Le génie pour l'industrie

Département de génie logiciel et des TI

Rapport de laboratoire

Nº de laboratoire	Laboratoire **2**
Étudiant(s)	Nicolas Picard
	Tommy Bédard
	Baptiste Viera
	Arielle Sipeyou
Cours-Groupe	MTI825-01
Session	A22
Professeur	Daniel Tremblay
Date de remise	02 Octobre 2022

Table des matières

1. Introduction

La pandémie de COVID19 a eu un grand impact sur les processus de beaucoup d'entreprises. Nous pouvons notamment penser à la montée en popularité du travail à distance, les remises de colis sans contact, etc. Bien que la plupart des changements se soient déroulés naturellement, certains changements tels que la prise de rendez-vous à distance pour les vaccins de COVID ont occasionné quelques frictions dans le changement. En effet, l'étude de cas analysée dans ce rapport présente les conséquences dues à un bris de service de la plateforme de prise de rendez-vous du CIUSSS. Ce rapport présente une solution afin de prévenir ce genre de problème dans le futur. La méthodologie utilisée par ce rapport repose en grande partie sur les principes exposés par la stratégie COBIT.

La stratégie utilisée par ce rapport est composée de 7 étapes :

1. **Parties prenantes** : explication des acteurs prenant part aux enjeux

2. **Objectifs de l'entreprise** : mise en contexte des objectifs de l'entreprise, ceux-ci ont un impact direct sur ce qui peut être mis en place ou non.

3. **Objectifs de gestion et de gouvernance** : mise en relation des objectifs de l'entreprise et des objectifs de gestion présentés dans COBIT.

4. **Objectifs et métriques pour l'entreprise** : présentation des métriques à mettre en place afin d'avoir une idée globale d'où faire les changements.

5. **Composantes de la gouvernance et de la gestion** : explication des diverses composantes de la gouvernance à considérer en priorité pour l'étude de cas.

6. **Intégration des éléments de COBIT dans l'entreprise** : processus de mise en place des composantes discuté dans le présent rapport.

7. **Résultats dans l'entreprise** : résultats attendus suite à l'implantation de la stratégie proposée.

Les étapes 4 et 5 seront présentées 2 fois une fois par objectifs de gestion identifiés par notre analyse.

2. Parties prenantes

Dans le CIUSSS, nous pouvons identifier 5 parties prenantes :

L'**informatique et les technologies de l'information**, dont les besoins seraient d'assurer la continuité des services. Ils auraient besoin de temps et de redondance.

Les **professionnels de la santé internes** (médecins, infirmier(e)s …), dont leurs besoins seraient d'avoir accès aux fiches des patients, aux rendez-vous et aux analyses en laboratoire.

Les **cliniques externes**, qui auraient besoin d'avoir accès aux analyses, aux rendez-vous et aux informations sur les patients.

Les **usagers touchés par la panne**, qui auraient besoin d'une consultation, d'un test ou d'un rendez-vous.

Enfin, les **chercheurs/équipes de laboratoire**, dont les besoins seraient d'accéder à l'environnement de recherche, aux travaux, aux analyses et à internet.

3. Objectifs de l'entreprise et objectifs d'alignement

Après avoir identifié les parties prenantes représentées ci-dessus, il est question de mieux comprendre la situation du CIUSSS en identifiant leur force et faiblesses afin d'en ressortir les objectifs de l'entreprise.

Force : la mobilisation du personnel compétent ainsi que l'aide des cliniques externes qui adoptent un comportement approprié ; prise en charge rapide des patients urgents.

Faiblesse : Défaillance du système informatique dû à la mauvaise gouvernance des technologies de l'information. Échec dans la satisfaction des demandes de rendez-vous des patients, quantité limitée de tests antigéniques et leur manque de précision.

Menace : nombre sans cesse grandissant des cas de COVID et le besoin constant de tests fiables

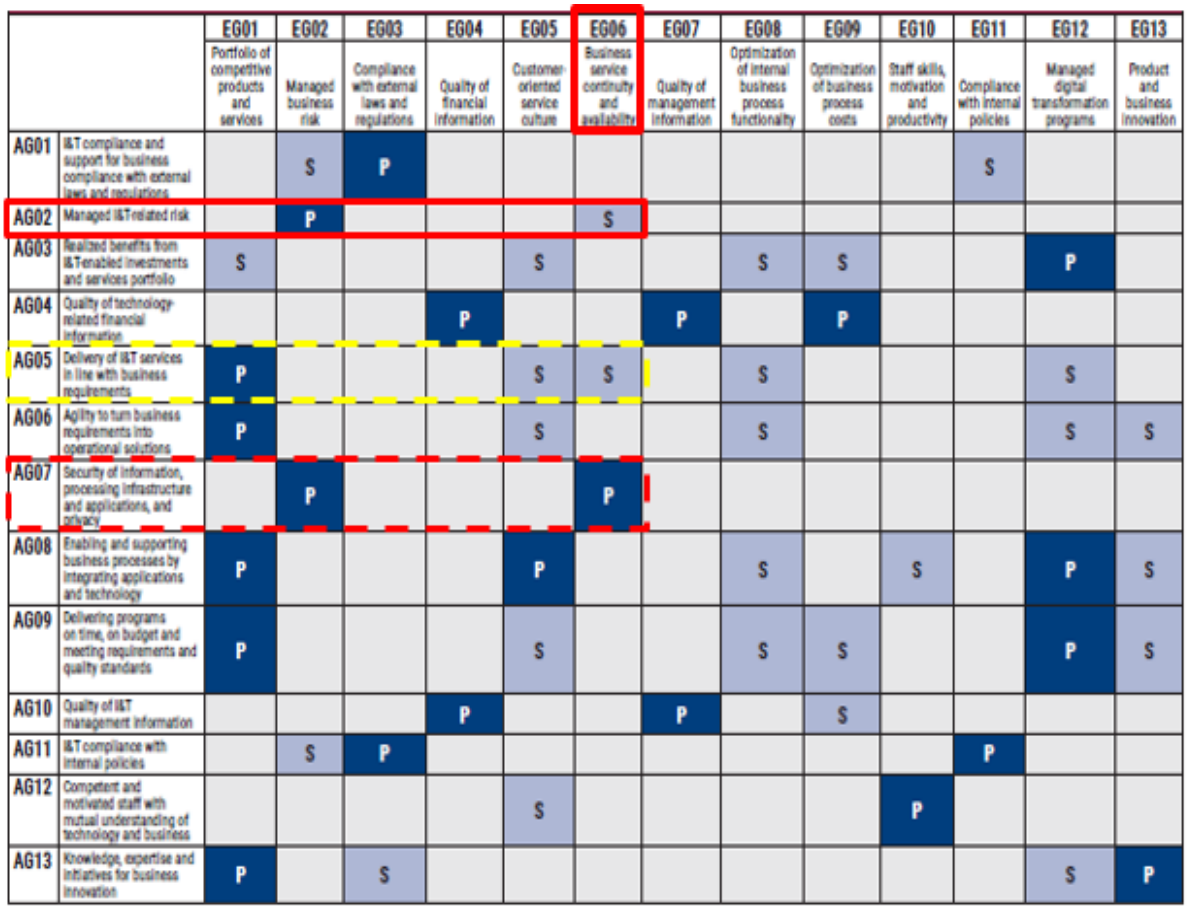
Il en ressort de cette analyse que le CIUSSS a besoin de fournir un service de technologies de l'information fonctionnelle à tous les usagers par le bon fonctionnement de leur système de la une meilleure gestion du risque ainsi que l'apport du personnel compétent.

De ce fait, les priorités du CIUSSS que nous avons identifié sont les suivantes :

- EG02 : Gestion du risque d'affaires
- EG05 : Culture de service orientée client
- **EG06** : Continuité et disponibilité des services d'affaires
- EG07 : Prise de décisions stratégiques basées sur l'information
- EG10 : Productivité opérationnelle et productivité du personnel

L'objectif principal du CIUSSS étant de fournir un service efficace en continu aux usagers, notre étude sera centrée sur EG06. La figure ci-dessous représente la matrice de correspondance entre les objectifs d'entreprise et les objectifs liés aux technologies de l'information.

Figure 1- Objectifs de l'entreprise et objectifs d'alignement cas du CIUSSS



		EG01 Portfolio of competitive products and services	EG02 Managed business risk	EG03 Compliance with external laws and regulations	EG04 Quality of financial information	EG05 Customer oriented service culture	EG06 Business service continuity and availability	EG07 Quality of management information	EG08 Optimization of internal business process functionality	EG09 Optimization of business process costs	EG10 Staff skills, motivation and productivity	EG11 Compliance with internal policies	EG12 Managed digital transformation programs	EG13 Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02	Managed I&T-related risk		P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04	Quality of technology-related financial information				P			P		P				
AG05	Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06	Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P				P							
AG08	Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10	Quality of I&T management information				P			P		S				
AG11	I&T compliance with internal policies		S	P								P		
AG12	Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S									S	P

Pour le cas du CIUSSS, nous avons déterminé que l'objectif d'alignement pertinent lié aux technologies de l'information est les **AG02** pour une bonne gestion du risque.

4. Objectifs de gestion et de gouvernance

La **Figure 2** ci-dessous présente une matrice de correspondances entre la gouvernance et la gestion avec pour connaissance les objectifs d'alignements. Pour le cas du CIUSSS, nous avons décidé de travailler avec l'objectif AG02. Voici la correspondance faite et les objectifs de gouvernance retenus.

Figure 2 - correspondances entre la gouvernance et la gestion avec les objectifs d'alignement

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T compliance and support for business compliance with external laws and regulations	Managed I&T-related risk	Realized benefits from I&T-enabled investments and services portfolio	Quality of technology-related financial information	Delivery of I&T services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of I&T management information	I&T compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02	Ensured benefits delivery			P		S	S		S					S
EDM03	Ensured risk optimization	S	P					P				S		
EDM04	Ensured resource optimization			S		S	S		S	P			S	
EDM05	Ensured stakeholder engagement				S						P	S		
APO01	Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02	Managed strategy			S		S	S		P				S	S
APO03	Managed enterprise architecture			S		S	P	S	P					
APO04	Managed innovation			S			P		S				S	P
APO05	Managed portfolio			P		P	S		S	S				
APO06	Managed budget and costs			S	P					P	S			
APO07	Managed human resources			S		S				S			P	P
APO08	Managed relationships			S		P	P		S	S			P	P
APO09	Managed service agreements					P			S					
APO10	Managed vendors					P	S			S				
APO11	Managed quality			S	S	S				P	P			
APO12	Managed risk		P					P						
APO13	Managed security	S	S					P						
APO14	Managed data	S	S		S			S			P			
BAI01	Managed programs			P			S		S	P				
BAI02	Managed requirements definition			S		P	P		S	P			S	
BAI03	Managed solutions identification and build			S		P	P		S	P				
BAI04	Managed availability and capacity					P		S		S				
BAI05	Managed organizational changes			P		S	S		P	P			S	
BAI06	Managed IT changes		S			S	P		S					
BAI07	Managed IT change acceptance and transitioning		S				P			S				
BAI08	Managed knowledge			S			S		S	S			P	P
BAI09	Managed assets				P						S			
BAI10	Managed configuration					S		P						
BAI11	Managed projects			P		S	P			P				
DSS01	Managed operations					P			S					
DSS02	Managed service requests and incidents		S			P		S						
DSS03	Managed problems		S			P		S						
DSS04	Managed continuity		S			P		P						
DSS05	Managed security services	S	P			S		P				S		
DSS06	Managed business process controls		S			S		S	P			S		
MEA01	Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02	Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03	Managed compliance with external requirements	P										S		
MEA04	Managed assurance	S	S		S	S		S			S	P		

Nous avons tout d'abord choisi de nous concentrer sur l'objectif de gestion EDM03, car nous pensons qu'il faut commencer par faire une analyse de risque de haut niveau afin que cette panne ne se reproduise pas. En effet, si nous avions évalué avant l'impact d'une telle panne,

l'entreprise aurait pu trouver un moyen de continuer ces activités malgré la panne, même si c'est en mode dégradé.

Puis, nous avons aussi décidé de mettre l'accent sur la gestion de la continuité (DSS04), car, dans notre cas, ceci va de pair avec le point EDM03. Suite à l'étude des risques, nous pourrons mettre en place une gestion de la continuité plus efficace, car nous connaîtrons les systèmes impactés par la panne.

5. Objectifs et métriques pour le CUISSS

Il est question ici de sélectionner les indicateurs pertinents pouvant être utilisés afin de mesurer la réalisation des objectifs d'entreprise et d'alignement que nous avons identifiés plus haut.

5.1. EDM03 - Assurer l'optimisation du risque.

La figure ci-après présente les métriques pertinentes en lien avec l'objectif de gouvernance EDM03 qui permettront de proposer des solutions afin de minimiser tous les risques de non-conformité au sein du CIUSSS.

Figure 3 - Métrique pour assurer l'optimisation du risque EDM03

Domain: Evaluate, Direct and Monitor **Governance Objective: EDM03 – Ensured Risk Optimization**	**Focus Area: COBIT Core Model**
Description	
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.	
Purpose	
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.	
The governance objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability	• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

Les indicateurs sélectionnés permettent de savoir si le CIUSSS gère de façon efficace les risques critiques liés aux technologies de l'information.

EG06. Le service de rendez-vous étant en panne, il s'agit bien d'une interruption d'un service client qui cause des incidents importants dans le processus de vaccination (notamment pour les personnes à risque). Cette panne du service de rendez-vous n'ayant pas été anticipée, cela engendrera une perte de temps pour trouver une alternative. Il sera également nécessaire de gérer les plaintes de la part des patients, mais aussi du personnel médical.

EG02. / AG02. La politique de CIUSSS n'était pas orientée gestion des risques. Le nombre d'incidents critiques n'a pas été au préalable bien évalué.

AG07. Il s'agit d'un incident de disponibilité / continuité qui engendre forcément une perte financière (perte de vaccins, trouver une alternative pour vacciner les patients). Cela va au-delà du cadre de l'entreprise puisque cela crée un désagrément dans la population.

5.2. DSS04 - Gérer la continuité.

La **figure 4** ci-dessous illustre diverses métriques pouvant être utilisées afin d'effectuer une gestion efficace de la continuité de l'offre de service du CIUSSS plus précisément sur l'objectif DSS04. Pour cette étude de cas, les métriques du type EG02, EG06, AG05 ainsi que AG07. Effectivement, ces métriques ont été sélectionnées, car celles-ci permettent d'obtenir plusieurs indicateurs permettant de bien identifier les problèmes reliés avec les bris de service et les incidents.

Figure 4 - métriques pour la continuité DSS04

Domain: Deliver, Service and Support **Management Objective: DSS04 - Managed Continuity**	**Focus Area: COBIT Core Model**
Description	
Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.	
Purpose	
Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG01 Portfolio of competitive products and services • EG02 Managed business risk • EG06 Business service continuity and availability • EG08 Optimization of internal business process functionality	• AG05 Delivery of I&T services in line with business requirements • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG05 a. Percent of business stakeholders satisfied that I&T service delivery meets agreed service levels b. Number of business disruptions due to I&T service incidents c. Percent of users satisfied with the quality of I&T service delivery
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	

EG02 permet de récolter les informations nécessaires liées au risque et ainsi de pouvoir créer des matrices risques, bénéfices et probabilités d'occurrence. Ce type de matrice permet d'identifier les risques devant être prévenus.

EG06 et **AG07** permettent tant qu'à eux de créer une image de la condition présente. Ce type de donnée permet de voir si les mesures mises en place ont eu un réel impact ou si le travail doit être continué. En effet, ces métriques identifient clairement la donnée que l'entreprise doit diminuer.

AG05 permet de voir si les utilisateurs du système sont satisfaits du changement. Ce type de donnée est utile pour l'amélioration continue.

6. Composantes de la gouvernance et de la gestion EDM03

Les composantes de gouvernance sélectionnées pour la pratique EDM03 sont :

- Processus
- Services, infrastructures et applications
- Information
- Personnes, aptitudes et compétences
- Culture, Ethique et Comportement

Figure 5 - Composantes de la gouvernance et de la gestion EDM03

6.1. Composante processus

La pratique de gouvernance EDM03 est composée de 3 pratiques de gestions dont :

- EDM03.01 Évaluer la gestion des risques
- EDM03.02 Diriger la gestion des risques
- EDM03.03 Surveiller la gestion des risques

L'utilisation de tout système informatique passe par une évaluation approfondie et continue des risques que cela pourrait avoir sur les services offerts. Le cas CIUSSS est un exemple qui montre que l'évaluation des risques n'a pas été faite convenablement.

Les pratiques de gestion qui se rapportent au cas du bris de service du CIUSSS que nous avons sélectionné sont le **EDM03.01, EDM03.02 et EDM03.03,** car il est question ici de gérer de façon efficace les risques critiques.

Figure 6 - activitées EDM03

A. Component: Process	
Governance Practice	**Example Metrics**
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Level of unexpected enterprise impact b. Percent of I&T risk that exceeds enterprise risk tolerance c. Refreshment rate of risk factor evaluation

Activities	Capability Level
1. Understand the organization and its context related to I&T risk.	2
2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	
3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.	
4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.	
5. Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.	3
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.	
7. Attract and maintain necessary skills and personnel for I&T Risk Management	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

Pour le CIUSSS, il est essentiel d'évaluer au préalable la tolérance aux risques. En effet, cette tolérance étant généralement faible pour les services médicaux, il est primordial de la connaître pour réagir au mieux et le plus rapidement possible aux éventuelles pannes comme la panne de prise de rendez-vous. Il est également important de mettre la considération des risques au cœur de la stratégie de l'entreprise ainsi que d'évaluer la gestion.

De ce fait, les activités 1, 2, 3 permettent d'évaluer le seuil de tolérance au risque du CIUSSS. Les activités 4, 5 et 6 vont permettre de mieux jauger l'effet du risque sur l'utilisation actuelle du système informatique. L'activité 7 permet d'évaluer si le personnel disponible est compétent et apte à réagir en cas de bris de système.

La pratique **EDM03.02** présentée ci-dessus illustre les activités à faire afin d'évaluer si la gestion des risques critiques par le CIUSSS est efficace.

Figure 7 - Pratique de gouvernance EDM03.02

Governance Practice	Example Metrics	
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate and that actual I&T risk does not exceed the board's risk appetite.	a. Level of alignment between I&T risk and enterprise risk b. Percent of enterprise projects that consider I&T risk	
Activities		**Capability Level**
1. Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.		2
2. Direct the development of risk communication plans (covering all levels of the enterprise).		
3. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).		
4. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.		
5. Identify key goals and metrics of the risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.		3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Cybermaturity Platform, 2018	RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives	
ISF, The Standard of Good Practice for Information Security 2016	IR1.1 Information Risk Assessment—Management Approach	
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 11	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.5 Assessment (Task 2)	

Les activités 2, 3, 4 et 5 sont essentielles, en ce sens qu'elles vont permettre de surveiller l'évolution des risques et de réagir le plus rapidement en cas d'incident afin de garantir la continuité des services du CIUSSS.

Dans le contexte de la COVID 19, la pratique **EDM03.03** va permettre de surveiller l'impact des risques liés aux technologies de l'information sur le CIUSSS.

Figure 8 Pratique de gouvernance EDM03.03

Governance Practice	Example Metrics	
EDM03.03 Monitor risk management. Monitor the key goals and metrics of the risk management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	a. Number of potential I&T risk areas identified and managed b. Percent of critical risk that has been effectively mitigated c. Percent of I&T risk action plans executed on time	
Activities		**Capability Level**
1. Report any risk management issues to the board or executive committee.		2
2. Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.		3
3. Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.		4
4. Enable key stakeholders' review of the enterprise's progress toward identified goals.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
COSO Enterprise Risk Management, June 2017	9. Review and Revision—Principle 17	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)	
The Open Group IT4IT Reference Architecture, Version 2.0	6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream	

Les activités 1, 2, 3 et 4 permettent de surveiller que le pourcentage des risques critiques ne dépasse pas la tolérance au risque du CIUSSS afin de prendre des mesures correctives.

6.2. Services, infrastructures et applications

Le CIUSSS a besoin d'évaluer sa tolérance au risque. Ceci passe par l'identification des services et infrastructures à tenir en compte afin de réduire les effets négatifs du risque les et des conséquences que cela pourrait entraîner.

Figure 9 Services, infrastructures et applications

G. Component: Services, Infrastructure and Applications
Risk management system

6.3. Informations

L'information produite par le CIUSSS lors de l'évaluation des risques va permettre de prendre des décisions afin d'assurer le bon fonctionnement de son système de gouvernance.

Figure 10 - Pratique de gouvernance, intrant et extrants EDM03

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	**Inputs**		**Outputs**	
EDM03.01 Evaluate risk management.	**From**	**Description**	**Description**	**To**
	APO12.01	Emerging risk issues and factors	Risk appetite guidance	APO04.01; APO12.03
	Outside COBIT	Enterprise risk management (ERM) principles	Evaluation of risk management activities	APO12.01
			Approved risk tolerance levels	APO12.03
EDM03.02 Direct risk management.	APO12.03	Aggregated risk profile, including status of risk management actions	Approved process for measuring risk management	APO12.01
	Outside COBIT	Enterprise risk management (ERM) profiles and mitigation plans	Key objectives to be monitored for risk management	APO12.01
			Risk management policies	APO12.01
EDM03.03 Monitor risk management.	APO12.02	Risk analysis results	Remedial actions to address risk management deviations	APO12.06
	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments • Opportunities for acceptance of greater risk	Risk management issues for the board	EDM05.01
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs			

Selon les pratiques de gouvernance relative à EDM03, présentée dans la figure ci-dessus, l'évaluation des facteurs de risques ainsi que les principes de gestions de risques du CIUSSS vont permettre d'établir le niveau de tolérance dans le contexte de la COVID 19 et d'en ressortir de l'information adéquate grâce aux activités identifiées dans la composante processus.

6.4. Personnes, aptitudes et compétences

Figure 11 Personnes, aptitudes et compétences

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business risk management	Skills Framework for the Information Age V6, 2015	BURM
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

Dans le secteur médical, et cela est d'autant plus vrai lors d'une crise sanitaire, il est primordial que des personnes au sein du CIUSSS aient des compétences en gestion de risques. Il est également encouragé à ce que du personnel suit des formations régulièrement sur cette thématique. Cela permettra ainsi, en cas de panne comme celle de la prise de rendez-vous au CIUSSS, de ne pas être submergé par les évènements et être en mesure de prendre de bonnes décisions rapidement.

6.5. Culture, éthique et comportement

Figure 12 Culture, éthique et comportement

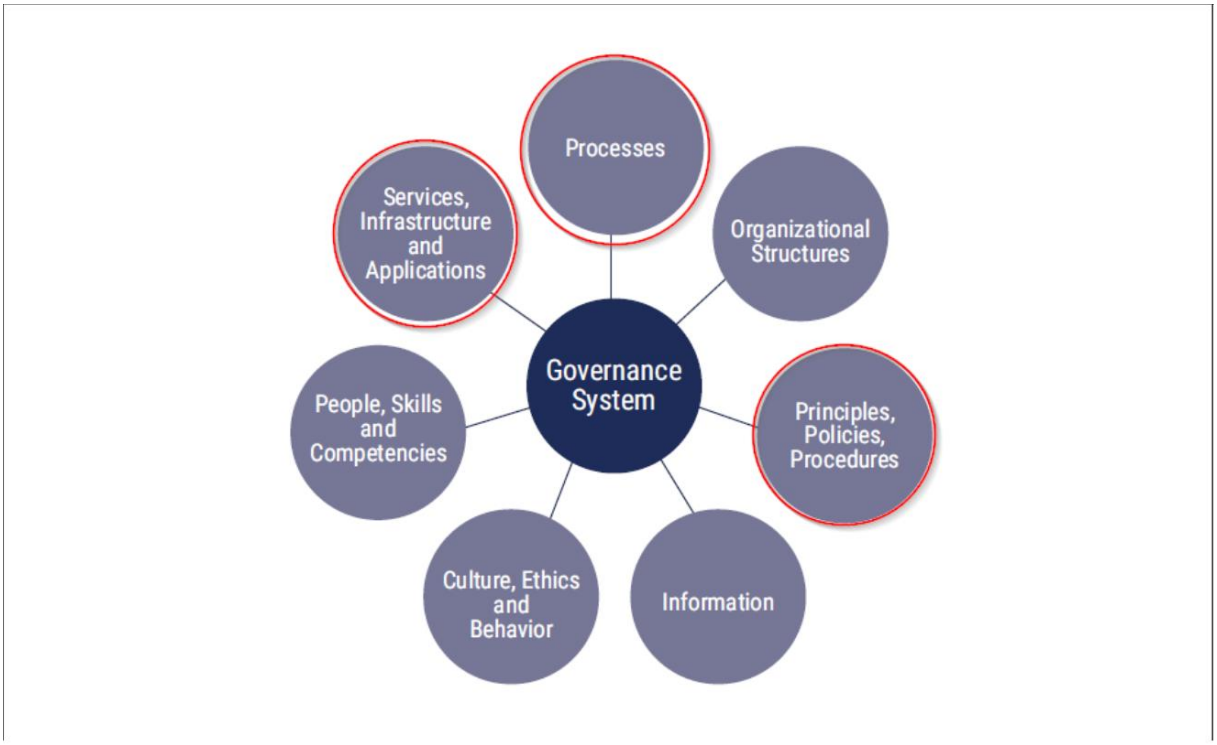
F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote an I&T risk-aware culture at all levels of the organization and empower the enterprise proactively to identify, report and escalate I&T risk, opportunity and potential business impacts. Senior management sets direction and demonstrates visible and genuine support for risk practices. Additionally, management must clearly define risk appetite and ensure an appropriate level of debate as part of business-as-usual activities. Desirable behaviors include encouraging employees to raise issues or negative outcomes and show transparency with regard to I&T risk. Business owners should accept ownership of I&T risk when applicable and demonstrate genuine commitment to I&T risk management by providing adequate resource levels.	COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principles 3 and 4

Ce point est particulièrement important, en particulier dans une situation de crise sanitaire. En effet, il est essentiel d'insuffler au sein de l'entreprise et cela à tous les niveaux, une culture de la gestion des risques. Toute personne, quelle que soit sa formation se doit d'informer les bonnes personnes vis-à-vis d'un éventuel risque constaté. Par exemple, dans notre étude de cas, si un des développeurs a le moindre doute sur l'implémentation du calendrier et de la gestion des rendez-vous, il doit avoir le réflexe de tenir informer ses collègues afin de limiter au maximum les risques. Ce sont aux spécialistes de la gestion des risques de mettre en place cette culture au CIUSSS et de sensibiliser au mieux le personnel sur cette thématique afin que tout le monde puisse réagir à son échelle pour limiter les pannes et agir rapidement en cas de panne.

7. Composantes de la gouvernance et de la gestion DSS04

COBIT propose 7 composantes fournissant des pistes de solutions afin d'optimiser la gouvernance d'une entreprise. Pour l'étude de cas en question, trois des 7 composantes ont été sélectionnées comme montré dans la **figure 3.** Ces 3 composantes ont été sélectionnées, car elles sont capitales pour le maintien du niveau approprié du taux de disponibilité. Les liens entre les composantes et le taux de disponibilité sont illustrés dans les parties suivantes.

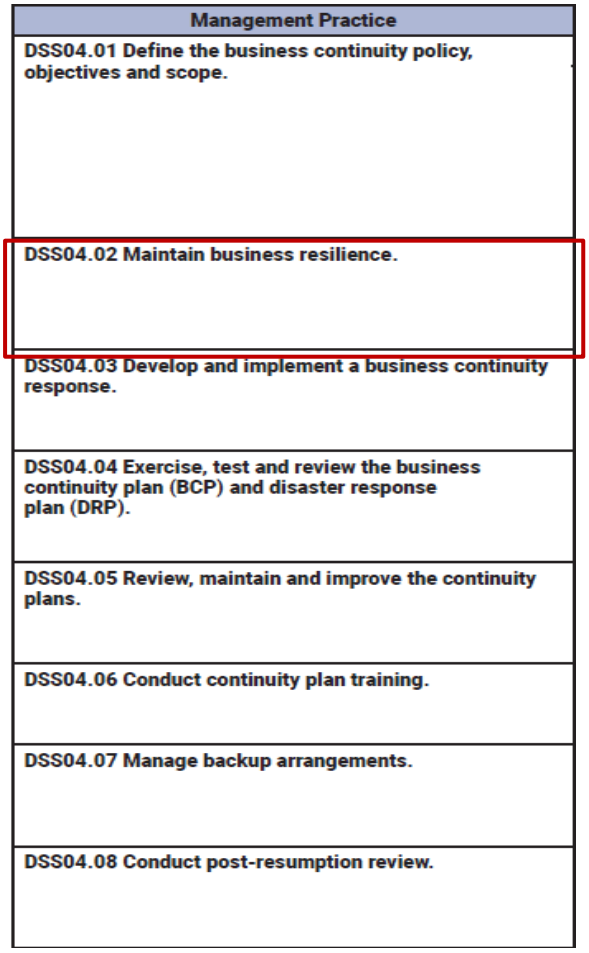
Figure 13 - Composantes de la gouvernance et de la gestion



7.1. Composante processus

La **figure 14** représente les différentes pratiques de gestion reliées à l'objectif de gouvernance DSS04. Nous décidons de nous focaliser sur le point **DSS04.02**. Ce point étant plus accès sur l'analyse des impacts et la continuité des services. Dans le cas du CIUSSS, il est très pertinent d'améliorer ce point, car c'est directement la disponibilité des services qui a été touchée.

Figure 14 - Les pratiques de gestion du composant processus pour DSS04



Management Practice
DSS04.01 Define the business continuity policy, objectives and scope.
DSS04.02 Maintain business resilience.
DSS04.03 Develop and implement a business continuity response.
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).
DSS04.05 Review, maintain and improve the continuity plans.
DSS04.06 Conduct continuity plan training.
DSS04.07 Manage backup arrangements.
DSS04.08 Conduct post-resumption review.

La **figure 15** indique les activités à mettre en place pour mettre en pratique la gestion DSS04.02 que nous avons choisie plus haut.

Figure 15 - Activités reliés aux pratiques de gestion de DSS04.02

Management Practice	Example Metrics	
DSS04.02 Maintain business resilience. Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.	a. Total downtime resulting from major incident or disruption b. Percent of key stakeholders involved in business impact analyses evaluating the impact over time of a disruption to critical business functions and the effect that a disruption would have on them	
Activities		**Capability Level**
1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.		2
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.		
3. Establish the minimum time required to recover a business process and supporting I&T, based on an acceptable length of business interruption and maximum tolerable outage.		
4. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.		
5. Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.		3
6. Analyze continuity requirements to identify possible strategic business and technical options.		
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.		
8. Obtain executive business approval for selected strategic options.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments	
ITIL V3, 2011	Service Design, 4.6 IT Continuity Management	
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-2)	

Pour mettre en place ce processus, nous pensons que ce serait indispensable de traiter toutes les activités encadrées dans la figure ci-dessus. Les activités 1, 2, 3 et 4 mettent en évidence l'analyse du risque (impact et vraisemblance des systèmes) qui est nécessaire pour assurer une disponibilité. Les activités 5 et 6 sont importantes pour la mise en place de solutions suite à l'analyse des risques faite en amont. Ils vont permettre concrètement d'éviter l'indisponibilité des services de CIUSSS. Finalement, l'activité 8 cherche seulement l'approbation de l'exécutif pour implémenter ces solutions.

7.2. Services, infrastructures et applications

La **figure 16** identifie les 3 ressources clefs à mettre en place pour améliorer l'infrastructure et la disponibilité des services de l'entreprise.

Figure 16 - Services, infrastructure et applications de DSS04

G. Component: Services, Infrastructure and Applications
• External hosting services • Incident monitoring tools • Remote storage facility services

Nous avons remarqué que la panne a entraîné une diminution de la disponibilité aux ressources du CIUSSS. Dans une démarche d'assurer la continuité, l'entreprise devrait avoir de la redondance. Ceci passe par l'ajout d'un hôte externe qui héberge les services essentiels, tels que la prise de rendez-vous, les analyses …
De plus, l'ajout d'un système de supervision des services critiques permettrait de réagir plus rapidement à la panne. En effet, grâce à un tel système, l'entreprise serait capable de cibler le problème beaucoup plus rapidement et donc de diminuer l'indisponibilité.
Enfin, pour limiter toute perte de données, nous recommandons que le CIUSSS ait de la redondance au niveau du stockage. Cette donnée est précieuse, car elle constitue toutes les analyses et les fiches patient.

7.3. Politiques et procédures

Les principes, les politiques ainsi que les procédures sont des aspects importants à traiter puisque celles-ci ont un impact direct au niveau des opérations faites tous les jours. De plus, ces derniers dictent les agissements des employés non administratifs ainsi ce sont les directives qui vont avoir un impact concret sur les méthodologies de l'entreprise.

La **figure 17** identifie les politiques les plus importantes à mettre en place afin d'atteindre les objectifs énoncés précédemment. Les politiques en lien avec la continuité d'affaires ont été préférées dans cette étude de cas puisque le contexte médical de cette dernière vient ajouter de l'importance aux taux de disponibilité. En effet, dans l'étude de cas le problème n'est pas une fuite de donnée ou des données perdues, mais bien un bris de service avec beaucoup de conséquences ce qui justifie de prioriser les politiques en lien avec la continuité d'affaires.

Figure 17 - Principes, politiques et procédures (DSS04)

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business continuity policy	Outlines management's commitment to the business impact assessment (BIA), business contingency plan (including trusted recovery), recovery requirements for critical systems, defined thresholds and triggers for contingencies, escalation plan, data recovery plan, training and testing.		
Crisis management policy	Sets guidelines and sequence of crisis response in key areas of risk. Along with I&T security, network management, and data security and privacy, crisis management is one of the operational-level policies that should be considered for complete I&T risk management.		

8. Intégration des éléments de COBIT dans l'entreprise

Si on avait à mettre en place ce qu'on a décrit plus haut pour le cas de figure du CIUSSS. Nous commencerons par les études plus haut niveau, soit le cas de gestion des risques (EDM03).

La pratique de gouvernance EDM03 nous a permis de comprendre que le CIUSSS n'a pas considéré tous les risques liés à leur système informatique. La panne du système informatique et le contexte de la COVID 19 assez critique montrent que le CIUSSS a certes pris conscience du problème et a tout de suite pris des mesures appropriées, mais aucune procédure standard n'est mise en place et les problèmes sont gérés au cas par cas. Il serait donc impératif de :

- Définir une échelle de tolérance au risque qui va permettre de mesurer facilement les risques de non-conformité
- Définir un ensemble de responsabilités exercées par les parties prenantes afin de gérer le risque adéquatement et de vérifier le niveau d'implication des employés du CIUSSS.
- Définir un ensemble de procédures et politiques à respecter et à suivre dans l'élaboration d'un système informatique.
- Élaborer des stratégies afin d'éviter tout incident ou tout transfert des risques
- Définir un plan de vérification et de maintenance des systèmes informatiques
- Encourager la direction et le personnel à réaliser un travail de qualité

Par la suite, nous mettrons en place la gestion de la continuité (DSS04). Pour cela, nous débuterons par traiter les 8 activités citées précédemment (analyse des incidents, des impacts et des processus déjà en place). Grâce à ces études, nous serions capables d'avoir une vision globale sur les points de défaillance, et de savoir comment les corriger tout en gardant un bon rapport efficacité/coûts. Puisque nous aurons une bonne idée des points de défaillance, nous pouvons venir les corriger avec une meilleure redondance au niveau infrastructure. Par exemple, utiliser du cloud pour s'éviter la gestion des serveurs, utiliser du load balancing afin d'assurer la continuité des services en cas de problème. Pour finir, nous redéfinissons les politiques et procédures de l'entreprise afin que ce genre d'incident ne se reproduise plus, ou du moins que l'on sache quoi faire si cela se reproduit. Pour cela, plusieurs plans vont être mis en place :

- plan de récupération sur les systèmes les plus critiques identifiés plus haut
- plan de récupération des donnés critiques
- plan d'entraînement et de test des solutions.

Ainsi, à la fin de cette étude, nous aurons analysé les failles/problèmes pouvant survenir, nous les aurons corrigés et nous aurons assuré une continuité des services dans le cas où un problème surviendrait malgré tout ça.

9. Résultats dans l'entreprise

La mise en place de ces solutions va permettre d'accroître le taux de disponibilité du système. En effet, la problématique relevée dans cette étude est un problème au niveau de la continuité du service offert. La mise en place des éléments COBIT va ainsi aider à réduire les chances d'incidents ainsi que de développer de meilleur réflexe pour la gestion de ceux-ci.

Ainsi, les changements vont impacter la méthodologie d'autorisation et de dérogation des manipulations effectuées par les opérateurs du système. Par ce fait même, les changements au niveau des systèmes critiques devront passer par des demandent spécifiques afin de réduire les risques et d'analyser le niveau de risque.

Ensuite, les données seront récoltées comme montré dans la section 5, objectifs et métriques pour l'entreprise. Ces données permettront de constater si les changements appliqués ont eu une incidence sur le nombre d'incidents et de vulnérabilités. Finalement, la mise en place du système de métrique permet aussi de lancer des alertes en cas d'anomalie des divers systèmes, les processus de l'entreprise devront donc s'adapter à ces nouvelles alertes.

Conclusion

Ce rapport basé sur la stratégie COBIT présente ainsi une solution afin de prévenir les conséquences dues à un bris de service de la plateforme de prise de rendez-vous du CIUSSS.

Dans un premier temps, nous avions bien identifié les parties prenantes qui sont le personnel spécialisé en TI qui devra assurer la continuité, les professionnels de la santé internes qui devront avoir entre autres accès aux fiches des patients et des rendez-vous, les cliniques externes devront avoir accès aux analyses, rendez-vous et aux informations sur les patients, les usagers touchés par la panne qui auront besoin d'une consultation et enfin les chercheurs de laboratoire devront avoir accès à l'environnement de recherche, aux travaux et aux analyses.

Nous avons ensuite bien déterminé l'objectif principal du CIUSSS qui est de fournir un service efficace en continu aux usagers. Donc l'objectif du CIUSSS devra alors s'inscrire dans le code EG06 (Continuité et disponibilité des services d'affaires), extrait du Cobit. L'objectif d'alignement associé que nous avons par la suite sélectionné est le AG02 afin de garantir une bonne gestion générale des risques.

Ensuite, associés à AG02, nous conseillons d'appliquer l'objectif de gestion EDM03 (*Assurer l'optimisation du risque*), car selon nous une analyse de risque de haut niveau permettra de mieux anticiper, d'agir plus rapidement et de manière organisée face aux risques. Cela permettra ainsi de minimiser tous les risques de non-conformité au sein du CIUSSS.
Quant à l'objectif de gouvernance qui va de pair, nous conseillons de suivre le DSS04 (*Gérer la continuité*) qui permettra de mettre en place une gestion de la continuité plus efficace, car nous connaîtrons les systèmes impactés par la panne.

Pour revenir sur l'objectif de gestion EDM03, nous avons sélectionné les composantes de gouvernance suivantes :

- Processus : EDM03.01 (*Évaluer*), EDM03.02 (*Diriger*), EDM03.03 (*Surveiller*)
- Services, infrastructures et applications
- Information
- Personnes, aptitudes et compétences
- Culture, Ethique et Comportement

Ces choix se justifient par le fait que le CIUSSS doit avoir une approche holistique de la gestion des risques. Il est nécessaire que le CIUSSS, et des personnes compétentes en TI soient aptes à évaluer les potentiels risques encourus, mais également à agir en conséquence. De plus, cette culture du risque devra être connue par l'ensemble du personnel du CIUSSS afin que chacun puisse agir à son échelle.

Concernant l'objectif de gouvernance DSS04, nous avons sélectionné les composantes de gouvernance suivantes :

- Processus (DSS04.02 *Maintenir la résilience de l'entreprise*)
- Services, infrastructures et applications
- Information
- Personnes, aptitudes et compétences
- Culture, Ethique et Comportement

Ces choix se justifient quant à eux par le fait que le CIUSSS doit maintenir un niveau approprié du taux de disponibilité, doit analyser les impacts et la continuité des services, les risques afin d'assurer la meilleure disponibilité. Cela leur permettra de mettre en place de solutions suite à l'analyse des risques faite en amont. À cela s'ajoute le fait, que le CIUSSS devra héberger les principaux services (prises de rendez-vous, analyses) chez un hôte externe pour avoir de la redondance, garantissant la continuité dans ses services. En parlant de redondance, nous conseillons aussi au CIUSSS d'avoir de la redondance dans ses précieuses données et de les stocker à différents endroits (support physique, cloud…). Enfin, le CIUSSS pourra mettre en place un système de supervision des services critiques afin d'agir rapidement et diminuer l'indisponibilité.
Pour terminer notre brève justification sur notre choix d'objectif de gouvernance qui est DSS04, nous conseillons au CIUSSS d'adopter une politique en lien avec la continuité d'affaires afin de mettre plus l'accent sur l'importance des taux de disponibilité.

Pour conclure, si le CIUSSS respecte et suit les recommandations citées précédemment, celui-ci ne connaîtra plus de problèmes liés à l'indisponibilité de ses services ou bien saura réagir de façon efficiente à toute difficulté.