui produit des logiciels pour la gestion TI et en particulier des outils de gestion pour le centre de services TI comme Remedy et Track-It!. BMC a été classifié par Gartner en août 2013 étant la seule compagnie qui touche le secteur de leader pour ITSSM [15];

  Les experts ont été interrogés sur les risques qui affectent leurs entreprises en particulier, les réponses ont été mises ensemble et la liste des risques a été créée. Cette liste n'est pas une liste exhaustive, elle est basée sur les données collectées.

Classifier les risques

Une fois les risques identifiés, un sondage a été utilisé pour les classifier. Le sondage a été réalisé par une correspondance directe avec certains experts utilisant un questionnaire à choix de réponses. Le formulaire utilisé est présenté dans l'annexe A, en français et anglais, et discuté en détail plus loin dans ce chapitre.

Dans certains cas, de rencontres et/ou entrevues téléphoniques ont été faites pour clarifier le type et niveau de service reçu et attendu, les risques connus et les méthodes de mitigation.

Le sondage et les entrevues d'après ont été utilisés pour identifier comment le type d'entreprise, y compris dimension, répartition géographique et secteur d'activité, influence ou

détermine le type, la dimension et la structure du centre de services, et plus loin les risques associés.

Réaliser le modèle graphique

Un modèle graphique a été créé en utilisant les risques identifiés. Les arcs ont été déduits en utilisant les relations logiques et les méthodes de mitigations révélées par les réponses au sondage.
Dans cette étape les nœuds n'ont pas de tableaux de probabilités associés, car utilisant le graphe au complet pour réaliser le réseau bayésien dépassait la portée de l'essai.

Choisir les risques qui seront utilisés pour modéliser le réseau bayésien

Un deuxième sondage a été publié sur Internet ou les répondants ont eu à choisir parmi les 10 options des réponses à la question : Quels sont les principaux risques qu'un gestionnaire d'un centre de services TI devrait considérer? Les répondants pouvaient aussi suggérer une autre variante de réponse. Les résultats de deux sondages ont été combinés pour choisir les risques qui ont été utilisés pour la construction du réseau bayésien.

Définir le réseau bayésien

Les risques choisis dans l'étape précédant ont été extraits du modèle graphique pour réaliser un modèle simplifié. Le graphe construit a gardé les arcs existants et des tableaux de probabilités ont été ajoutés à chaque nœud. Ces probabilités ont été calculées en utilisant les

résultats du premier sondage, plus précisément, pour chaque risque, l'impact et la probabilité d'occurrence.

Dans cette étape un accord de niveau de service (SLA) est défini en utilisant encore des normes et valeurs trouvées dans la littérature ou révélées par les entrevues avec les experts.

Le réseau bayésien construit devrait vérifier que le SLA est respecté.

Validation du modèle

La validation du modèle est faite en utilisant le logiciel AgenaRisk [13]. AgenaRisk est un logiciel intuitif conçu pour la modélisation, l'analyse et la prédiction du risque en utilisant les réseaux bayésiens.

3.4 Construction du modèle de réseau bayésien

La construction du modèle de réseau bayésien est faite dans le cadre théorique défini en suivant les étapes du processus de développement présentées dans la section précédente.

3.4.1 Identifier les risques

Dans la littérature, plusieurs risques sont récurrents, peu importe le domaine d'activité ou la structure de l'entreprise, comme le budget insuffisant ou le manque du support de la haute direction. Un budget inadéquat peut affecter un ou plusieurs services ou départements de la compagnie et le centre de services ne fait pas exception. De plus, parfois, pour les compagnies qui n'ont pas comme objet d'activité les produits TI, le département informatique est perçu comme non productif et consommateur de ressources, car le retour en investissement du

département TI n'est pas facilement quantifiable. Cela peut entrainer le manque du support de la haute direction et de la confiance de celle-là dans le centre de services.

D'autres risques sont spécifiques au TI. Ces risques ont été identifiés pendant les entrevues réalisées avec les experts et sont de risques pour lesquels les répondants ont vécu déjà des effets.

Tous les risques identifiés sont présentés et classifiés dans le chapitre suivant.

3.4.2 Classifier les risques

Pour chaque répondant au sondage, la première étape de la recherche a été l'identification de l'entreprise et du type de centre de services.
Dans le sondage, le critère d'identification des entreprises a été la dimension de l'entreprise en fonction du nombre d'employés. Le domaine d'activité des entreprises était en général connu en préalable, sinon il a été identifié par des recherches sur Internet ou par des questions adressées aux répondants au sondage.
La distribution de réponses du sondage en fonction du nombre d'employés de l'entreprise a été la suivante :

- 1 – 10 employés – 0 réponse
- 10 – 99 employés – 1 réponse
- 100 – 999 employés – 3 réponses
- 1000 – 5000 employés – 3 réponses
- 5000 – 25000 employés – 1 réponse
- Plus de 25000 employés – 1 réponse

L'entreprise avec moins de 100 employés et une des entreprises de 100 employés et plus n'avaient un centre de services dans la perspective ITIL, car ils n'ont pas un point central de

contact pour les problèmes TI. Ces entreprises utilisent un nombre très réduit d'applications. Si le logiciel est très connu, par exemple la suite Office de Microsoft, ils cherchent des solutions à leurs problèmes sur Internet. Si le logiciel est très spécifique, ils ont des contrats de service avec le producteur du ledit logiciel; c'est le cas pour des applications de comptabilité ou même de logiciels PGI. Pour leurs problèmes de matériel, ils remplacent l'équipement ou ils font appel à un service de type *geek squad*. Il existe souvent des employés qui sont considérés des experts dans certaines applications ou technologies et qui offrent leur support en fonction de leur disponibilité. La direction de ces entreprises considère que les avantages d'avoir un centre de services ne justifient pas les coûts associés.

Toutes les autres entreprises avaient un centre de services, un externe et six internes. Dans la perspective ITIL, le centre externe et un centre interne sont des centres virtuels, deux centres sont centralisés et trois centres sont décentralisés.

Dans la demande initiale, seulement le nombre approximatif de membres du centre de services était demandé, mais cela n'était pas représentatif, donc un retour a été effectué et le ratio technicien par utilisateur est demandé ou calculé. Évidemment, pour les entreprises qui n'avaient pas de centre de services, le ratio était zéro. Pour les entreprises avec centre de services externe, le ratio était inconnu. Pour les autres entreprises, ce ratio variait de 1/75 à 1/300. Ce ratio variait en fonction du secteur d'activité des entreprises et du niveau de services attendu ou requis.

Par secteur d'activité, les entreprises ont été classifiées de façon suivante :

- Communication – 1
- Transport/Automobile – 4
- Services financiers – 1
- Constructions – 1
- Minière – 2

Une fois l'identification du type d'entreprise terminée, les répondants ont eu à classifier 18 risques en fonction de leur probabilité d'occurrence et de l'impact associé, sur une échelle qui comprenait pour les deux critères quatre niveaux : bas, moyen, élevé et très élevé. Les répondants pouvaient fournir de mesures de mitigation pour chaque risque.
Les 18 risques sont présentés plus loin :

1. Personnel insuffisant – le nombre de techniciens ne correspond pas au nombre d'utilisateurs desservis, des demandes des services ne sont pas du tout traitées ou sont traitées en retard.

   Cause : la perte de personnel; la difficulté de trouver du personnel compétent; la sous-estimation des besoins.

   Mitigation: ajouter de personnel; améliorer le processus TI, quelques exemples : standardiser l'équipement, restreindre l'accès des usagers, utiliser des images, utiliser des méthodes de déploiement à distance.
2. Personnel incompétent – le personnel disponible n'a pas la capacité technique pour répondre aux demandes, barrière linguistique ou culturelle dans la communication avec les utilisateurs, la qualité de service offert est inadéquate.

   Cause : La main d'œuvre qualifiée est trop chère ou inexistante.

   Mitigation: augmenter le budget; trouver des ressources ailleurs; externaliser le service.
3. Personnel inexpérimenté / non formé – le personnel n'est pas familiarisé avec les applications et outils utilisés par l'entreprise, faible taux de résolution de problèmes.

   Cause : Roulement élevé de personnel, des techniciens juniors sont embauchés.

   Mitigation : Former le personnel.
4. Roulement élevé du personnel - le personnel ne reste pas suffisamment dans l'entreprise, les remplacements, s'ils existent, ne sont pas formés, faible taux de résolution de problèmes.

Cause : Le budget ou le milieu de travail inadéquat.

Mitigation : aligner les salaires avec le marché; réévaluer la culture de l'entreprise ou département.

5. Logiciel de gestion utilisé par le centre de services inadéquat – le logiciel utilisé pour la gestion d'incidents est inexistant ou il ne produit pas les résultats voulus, manque de cohérence dans la résolution de problèmes, de rétractabilité de problèmes, niveau bas de réutilisation de connaissances acquises, faible taux de résolution.

   Cause : Le logiciel est mal conçu pour les besoins du centre de services; le logiciel est mal utilisé.

   Mitigation : analyser et adapter le logiciel au besoin; changer le logiciel; former le personnel.

6. Outils et ressources insuffisantes – outils ou ressources non adaptés au besoin, réduisant l'efficacité du personnel et la qualité du service fourni.

   Cause : Outils obsolètes; ressources insuffisantes; ressources mal gérées; budget insuffisant.

   Mitigation : Changer/adapter les outils et les ressources utilisées.

7. Emplacement / espace bureau inadéquat – l'espace de travail est inadéquat pour l'activité du centre de services; il peut causer l'insatisfaction et l'inefficacité du personnel, affecter la qualité du service, générer un taux élevé de roulement du personnel.

   Cause : Espace insuffisant, milieu défavorable; exemples : bruit élevé, manque de confidentialité.

   Mitigation : relocaliser le centre de services.

8. Utilisateurs non expérimentés – les utilisateurs n'ont pas les connaissances nécessaires à travailler avec le matériel informatique, causant un nombre élevé d'appels de service.

   Cause : Manque de formation, processus de recrutement non adéquat.

   Mitigation : Former les utilisateurs, distribuer des procédures et manuels.

9. Logiciels / matériel non-standard – les logiciels utilisés ne sont pas les mêmes ou sont de versions différentes; les modèles des ordinateurs et des équipements périphériques varient beaucoup, difficulté à offrir ou implémenter des solutions cohérentes.

   Cause : Manque de gestion de versions; manque des standards dans le processus d'acquisition.

   Mitigation : Réduire le nombre de logiciel et versions utilisées, standardiser l'équipement acheté.
10. Manque de procédures / politiques / normes – manque de contrôle sur les logiciels et les ressources utilisées, le processus de support n'est pas cohérent, variation du niveau de service offert.

    Cause : Difficulté à établir ou implémenter de normes; budget inadéquat.

    Mitigation : Imposer des normes et politiques, créer et diffuser des procédures.
11. Infrastructure inadéquate : une source de problèmes affectant tous ou une partie d'utilisateurs, observée par la récurrence d'apparition des mêmes problèmes

    Cause : Équipement mal configuré, mises à jour non installées.

    Mitigation : Plan de maintenance pour l'infrastructure, automatisation des mises à jour.
12. Faible niveau de sécurité – perte de données, difficulté à gérer et sécuriser l'accès, problèmes causés par des intrusions comme les virus, manque de confiance dans la ressource TI.

    Cause : Système de sécurité inefficace ou désuet.

    Mitigation : Implémenter de normes de sécurité, restreindre l'accès, installer une solution antivirus adéquate
13. Manque de soutien de la haute direction – le centre de services n'est pas considéré une ressource critique de l'entreprise, le budget alloué est inadéquat, l'application des règles ou normes est difficile.

    Cause : Les TI sont considérés comme une ressource non critique par l'entreprise, insatisfaction d'usagers envers le service offert.

Mitigation : Augmenter la qualité du service, présenter à la direction les opportunités et les bénéfices apportés par le centre de services.

14. Mauvaise réputation – les utilisateurs ne font pas confiance au centre de services, utilisateurs non coopérants et réticents à l'implémentation des solutions de correction.

    Cause : Qualité du service non conforme, personnel incompétent ou non formé.

    Mitigation: Évaluer le processus de support, trouver les modalités à augmenter la qualité du service offert, mettre en place un service de suivi de la satisfaction d'utilisateurs.

15. Budget insuffisant – salaires et avantages non alignés au marché, acquisition d'équipement non performant, manque d'outils, tout se reflète dans la qualité du service offert.

    Cause : Difficultés économiques, répartition insuffisante de fonds pour le centre de services.

    Mitigation : Utilisation efficace du budget disponible, convaincre la direction à augmenter le budget.

16. Matériel informatique vieux ou obsolète – systèmes informatiques qui sont usés physiquement, taux d'appels de service élevé.

    Cause : Gestion défectueuse de l'inventaire informatique, changement de la technologie, exigences mal définies.

    Mitigation : Gestion d'inventaire considérant la durée de vie normale de l'équipement, recyclage d'équipement obsolète, implémenter des normes et procédures pour définir les besoins et adapter le parc informatique en conséquence.

17. Mauvaise documentation – systèmes et applications non documentés, utilisateurs non formés sur les outils de travail, nombre élevé d'appels de service, réutilisation faible de connaissances.

    Cause : Documentation non existante ou publiée/partagée de façon inadéquate.

    Mitigation : Créer des procédures, former les techniciens et former les utilisateurs.

18. Communication insuffisante – manque de communication avec les utilisateurs ou la direction, procédures et documentation mal distribuées, mauvaise réputation du TI.
    Cause : Gestion de la communication déficitaire, manque d'outils de communication.
    Mitigation : Implémenter un plan de communication, réaliser ou mettre à jour des outils de communication : site Intranet, courriel d'information, matériel publicitaire.

3.4.3 Le modèle graphique

Les 18 risques ont été mis ensemble dans un graphe acyclique présenté dans la figure 3.3.
Les arcs représentent l'influence unidirectionnelle logique entre ces risques en considérant les mesures de mitigation mentionnées dans les sondages et les suivis à ces sondages. Les effets causés par la matérialisation de ces risques sont reflétés finalement dans le niveau de service offert par le centre de services.

Parmi les indicateurs clés de performance du centre de services se retrouvent :

- Temps de réponse aux incidents – le délai entre le moment où l'utilisateur a communiqué le problème et le moment où un technicien a commencé le processus de diagnostic et résolution
- Temps de résolution d'incidents – le délai entre le moment où le technicien a commencé le processus de diagnostic et résolution et le moment où l'utilisateur a validé et accepté la résolution.
- Nombre des incidents récurrents – incidents qui sont rapportés de nouveau après qu'une solution a été fournie
- Taux de satisfaction d'utilisateurs – est mesuré par des sondages concernant la satisfaction du client en rapport avec la clarté de la solution, les délais, la communication ou l'effort requis.

Le graphe réalisé sera utilisé dans la construction du modèle de réseau bayésien.

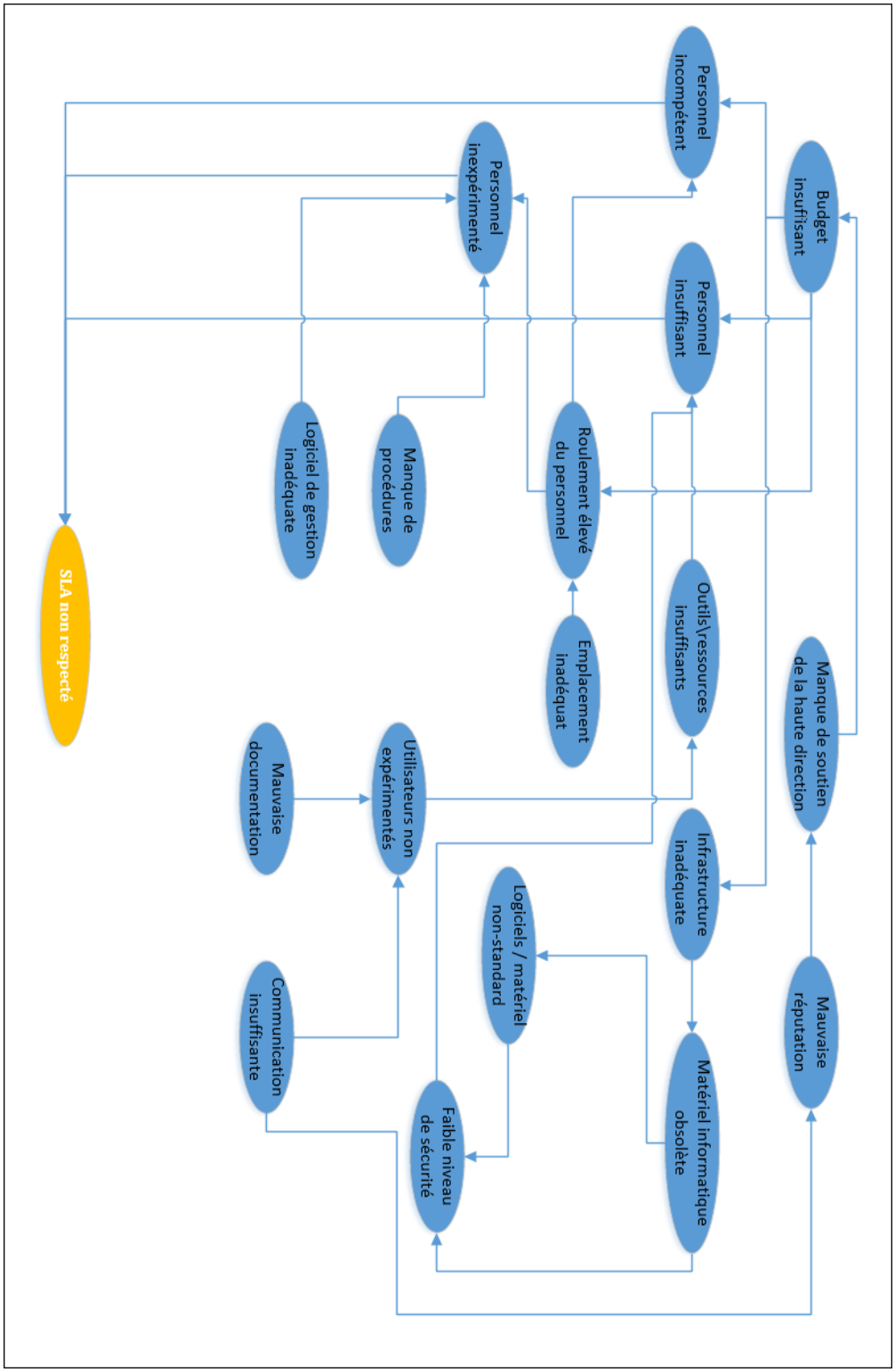

Figure 3.2 Modèle graphique

3.4.4 Choisir les risques

Même si le modèle graphique pouvait constituer la base pour réaliser le modèle du réseau bayésien, la complexité dépassait la portée de l'essai, donc seulement 5 risques sont retenus.
Dans les sondages les répondeurs ont eu à indiquer, pour chaque risque, la probabilité d'occurrence et l'impact. En utilisant ces options, un score a été calculé de façon suivante pour chaque risque :

$$\text{Score Risque} = \text{ProbF} \times 1 + \text{ProbM} \times 2 + \text{ProbE} \times 3 + \text{ProbTE} \times 4 + \text{ImpF} \times 1 + \\ + \text{ImpM} \times 2 + \text{ImpE} \times 3 + \text{ImpTE} \times 4$$

tel que :

ProbF – nombre de votes pour une probabilité faible
ProbM – nombre de votes pour une probabilité moyenne
ProbE – nombre de votes pour une probabilité élevée
ProbTE – nombre de votes pour une probabilité très élevée
ImpF – nombre de votes pour un impact faible
ImpM – nombre de votes pour un impact moyen
ImpE – nombre de votes pour un impact élevé
ImpTE – nombre de votes pour un impact très élevé

Les résultats sont présentés dans le tableau 3.1 :

Tableau 3.1 Score des risques

Risque	Probabilité d'occurrence				Impact				Score
	Faible	Moyenne	Élevée	Très élevée	Faible	Moyen	Élevé	Très élevé	
Roulement élevé du personnel	x	xxxx	x	xxx		xxx	xxxxx	x	49
Infrastructure inadéquate	xxx	xxxx	xx				xxxxx	xxxx	48
Manque de procédures / politiques / normes	xxx	xxx	xxx			x	xxxx	xxxx	48
Manque de soutien de la haute direction	x	xxxxxx	xx			x	xxxxx	xxx	48
Utilisateurs non expérimentés	xx	xx	xxx	xx	x	xx	xxxx	xx	48
Personnel insuffisant	x	xxxxxx	xx			x	xxxxxx	xx	47
Budget insuffisant	xx	xx	xxx	xx	x	xx	xxxxxx		46
Matériel informatique vieux ou obsolète	xxxx	xx	xxx		x		xxxx	xxxx	46
Personnel inexpérimenté / non formé	x	xxxxxx	xx			xx	xxxxx	xx	46
Outils et/ou ressources insuffisants	xx	xxxxx		xx	x	xx	xxxxx	x	44
Faible niveau de sécurité	xxxx	xxx	xx			xx	xxxxx	xx	43
Logiciels / matériel non-standard		xxxxxxx	x	x	x	xxxx	xxx	x	43
Communication insuffisante	xxx	xxx	xx	x	x	xxxx	xxx	x	41
Mauvaise documentation	xx	xxx	xxxx			xxxxxx	xxx		41
Personnel incompétent	xxxxxxx	xx				x	xxxx	xxxx	41
Mauvaise réputation	xxxx	xxxx		x		xxxxx	xx	xx	40
Logiciel de gestion inadéquate utilisé par le centre de service	xxxxxx	xxx				xxxxxxx	xx		32
Emplacement / espace bureau inadéquat	xxxxxx	xxx			xxxxxx	xxx			24

En prenant les 10 premiers risques, un deuxième sondage a été réalisé sur Internet, un sondage seulement quantitatif, les répondants ayant à répondre à la question : *Quels sont les principaux risques qu'un gestionnaire d'un centre de services TI devrait considérer?* Les premiers cinq risques de ce sondage ont été choisis pour la construction du réseau bayésien.

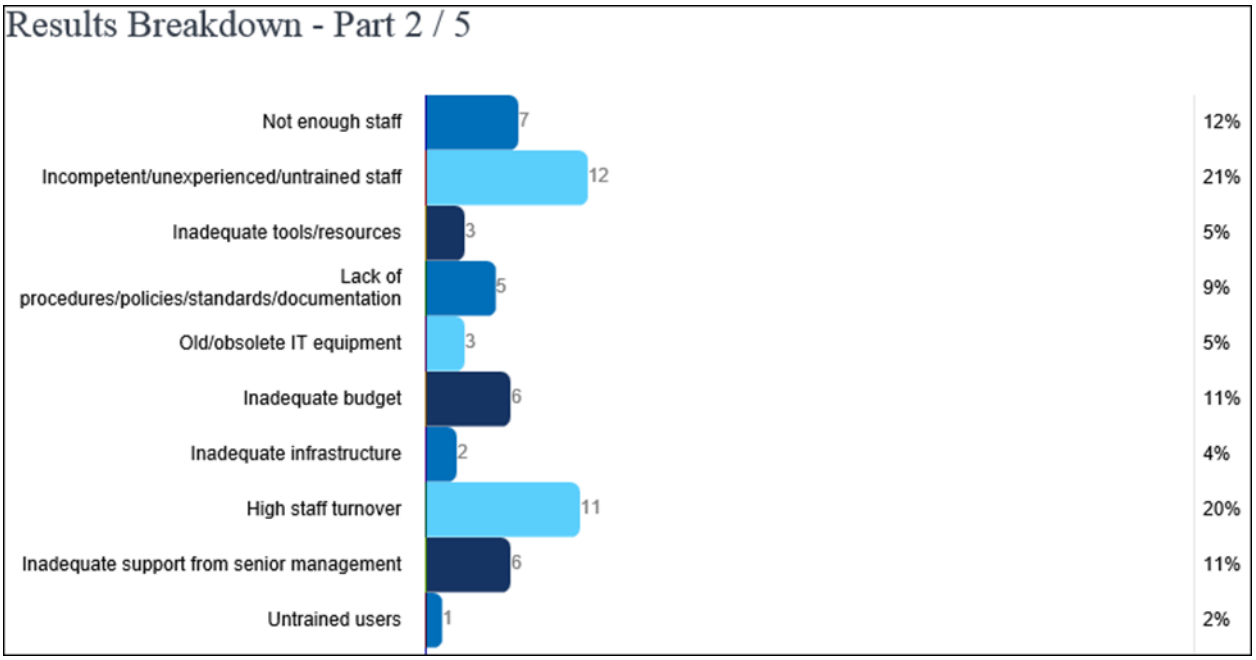

Figure 3.3 Résultats sondage Internet

3.4.5 Le modèle de réseau bayésien

Les risques suivants ont été choisis pour la construction du modèle de réseau bayésien:

- Personnel inexpérimenté
- Roulement élevé du personnel
- Personnel insuffisant
- Budget insuffisant
- Manque de soutien de la haute direction

Les cinq risques ont été extraits du graphe initial et un nouveau graphe a été réalisé :

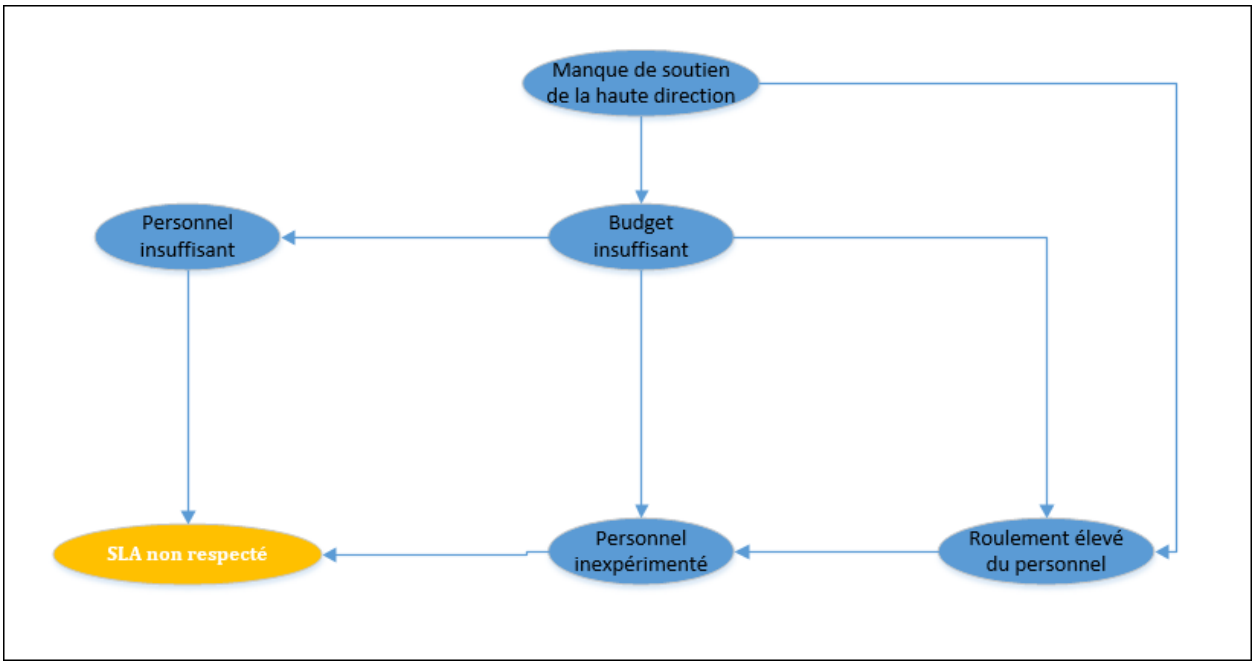

Figure 3.4 Modèle de réseau bayésien

Dans la section suivante, des tableaux de probabilités sont définis pour tous les nœuds. Pour le nœud sans parent, une distribution marginale est utilisée; pour les nœuds avec des parents, des équations déterministes sont utilisées, ensuite elles doivent être converties en probabilités [9, p. 211]. Pour chaque équation, une valeur initiale P0( ) est introduite et elle est obtenue en utilisant l'opinion des experts ou des données statistiques. Les coefficients dans chaque équation sont des probabilités d'inférence et ils sont estimées en se basant sur les observations cause/effet révélées par les sondages avec les experts.

Le manque de soutien de la haute direction

Plusieurs facteurs peuvent déterminer la haute direction de ne pas soutenir le centre de services :

- Rendement réduit du centre de services
- Utilisation limitée des TI dans l'activité de l'entreprise

- Manque de clarté ou incohérence relativement aux attentes
- Une mauvaise réputation qui peut être déterminée par les facteurs mentionnés avant, par la culture organisationnelle ou d'autres facteurs subjectifs

Le manque de soutien de la haute direction a comme conséquences l'assignation d'un budget limité et parfois l'exclusion des gestionnaires TI du processus de prise de décision. Les gestionnaires peuvent avoir des difficultés à faire approuver et implémenter des solutions ou projets, d'assurer les ressources nécessaires telles que l'espace de travail, les outils ou les technologies. Dans ce cas la satisfaction des employées est affectée et elle entraîne le roulement élevé du personnel.

Le premier domaine de Risk IT, la gouvernance du risque, offre des processus et activités pour mettre en place une structure qui peut éliminer ou diminuer les facteurs négatifs et formaliser les attentes de l'entreprise envers le centre de services.

Le tableau de probabilité associé à ce nœud contient la distribution suivante, les états seront utilisés pour le modèle, mais, au besoin, des états différents peuvent être ajoutés. Quelques exemples de valeurs sont donnés dans le tableau 3.2 :

Tableau 3.2 Tableau probabilités marginales pour le soutien de la haute direction

Soutien de la haute direction	Vrais	Faux
Nul	0	1
Faible	0.25	0.75
Moyen	0.5	0.5
Fort	0.75	0.25
Total	1	0

Budget insuffisant

Le budget du centre de services peut être influencé de plusieurs facteurs internes ou externes :

- Marché difficile

- Secteur d'activité en difficulté
- Utilisation inefficace de ressources
- Ressources disponibles et/ou nécessaires mal évaluées

Le budget du centre de services est directement influencé par le budget de l'entreprise. Toutefois, l'importance du centre de services dans la vision des facteurs décisionnels peut influencer le budget alloué au centre de services. Le tableau de probabilités conjointes associé à ce nœud est défini à l'aide de l'équation déterministe suivante :

$$P(Budget/Soutien\ HD) = P0(Budget)\ x\ (0.75 + 0.25*Soutien\ HD)$$

Quelques exemples sont présentés plus bas :

Tableau 3.3 Exemples valeurs nœud Budget insuffisant

Budget		Soutien HD		Vrai	Faux
Bas	0.25	Moyen	0.5	0.22	0.78
Bas	0.25	Fort	0.75	0.23	0.77
Élevé	0.75	Faible	0.25	0.61	0.39
Élevé	0.75	Fort	0.75	0.7	0.3
Moyen	0.5	Moyen	0.5	0.44	0.56
Moyen	0.5	Fort	0.75	0.47	0.53
Très Élevé	1	Faible	0.25	0.81	0.19
Très Élevé	1	Total	1	1	0

Roulement élevé du personnel

Le centre de support est un des départements le plus affectés par le roulement élevé de personnel. Des études effectuées pour les centres d'appel ont révélé un taux de roulement entre 30 et 45 pour cent [12].

Plusieurs facteurs déterminent cela :

- Salaires et avantages peu motivants
- Départ pour le développement de carrière
- Stress
- Routine des tâches
- Recrutement difficile

Le roulement élevé détermine des coûts plus élevés pour former les nouveaux employés qui demandent aussi un grade de supervision plus élevé, voir coûts additionnels. Les nouveaux employés sont peu expérimentés, ils sont plus lents au début et ils commettent plus des erreurs, ce qui diminue l'efficacité et augmente le taux d'insatisfaction.

En suivant les activités de Risk IT, les gestionnaires doivent s'assurer que l'entreprise est informée, que la direction comprend les effets de ce risque, que les seuils de tolérance sont acceptés et que des activités de réponse sont mises en place :

- Ajuster les salaires et bonifications pour rester compétitive au marché de travail
- Assurer un milieu de travail motivant et une atmosphère conviviale
- Créer de plans de formation et de développement de carrière
- Améliorer le processus de recrutement en fournissant de descriptions de poste claires et rechercher de candidats compétents

L'équation déterministe est présentée plus bas. Budget et Soutien HD sont les valeurs de nœuds *Budget insuffisant* et respectivement *Manque de soutien de la haute direction.*

$$P(Roulement/Budget/Soutien\ HD) = P0(Roulement)\ (0.65 + 0.25 \times P(Budget) + 0.1 \times Soutien\ HD)$$

Personnel insuffisant

Le manque de personnel est causé par deux facteurs : les départs et la difficulté à recruter.
Les facteurs déterminants pour les départs sont encore :

- Salaires et avantages peu motivants
- Le développement de carrière
- Stress
- Routine des tâches

Le recrutement est influencé par :

- Les conditions financières et les avantages offerts
- Le milieu de travail : réputation de l'entreprise, localisation, accessibilité, horaire de travail
- La formation, la possibilité d'avancement et le développement de carrière
- La disponibilité de la main-d'œuvre sur le marché de travail

L'équation suivante calcule les probabilités conjointes pour ce nœud :

$$P(Pers\_Suf, Budget) = P0(Pers\_Suf) \times (0.5 + 0.5 \times P(Budget))$$

Personnel inexpérimenté

Le personnel inexpérimenté est causé par quelques facteurs :

- Le budget insuffisant : dans le processus de recrutement, même si des ressources sont disponibles sur le marché, un budget restreint ne permet pas de recruter du personnel haut qualifié ou expérimenté;

- Le roulement élevé : même si l'entreprise a un plan de formation adéquat, le changement de personnel régulier ne permet pas une formation efficace et complète;
- Formation inadéquate : le personnel n'est pas formé adéquatement.

L'équation déterministe suivante est utilisée pour le calcul de probabilités conjointes :

$$P(Pers\_Exp, Budget, Roulement) = P0(Pers\_Exp) \times (0.5 + 0.3 \times P(Budget) + 0.2 \times P(Roulement))$$

SLA non respecté

Ce nœud est représenté par une valeur qu'on détermine utilisant les quatre indicateurs suivants. Pour chacun, une valeur P0( ) est introduite, elle est obtenue des données statistiques.

Les valeurs des quatre ICP sont calculées avec des équations déterministes, les coefficients sont de probabilités d'inférence des nœuds Personnel Insuffisant (Pers_suf) et Personnel inexpérimenté (Pers_exp), ils sont approchés en se basant sur les observations cause/effet révélées par les sondages avec les experts.

Le temps de réponse aux incidents : est directement influencé par le nombre de techniciens disponibles qui répondent aux appels, mais aussi par le temps de résolution et/ou de dépannage initial. Si les techniciens ne sont pas expérimentés, des délais significatifs peuvent arriver.

$$P(TRep/Pers\_Suf/Pers\_Exp) = P0(TRep) \times (0.5 + 0.3 \times Pers\_suf + 0{,}2 \times Pers\_exp)$$

Temps de résolution d'incidents : similaire au temps de réponse, le temps de résolution est influencé par le nombre de techniciens disponibles et par leurs compétences.

$$TRes = P0(TRes) \times (0.34 + 0.33 \times Pers\_suf + 0{,}33 \times Pers\_exp)$$

Nombre des incidents récurrents : si le nombre des techniciens est limité, ils sont obligés à traiter plus d'appels et de réduire le temps alloué pour la résolution, cela peut introduire des erreurs ou des solutions incomplètes. Si les techniciens sont inexpérimentés, la probabilité d'occurrence de ces erreurs est encore plus élevée.

$$TRec = P0(TRec) \times (0.7 + 0.1 \times Pers\_suf + 0{,}2 \times Pers\_exp)$$

Taux de satisfaction d'utilisateurs : les déviations des trois critères antérieurs génèrent l'insatisfaction d'utilisateurs. Le taux d'insatisfaction est mesuré par de sondages dans lesquels plusieurs catégories sont offertes aux répondants, catégories qui vont en général de *totalement insatisfait* à *totalement satisfait* avec plusieurs valeurs intermédiaires. En fonction de SLA, un seuil d'acceptation est défini, par exemple tous les incidents pour lesquels la solution offerte a été au moins satisfaisante.

$$TSat = P0(TSat) \times (0.8 + 0.1 \times Pers\_suf + 0{,}1 \times Pers\_exp)$$

La valeur du nœud SLA est obtenue avec la formule :

$$SLA = (TRep > TRepSLA) \cap (TRes > TResSLA) \cap (TRec > TRecSLA) \cap (TSat > TSatSLA)$$

TRepSLA, TResSLA, TRecSLA et TSatSla sont les pourcentages prévus dans SLA pour le temps de réponse, le temps de résolution, les incidents récurrents et le taux de satisfaction.
Des exemples complets seront offerts dans la section suivante.

3.4.6 Validation du modèle

Le modèle de réseau bayésien a été refait utilisant AgenaRisk Lite [13], les nœuds et les liens ont été définis, les formules présentées plus haut ont été introduites. Le logiciel a validé la structure du réseau bayésien y compris les liens entre les nœuds ainsi que la cohérence des formules déterministes.

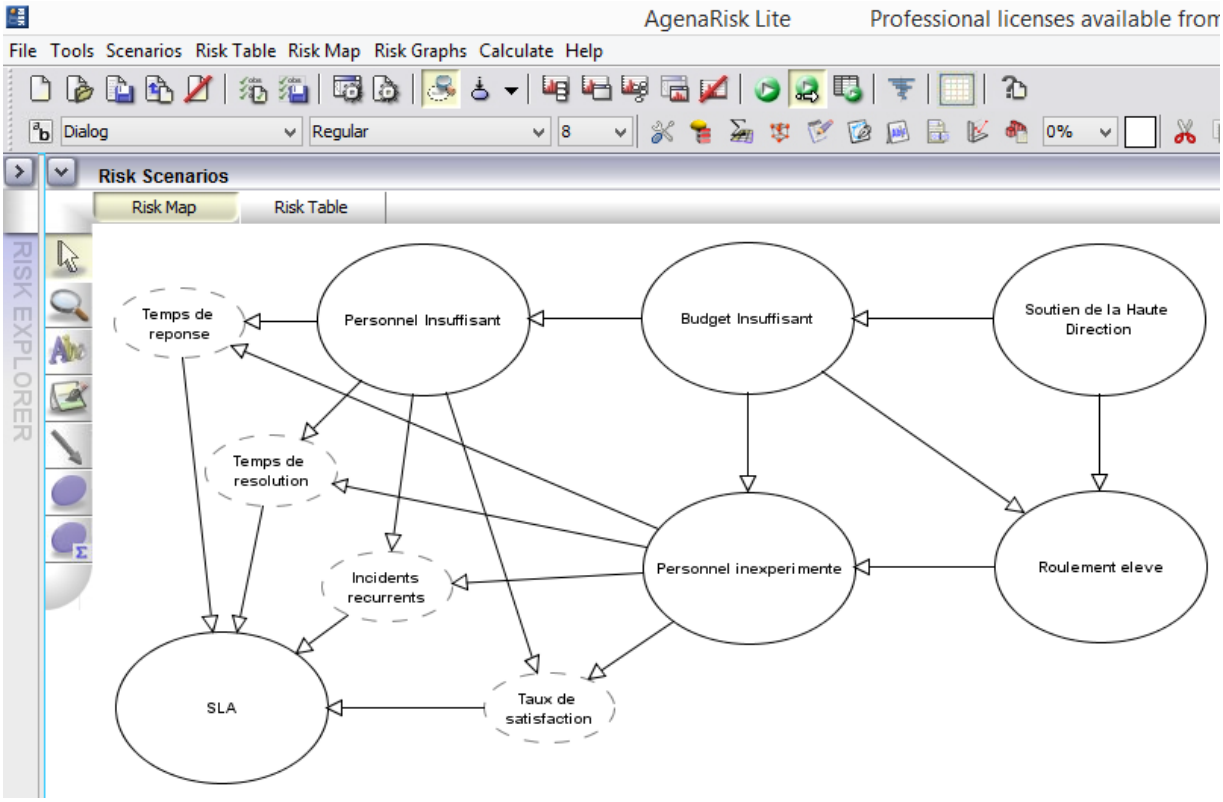

Figure 3.5 Le modèle de réseau bayésien dans AgenaRisk

Exemples

Le modèle est validé avec deux exemples. Le logiciel AgenaRisk a généré plusieurs erreurs à cause de quelques bogues connus pour cette version, donc une méthode manuelle de calcul est utilisée pour démontrer l'inférence et la propagation dans le modèle bayésien.

Dans le premier exemple, un exemple de type what-if , toutes les hypothèses suivantes sont vraies, elles sont basées sur le centre de services d'une entreprise réelle:

- La haute direction est satisfaite de l'activité du centre de services, elle offre un support total.
- Le personnel du centre de services est suffisant, personne n'a quitté dans le dernier an, tous les techniciens ont suivi les formations requises par leurs postes
- Le SLA est respecté, les ICP sont dépassés. Les ICP définies dans SLA pour le temps de réponse, temps de résolution, incidents récurrents et taux de satisfaction sont : 90 %, 85 %, 98 % et 90 %. Pour cette mise en situation les pourcentages statistiques sont : 95, 90, 99,5 et 95 respectivement.

Dans cet environnement un facteur de risque potentiel est introduit: la compagnie traverse une période financière difficile et la haute direction décide de couper le budget par 25 %.

Les valeurs suivantes sont obtenues :

Tableau 3.4 Exemple "what-if"

Nœud	Variable Entrée		Équation déterministe	Variable Sortie	
	Nom	Valeur		Nom	Valeur
Manque de soutien de la haute direction	Soutien HD	1	Soutien Total de la Haute direction	Soutien HD	1.00
Budget insuffisant	P0(Budget)	**0.75**	P(Budget/Soutien HD) = P0(Budget) x (0.75 + 0.25 x Soutien HD)	Budget	0.75
Roulement élevé du personnel	P0(Roulement)	1	P (Roulement/Budget/Soutien HD) = P0(Roulement) (0.65 + 0.25 x P(Budget) + 0.1 x Soutien HD	Roulement	0.94
Personnel insuffisant	P0(Pers_Suf)	1	P(Pers_Suf, Budget) = P0(Pers_Suf) x (0.5 + 0.5 x P(Budget))	Pers_suf	0.88
Personnel inexpérimenté	P0(Pers_Exp)	1	P(Pers_Exp, Budget, Roulement) = P0(Pers_Exp) x (0.5 + 0.3 x P(Budget) + 0.2 x P (Roulement))	Pers_exp	0.91
SLA	P0(TRep)	0.95	TRep = P0(TRep) x (0.5 + 0.3 x Pers_suf + 0,2 x Pers_exp)	TRP	0.90
	P0(TRes)	0.9	TRes = P0(TRes) x (0.34 + 0.33 x Pers_suf + 0,33 x Pers_exp)	TRS	**0.84**
	P0(TRec)	0.995	TRec = P0(TRec) x (0.7 + 0.1 x Pers_suf + 0,2 x Pers_exp)	TRC	**0.97**
	P0(TSat)	0.95	TSat = P0(TSat) x (0.8 + 0.1 x Pers_suf + 0,1 x Pers_exp)	TST	0.93
	SLA	TRUE	(TRep > 0.9) Λ (TRes > 0.8) Λ (TRec > 0.98) Λ (TSat > 0.9)	SLA	**FALSE**

On observe que les ICP ont baissé et deux entre eux ne correspondent plus au SLA. On peut supposer que la réduction du budget a généré de réduction de personnel ou de remplacements de personnes qualifiées par de personnel moins qualifié. Cela est reflété dans les valeurs de deux nœuds Personnel Insuffisant et Personnel Inexpérimenté.

Dans l'analyse de type « *what-if* » les gestionnaires peuvent utiliser plusieurs scénarios et décider sur l'acceptabilité des mesures de mitigation qui s'imposent en fonction de l'impact du risque introduit sur les autres indicateurs. Si les scénarios de risque se matérialisent, ces résultats doivent être enregistrés dans le catalogue des risques en concordance avec les processus et les activités de Risk IT et, si nécessaire, les tableaux de probabilités du réseau bayésien sont ajustés.

Un deuxième exemple est basé sur des données statistiques. L'environnement correspond à une entreprise réelle pour laquelle toutes les données statistiques sont déjà connues : la compagnie a un centre de services efficace, le personnel est expérimenté et le nombre de techniciens adéquat, le budget et suffisant, la haute direction offre tout le support nécessaire. Les ICP sont le même que ceux utilisés dans l'exemple antérieur. On introduit maintenant un facteur de risque : la non-disponibilité d'une partie de personnel de centre de risque. Dans cet exemple apparait un évènement qui s'est déjà passé et pour lequel on a déjà de statistiques montrant l'impact : pendant les mois de juillet et deux semaines d'aout 2013, le centre de services a perdu 28 % de son personnel dû à un congé de paternité et des vacances. Ces données sont introduites dans le modèle et sont comparées avec la statistique réelle.
Voici les valeurs obtenues avec le modèle :

Tableau 3.5 Exemple a posteriori

Nœud	Variable Entrée		Équation déterministe	Variable Sortie	
	Nom	Valeur		Nom	Valeur
Manque de soutien de la haute direction	Soutien HD	1	Soutien Total de la Haute direction	Soutien HD	1.00
Budget insuffisant	P0(Budget)	1	P(Budget/Soutien HD) = P0(Budget) x (0.75 + 0.25 x Soutien HD)	Budget	1.00
Roulement élevé du personnel	P0(Roulement)	1	P (Roulement/Budget/Soutien HD) = P0(Roulement) (0.65 + 0.25 x P(Budget) + 0.1 x Soutien HD	Roulement	1.00
Personnel insuffisant	P0(Pers_Suf)	**0.72**	P(Pers_Suf, Budget) = P0(Pers_Suf) x (0.5 + 0.5 x P(Budget))	Pers_suf	0.72
Personnel inexpérimenté	P0(Pers_Exp)	1	P(Pers_Exp, Budget, Roulement) = P0(Pers_Exp) x (0.5 + 0.3 x P(Budget) + 0.2 x P (Roulement))	Pers_exp	1.00
SLA	P0(TRep)	0.95	TRep = P0(TRep) x (0.5 + 0.3 x Pers_suf + 0,2 x Pers_exp)	TRP	**0.87**
	P0(TRes)	0.9	TRes = P0(TRes) x (0.34 + 0.33 x Pers_suf + 0,33 x Pers_exp)	TRS	**0.82**
	P0(TRec)	0.995	TRec = P0(TRec) x (0.7 + 0.1 x Pers_suf + 0,2 x Pers_exp)	TRC	**0.97**
	P0(TSat)	0.95	TSat = P0(TSat) x (0.8 + 0.1 x Pers_suf + 0,1 x Pers_exp)	TST	0.92
	SLA	TRUE	(TRep > 0.9) Λ (TRes > 0.8) Λ (TRec > 0.98) Λ (TSat > 0.9)	SLA	**FALSE**

Les ICPs pour le temps de réponse et le délai de résolution ne correspondent plus au SLA, donc le SLA n'est plus respecté.

Le rapport présenté dans la Figure 3.6 est fourni par le logiciel Track-IT!, il est basé sur des données statistiques d'une entreprise pour une période de six mois, de juin à novembre 2013. Dans le graphique s'observe que le temps de résolution a augmenté de 30 % au mois de juillet ce qui a déterminé un manque de conformité au SLA pour environ 21 % des incidents, 279 incidents avec un délai de résolution dépassé d'un total de 1343 incidents fermés. Pour le même mois, le pourcentage calculé pour les incidents récurrents a été de presque 4 %, 52 incidents rouverts de 1343 incidents fermés.

Les résultats calculés à l'aide du réseau bayésien en utilisant les équations déterministes reflètent la tendance dans la statistique réelle. On observe que les valeurs obtenues sont comparables, si les tableaux de probabilités conjointes sont générés et ajustés en conséquence, ces résultats deviennent encore plus précis.

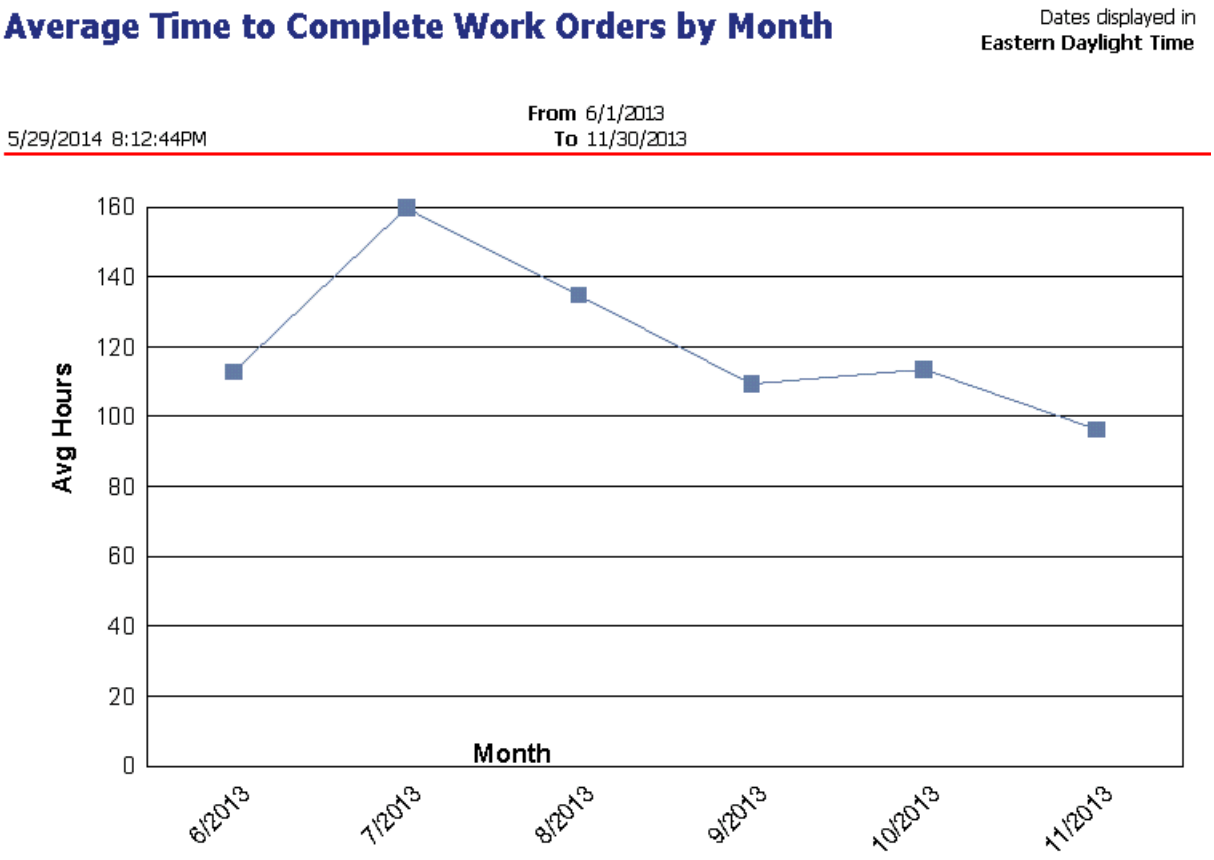

Figure 3.6 Temps moyen pour fermer des incidents (extrait du logiciel Track-It!)

Avec les résultats obtenus en utilisant le modèle de réseau bayésien les gestionnaires peuvent utiliser les activités de Risk IT et ITIL pour appliquer des actions de traitement du risque et même d'amélioration du processus de la gestion du centre de services.

Conclusions

Lors des entrevues avec les experts, un des problèmes mentionnés souvent est la faible importance accordée à la gestion du risque dans le secteur de services. La gestion du risque fait partie de la plupart de projets, mais ce n'est pas une priorité dans la gestion des services informatiques.

Le modèle construit vient à l'aide des gestionnaires en offrant des solutions pour l'identification et la classification des risques surtout au niveau de l'impact et de la probabilité d'occurrence pour les risques identifiés.

Le modèle n'est pas conçu comme un outil indépendant, mais comme un outil intégré avec les bonnes pratiques d'ITIL et Risk IT. Les dernières versions d'ITIL mettent l'accent sur le cycle de vie des services, les bonnes pratiques visent le développement continu du service en améliorant l'expérience du client, dans ce cas-ci, l'utilisateur du système informatique de l'entreprise. Risk IT est toujours connecté au besoin de l'entreprise et, comme ITIL, il propose aussi un processus continu.

Les étapes utilisées dans la construction du modèle ont été conçues en lien avec les activités d'ITIL et Risk IT. Par exemple, l'identification des risques est une partie intégrante du domaine d'évaluation du risque du Risk IT. Une fois les risques identifiés, il faut les ajouter dans le registre des risques et passer ensuite aux activités du domaine de traitement du risque. Toutefois, l'intégration avec toutes les activités d'ITIL et/ou Risk IT dépasse la portée de l'essai.

L'identification des risques montre que les risques, ou la perception de ces risques sont différents d'une entreprise à l'autre. Des risques qui sont considérés critiques pour une

entreprise sont considérés négligeables par une autre entreprise. Cela dépend de la taille de l'entreprise, du secteur d'activité, du type de centre de services, mais finalement c'est une question subjective pour chaque gestionnaire.

La liste des risques identifiés est loin d'être exhaustive, d'autres risques ont été identifiés pendant la réalisation de cet essai, mais, comme la liste été déjà trop complexe, ils n'ont pas été inclus: des risques reliés à l'économie globale, des risques environnementaux, des risques politiques ou légaux.

Le modèle de réseau bayésien a été réalisé en fonction de réponses reçues pendant l'étape de collecte de données. Il peut être utilisé comme tel ou adapté en fonction des besoins. Les valeurs utilisées sont des suggestions, mais elles sont basées sur les valeurs d'une entreprise réelle. À titre d'exemple, les valeurs des indicateurs clés de performance peuvent être plus exigeantes pour certaines entreprises, cela dépend encore de plusieurs facteurs, comme le secteur d'activité.

Le logiciel utilisé, AgenaRisk, a fonctionné correctement jusqu'à un point où des erreurs système ont été reçues. Certains bogues ont été rapportés comme connus et réglés par le fournisseur dans les versions plus récentes, mais malheureusement la version « *Lite* » utilisée ne supporte pas des mises à jour. L'utilisation d'une version serveur ou professionnelle peut constituer une prochaine phase et dans ce cas plusieurs nœuds, voir risques, peuvent être ajoutés au modèle. Un autre élément qui manque et qui peut constituer un développement ultérieur est l'apprentissage pour le réseau bayésien.

Le modèle réalisé a été utilisé en production en mode expérimental, les données obtenues ne se sont pas concrétisées dans des actions jusqu'ici car plusieurs validations sont encore nécessaires avant de le mettre en production. L'auteur est toutefois convaincu que ce modèle est une bonne base qui, avec certaines adaptations, peut être utilisée dans la gestion des risques dans la gouvernance d'un centre de services informatiques.

Liste des références

[1] Union internationale des télécommunications, http://www.itu.int/wsis/index-fr.html, 12 septembre 2013

[2] Union internationale des télécommunications, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, 12 Septembre 2013

[3] IBM, http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html, 11 Novembre 2013

[4] IBM, http://www-01.ibm.com/software/data/bigdata/industry.html, 11 Novembre 2013

[5] Van Bon, J., Gestion des services informatiques, une introduction basée sur l'ITIL, 1er éd., Van Haren Publishing, Zeewolde, 2005, 237 p.

[6] Schwalbe, K., Information Technology Project Management, 7eme éd., Course Technology, Boston, 2012, 528 p.

[7] ISACA, COBIT 5 Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise, ISACA, Rolling Meadows, 2012

[8] ISACA, The Risk IT Framework, ISACA, Rolling Meadows, 2009

[9] Naïm, P., Wuillemin, P., Leray, P., Pourret, O., Becker, A., Réseaux bayésiens, 3e éd., Eyrolles, Paris, 2007, 424 p.

[10] Koski, M., Noble, J.M., Bayesian Networks, John Wiley & Sons, Chichester, 2009, 356 p.

[11] Holmes, D., Jain, L., Innovations in Bayesian Networks, Springer, Heidelberg, 2008, 317 p.

[12] Cincom, http://cds.cincom.com/?elqPURLPage=26, 11 Mai 2014

[13] Agena. http://www.agenarisk.com/, 14 Mars 2013

[14] Fenton, N., Neil, M., Risk Assessment and Decision Analysis with Bayesian Networks, CRC Press, Boca Raton, 2012

[15] BMC, https://communities.bmc.com/community/bsm_initiatives/itsm/blog/2013/10/17/bmc-highest-rated-itssm-vendor-for-completeness-of-vision, 01 Mars 2014

[16] ITSM Portal, http://www.itsmportal.com/columns/itil-meets-risk-management#.U4M7t_ldVl0, 20 mai 2014

Annexe 1

Formulaire sondages français

Identifications des risques pour un centre de services

Le formulaire suivant est utilisé comme un outil pour identifier et classifier les risques associés à la gestion d'un centre de services TI (Help Desk, centre d'appels ou autre). Quelques risques ont été identifiés, s'il vous plaît évaluez-les et n'hésitez pas à ajouter d'autres risques à votre discrétion

S'il vous plaît notez que les résultats sont utilisés seulement dans la rédaction de mon essai académique

S'il vous plaît remplissez le formulaire ci-dessous et me le retournez par courriel à l'adresse suivante : cristich@yahoo.com.

Nom												
Entreprise												
Titre												
Dimension de l'entreprise (nombre des employés)	1 - 10		10 - 99		100 - 999		1000 - 5000		5000 - 25000		Plus que 25000	
Type de centre de services	Aucun		Interne		Extern							
Dimension du centre de services (nombre des employés)	1 à 3		4 à 10		10 à 30		30 à 100		100 à 1000		Plus que 1000	

Risque	Probabilité d'occurrence				Impact				Mesures de mitigation/Commentaires
	bas	moyen	élevé	très élevé	bas	moyen	élevé	très élevé	
Personnel									

insuffisant									
Personnel incompétent									
Personnel inexpérimenté / non formé									
Roulement élevé du personnel									
Logiciel de gestion utilisé par le centre de services inadéquat									
Outils et/ou ressources insuffisantes									
Emplacement / espace bureau inadéquat									
Utilisateurs non expérimentés									
Logiciels / matériel non-standard									
Manque de procédures / politiques / normes									
Infrastructure inadéquate									
Faible niveau de sécurité									

Manque de soutien de la haute direction									
Mauvaise réputation									
Budget insuffisant									
Matériel informatique vieux ou obsolète									
Mauvaise documentation									
Communication insuffisante									
Risque	Probabilité d'occurrence				Impact				
	bas	moyen	élevé	très élevé	bas	moyen	élevé	très élevé	

Annexe 2

Formulaire sondages anglais

Service Desk Risks Identification

The following form is used as a tool to identify the risks associated with the management of an IT Service Desk (Help Desk, Call Center or other). Few standard risks have been identified, please rate them and feel free to add other risks on the list at your discretion

Please note the results are going to be used only as a baseline for an academic thesis.

Please fill in the form below and return it to me by email at the following address: cristich@yahoo.com.

Name (optional)												
Company (optional)												
Title												
Company size (number of employees)	1 - 10		10 - 99		100 - 999		1000 - 5000		5000 - 25000		more than 25000	
Service Desk Type	None		Internal		External							
Service Desk Size (number of employees)	1 to 3		4 to 10		10 to 30		30 to 100		100 to 1000		more than 1000	

Risk	Probability of occurrence				Impact				Mitigation/Comments
	Low	Medium	High	Very High	Low	Medium	High	Very High	
Not enough staff									
Incompetent staff									
Unexperienced/un									

trained staff									
High staff turnover									
Inadequate Service Center management software									
Inadequate tools/resources									
Inadequate location/ office space									
Untrained users									
Non-standard software/hardware									
Lack of procedures/ policies/standards									
Inadequate infrastructure									
Weak security									
Inadequate support from senior management									
Bad reputation									
Inadequate budget									
Old/obsolete IT equipment									
Poor documentation									

Inadequate communication									
Risk	Probability of occurrence				Impact				Mitigation/Comments
	Low	Medium	High	Very High	Low	Medium	High	Very High	