Le génie pour l'industrie

Department of Software and IT Engineering

Laboratory report

Nº of laboratory	Laboratory **2**
Student(s)	Nicolas Picard
	Tommy Bédard
	Baptiste Viera
	Arielle Sipeyou
Courses-Group	MTI825-01
Session	A22
Professor	Daniel Tremblay
Date of delivery	02 October 2022

Table of contents

1. Introduction

The COVID19 pandemic has had a great impact on the processes of many companies. We can think in particular of the rise in popularity of remote working, contactless package deliveries, etc. While most of the changes have been natural, some changes such as remote appointment scheduling for COVID vaccines have caused some friction in the change. Indeed, the case study analyzed in this report presents the consequences due to a service failure of the CIUSSS appointment scheduling platform. This report presents a solution to prevent this type of problem in the future. The methodology used in this report is largely based on the principles outlined by the COBIT strategy.

The strategy used by this report is composed of 7 steps:

1. **Stakeholders**: explanation of the actors involved in the issues

2. **Company objectives**: contextualization of the company's objectives, which have a direct impact on what can or cannot be implemented.

3. **Management and governance objectives**: linking the company's objectives to the management objectives presented in COBIT.

4. **Objectives and metrics for the company**: presentation of the metrics to be put in place in order to have a global idea of where to make the changes.

5. **Governance and Management Components**: Explanation of the various governance components that should be prioritized for the case study.

6. **Integration of COBIT elements in the company**: implementation process of the components discussed in this report.

7. **Business outcomes**: expected results following the implementation of the proposed strategy.

Steps 4 and 5 will be presented twice, once for each management objective identified by our analysis.

2. Stakeholders

In the CIUSSS, we can identify 5 stakeholders:

Computer and information technology, whose needs would be to ensure continuity of services. They would need time and redundancy.

Internal health professionals (doctors, nurses . . .), whose needs would be to have access to patient records, appointments and laboratory tests.

Outpatient clinics, which would need access to tests, appointments and patient information.

Users affected by the outage who may need a consultation, test or appointment.

Finally, **researchers/laboratory teams**, whose needs would be t o access the research environment, work, analysis and the internet.

3. Business and alignment objectives

After having identified the stakeholders represented above, it is a question of better understanding the situation of the CIUSSS by identifying their strengths and weaknesses in order to highlight the objectives of the enterprise.

Strength: mobilization of competent staff as well as the assistance of outpatient clinics that behave appropriately; rapid management of urgent patients.

Weaknesses: Computer system failure due to poor IT governance. Failure to meet patient appointment requests, limited amount of antigenic testing and lack of accuracy.

Threat: ever-increasing number of COVID cases and the constant need for reliable testing

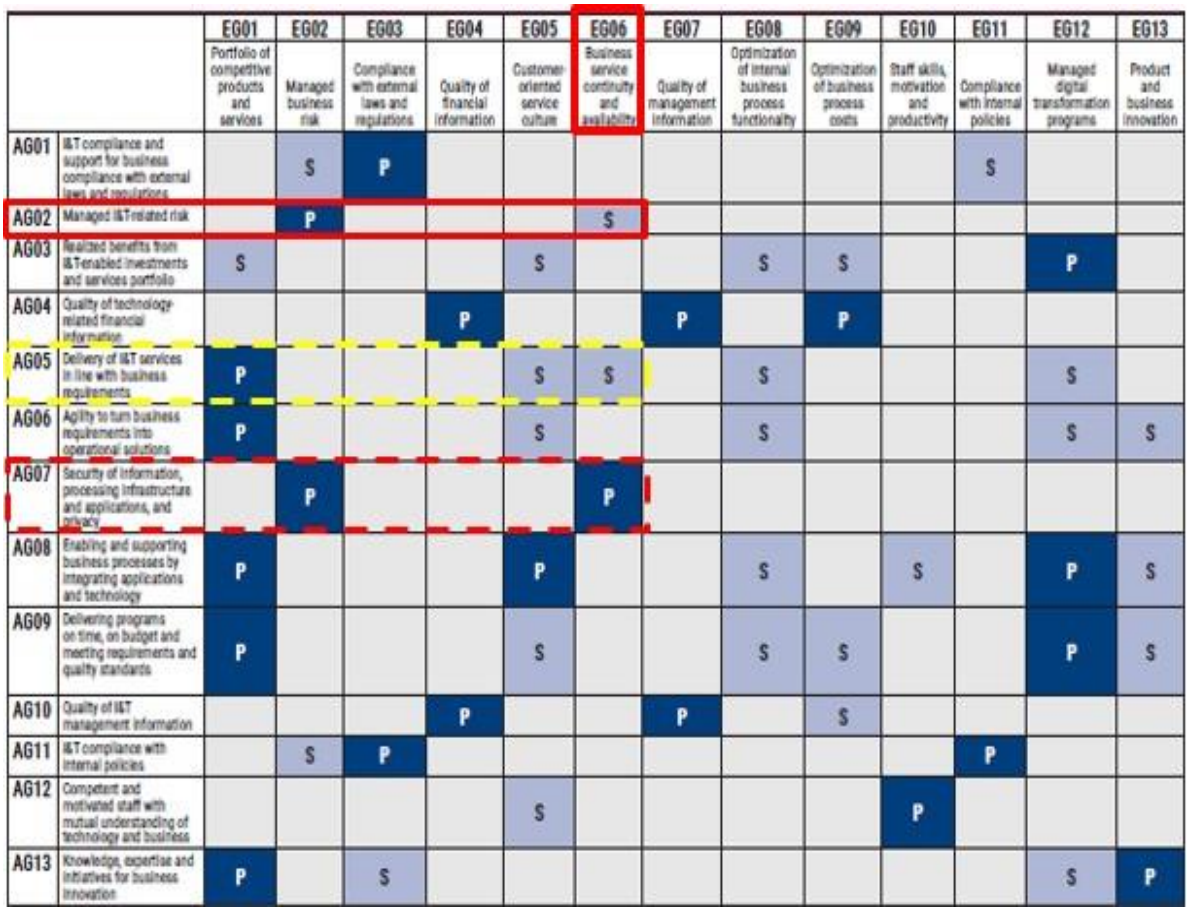
This analysis shows that the CIUSSS needs to provide a functional information technology service to all users through the proper functioning of their system and better risk management as well as the contribution of competent personnel.

As a result, the CIUSSS priorities that we have identified are as follows:

- EG02 : Business Risk Management
- EG05 : Customer-oriented service culture
- **EG06** : Continuity and availability of business services
- EG07 : Information-based strategic decision making
- EG10 : Operational and Staff Productivity

Since the main objective of the CIUSSS is to provide a continuous efficient service to users, our study will focus on EG06. The figure below represents the correspondence matrix between the business objectives and the information technology objectives.

Figure 1 - Corporate objectives and alignment objectives of the 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

For the ICUHSS case, we have identified the relevant alignment objective related to information technology as **AG02** for good risk management.

4. Management and governance objectives

Figure 2 below presents a matrix of correspondences between governance and management with the knowledge of the alignment objectives. In the case of CIUSSS, we decided to work with objective AG02. Here is the correspondence made and the governance objectives retained.

Figure 2 - Governance and management correspondences with alignment objectives

		AG01 I&T compliance and support for business compliance with external laws and regulations	AG02 Managed I&T-related risk	AG03 Realized benefits from I&T-enabled investments and services portfolio	AG04 Quality of technology-related financial information	AG05 Delivery of I&T services in line with business requirements	AG06 Agility to turn business requirements into operational solutions	AG07 Security of information, processing infrastructure and applications, and privacy	AG08 Enabling and supporting business processes by integrating applications and technology	AG09 Delivering programs on time, on budget and meeting requirements and quality standards	AG10 Quality of I&T management information	AG11 I&T compliance with internal policies	AG12 Competent and motivated staff with mutual understanding of technology and business	AG13 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		

We first chose to focus on the EDM03 management objective, because we believe that a high-level risk analysis should be done first to ensure that this failure does not happen again. Indeed, if we had assessed the impact of such a failure before,

the company could have found a way to continue these activities despite the outage, even if it is in a degraded mode.

Then, we also decided to focus on continuity management (DSS04), because, in our case, this goes hand in hand with point EDM03. Following the risk study, we will be able to set up a more efficient continuity management, because we will know the systems impacted by the failure.

5. Objectives and Metrics for CUISSS

This involves selecting relevant indicators that can be used to measure the achievement of the business and alignment objectives we identified above.

5.1. EDM03 - Ensure risk optimization.

The figure below presents the relevant metrics related to the governance objective EDM03 that will allow us to propose solutions to minimize all risks of non-compliance within the CIUSSS.

Figure 3 - Metrics to ensure risk optimization 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

The selected indicators provide insight into whether ICUH is effectively managing critical information technology risks.

EG06. Since the appointment service is down, this is indeed an interruption of a customer service that causes major incidents in the vaccination process (especially for people at risk). This breakdown of the appointment service was not anticipated and will result in a loss of time to find an alternative. It will also be necessary to manage complaints from patients, but also from medical staff.

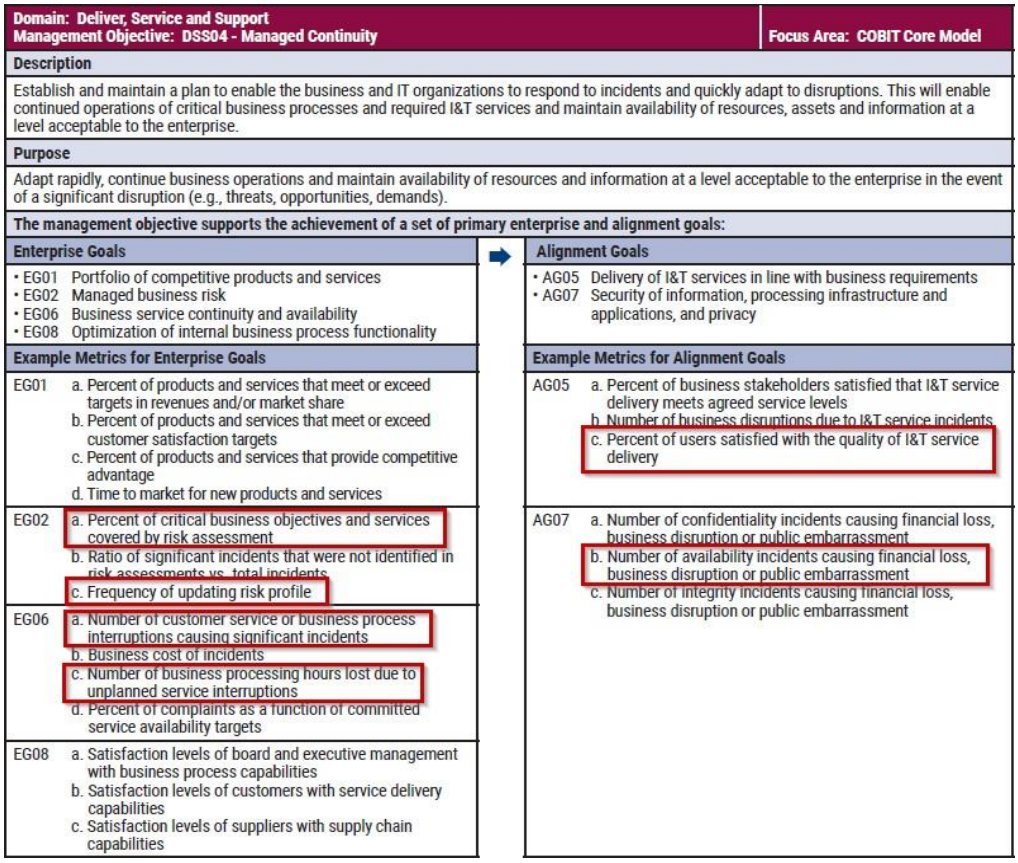
EG02 / AG02. CIUSSS policy was not risk management oriented. The number of critical incidents was not properly assessed beforehand.

AG07. This is an incident of availability/continuity which necessarily generates a financial loss (loss of vaccines, finding an alternative to vaccinate patients). This goes beyond the framework of the company since it creates an inconvenience in the population.

5.2. DSS04 - Managing continuity.

Figure 4 below illustrates various metrics that can be used to effectively manage the continuity of the CIUSSS service offering, specifically on the DSS04 objective. For this case study, metrics of the type EG02, EG06, AG05 and AG07 were selected. Indeed, these metrics were selected because they provide several indicators to identify problems related to service breakdowns and incidents.

Figure 4 - metrics for DSS04 continuity



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 allows to collect the necessary information related to the risk and thus to create risk, benefit and probability of occurrence matrices. This type of matrix allows to identify the risks that need to be prevented.

EG06 and **AG07** are used to create a picture of the current condition. This type of data allows to see if the measures implemented have had a real impact or if the work must be continued. Indeed, these metrics clearly identify the data that the company must decrease.

AG05 allows to see if the users of the system are satisfied with the change. This type of data is useful for continuous improvement.

6. Governance and management components EDM03

The governance components selected for Practice EDM03 are:

- Process
- Services, infrastructure and applications
- Information
- People, skills and competencies
- Culture, Ethics and Behavior

Figure 5 - Governance and Management Components EDM03

6.1. Process component

The EDM03 governance practice is composed of 3 management practices including:

- EDM03.01 Assessing Risk Management
- EDM03.02 Leading Risk Management
- EDM03.03 Monitor risk management

The use of any computer system requires a thorough and continuous assessment of the risks that it could have on the services offered. The CIUSSS case is an example that shows that the risk assessment was not done properly.

The management practices that are relevant to the CIUSSS service breakdown case we selected are **EDM03.01, EDM03.02 and EDM03.03,** because we are talking about effectively managing critical risks.

Figure 6 - EDM03 activities

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

For the CIUSSS, it is essential to evaluate risk tolerance beforehand. Indeed, since this tolerance is generally low for medical services, it is essential to know it in order to react as well and as quickly as possible to possible breakdowns such as the breakdown of appointment scheduling. It is also important to put the consideration of risks at the heart of the company's strategy and to evaluate the management.

As a result, activities 1, 2, 3 allow for an assessment of the CIUSSS' risk tolerance threshold. Activities 4, 5 and 6 will allow us to better gauge the effect of the risk on the current use of the computer system. Activity 7 allows us to assess whether the available personnel are competent and able to react in the event of a system failure.

Practice **EDM03.02** above illustrates the activities to be done to assess whether ICUH's management of critical risks is effective.

Figure 7 - Governance Practice 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)	

Activities 2, 3, 4 and 5 are essential in that they will allow us to monitor the evolution of risks and to react as quickly as possible in the event of an incident in order to guarantee the continuity of CIUSSS services.

In the context of COVID 19, practice **EDM03.03** will monitor the impact of information technology risks on the ICUH.

Figure 8 Governance Practice 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	

Activities 1, 2, 3, and 4 monitor that the percentage of critical risks does not exceed ICUH's risk tolerance in order to take corrective action.

6.2. Services, infrastructure and applications

CIUSSS needs to assess its risk tolerance. This involves identifying the services and infrastructure that need to be considered in order to reduce the negative effects of risk and the consequences that may result.

Figure 9 Services, infrastructure and applications

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

6.3. Information

The information generated by CIUSSS during the risk assessment process will allow decisions to be made to ensure the proper functioning of its governance system.

Figure 10 - Governance Practice, Inputs and Outputs 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		

According to the governance practices related to EDM03, presented in the figure above, the assessment of risk factors and the CIUSSS risk management principles will make it possible to establish the tolerance level in the context of COVID 19 and to obtain adequate information through the activities identified in the process component.

6.4. People, skills and competencies

Figure 11 People, skills and competencies

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

In the medical sector, and this is especially true during a health crisis, it is essential that people within the CIUSSS have risk management skills. It is also encouraged that staff receive regular training on this topic. This will ensure that, in the event of a breakdown such as the appointment booking process at CIUSSS, they are not overwhelmed by events and are able to make good decisions quickly.

6.5. Culture, ethics and behaviour

Figure 12 Culture, ethics and behaviour

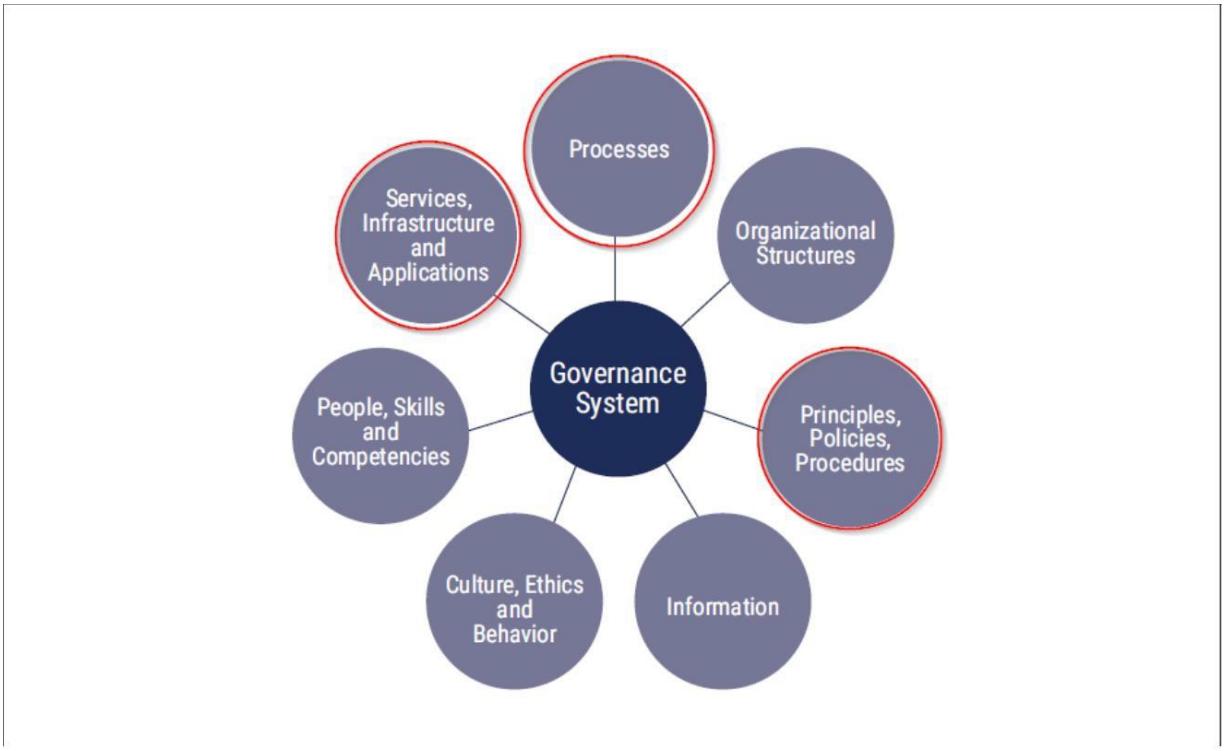
F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote an I&T risk-aware culture at all levels of the organization and empower the enterprise proactively to identify, report and escalate I&T risk, opportunity and potential business impacts. 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

This is particularly important in a health crisis situation. Indeed, it is essential to instill a culture of risk management within the company at all levels. Everyone, regardless of their training, must inform the right people about a possible risk. For example, in our case study, if one of the developers has the slightest doubt about the implementation of the calendar and appointment management, he must have the reflex to inform his colleagues in order to limit the risks as much as possible. It is up to the risk management specialists to implement this culture at the CIUSSS and to make the staff as aware as possible of this issue so that everyone can react at their own level to limit breakdowns and act quickly in case of failure.

7. Governance and Management Components DSS04

COBIT proposes 7 components that provide solutions to optimize the governance of an enterprise. For the case study in question, three of the seven components were selected as shown in **Figure 3.** These three components were selected because they are critical to maintaining the appropriate level of availability. The links between the components and the availability rate are illustrated in the following sections.

Figure 13 - Governance and Management Components



7.1. Process component

Figure 14 represents the different management practices related to the governance objective DSS04. We have decided to focus on point **DSS04.02**. This point is more focused on the analysis of impacts and continuity of services. In the case of the CIUSSS, it is very relevant to improve this point, because it is directly the availability of services that has been affected.

Figure 14 - Process component management practices for 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.

Figure 15 shows the activities that need to be implemented to put into practice the DSS04.02 management that we chose above.

Figure 15 - Activities related to the management practices of 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)

To implement this process, we believe it would be essential to address all the activities framed in the figure above. Activities 1, 2, 3 and 4 highlight the risk analysis (impact and likelihood of systems) that is necessary to ensure availability. Activities 5 and 6 are important for the implementation of solutions following the risk analysis done upstream. In concrete terms, they will help avoid the unavailability of CIUSSS services. Finally, activity 8 only seeks the approval of the executive to implement these solutions.

7.2. Services, infrastructure and applications

Figure 16 identifies the 3 key resources to be put in place to improve the infrastructure and availability of enterprise services.

Figure 16 - DSS04 services, infrastructure and applications

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

We noted that the outage resulted in a decrease in the availability of CIUSSS resources. In order to ensure continuity, the company should have redundancy. This can be achieved by adding an external host to host essential services, such as appointment scheduling, analyses, etc. In addition, the addition of a supervision system for critical services would make it possible to react more quickly to the breakdown. Indeed, thanks to such a system, the company would be able to target the problem much more quickly and thus reduce the unavailability.
Finally, to limit any loss of data, we recommend that the CIUSSS have redundancy in storage. This data is valuable, as it constitutes all analyses and patient records.

7.3. Policies and procedures

Principles, policies and procedures are important aspects to deal with since they have a direct impact on the operations done every day. Moreover, they dictate the actions of non-administrative employees, so it is the directives that will have a concrete impact on the company's methodologies.

Figure 17 identifies the most important policies that need to be in place to achieve the above objectives. The policies related to business continuity were preferred in this case study because the medical context of the latter adds importance to the availability rates. Indeed, in this case study, the problem is not a data leak or lost data, but a service failure with many consequences, which justifies prioritizing policies related to business continuity.

Figure 17 - Principles, Policies and Procedures (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. Integration of COBIT elements in the company

If we were to implement what we described above for the CIUSSS case. We will start with the higher level studies, the risk management case (EDM03).
The EDM03 governance practice allowed us to understand that CIUSSS did not consider all the risks related to their computer system. The computer system failure and the rather critical COVID 19 context show that although CIUSSS was aware of the problem and immediately took appropriate measures, no standard procedures are in place and problems are managed on a case-by-case basis. It would therefore be imperative to :

- Define a risk tolerance scale that will make it easy to measure the risks of non-compliance
- Define a set of responsibilities exercised by the stakeholders in order to properly manage the risk and verify the level of involvement of CIUSSS employees.
- Define a set of procedures and policies to be followed in the development of an IT system.
- Develop strategies to avoid incidents or risk transfer
- Define an audit and maintenance plan for computer systems
- Encourage management and staff to do quality work

Then, we will set up the continuity management (DSS04). To do this, we will start by treating the 8 activities mentioned above (analysis of incidents, impacts and processes already in place). Thanks to these studies, we will be able to have a global vision on the points of failure, and to know how to correct them while keeping a good efficiency/cost ratio. Since we will have a good idea of the points of failure, we can come and correct them with better redundancy at the infrastructure level. For example, use the cloud to avoid server management, use load balancing to ensure continuity of services in case of problems. Finally, we are redefining the company's policies and procedures so that this type of incident does not happen again, or at least so that we know what to do if it does happen again. For this, several plans will be put in place:

- recovery plan on the most critical systems identified above
- critical data recovery plan
- training and testing plan for solutions.

Thus, at the end of this study, we will have analyzed the flaws/problems that could occur, we will have corrected them and we will have ensured a continuity of services in case a problem would occur despite all that.

9. Results in the company

The implementation of these solutions will increase the system availability rate. Indeed, the problem identified in this study is a problem in the continuity of the service offered. The implementation of COBIT elements will help to reduce the chances of incidents as well as to develop better reflexes for their management.

Thus, the changes will impact the methodology for authorizing and waiving the manipulations performed by the system operators. Therefore, changes in critical systems will have to go through specific requests in order to reduce the risks and analyze the level of risk.

Next, data will be collected as shown in Section 5, Goals and Metrics for the Enterprise. This data will allow us to see if the changes applied have had an impact on the number of incidents and vulnerabilities. Finally, the implementation of the metrics system also allows alerts to be issued in the event of anomalies in the various systems, so the company's processes will have to adapt to these new alerts.

Conclusion

This report, based on the COBIT strategy, presents a solution to prevent the consequences of a service failure on the CIUSSS appointment scheduling platform.

Initially, we had identified the stakeholders who are the specialized IT personnel who will have to ensure continuity, the internal health professionals who will have to have access to the patients' files and appointments, the external clinics who will have to have access to the analyses, appointments and information on the patients, the users affected by the breakdown who will need a consultation and finally the laboratory researchers who will have to have access to the research environment, to the works and to the analyses.

We then clearly identified the main objective of the CIUSSS, which is to provide an efficient and continuous service to users. Therefore, the CIUSSS objective should fall under the code EG06 (Continuity and availability of business services), extracted from Cobit. The associated alignment objective that we have subsequently selected is AG02 to ensure good overall risk management.

Then, associated with AG02, we recommend applying management objective EDM03 (*Ensure risk optimization*), because we believe that a high-level risk analysis will allow us to better anticipate, act more quickly and in an organized manner in the face of risks. This will minimize all risks of non-compliance within the CIUSSS.
As for the governance objective that goes with it, we advise following DSS04 (*Manage Continuity*) which will allow us to implement a more efficient continuity management, because we will know the systems impacted by the failure.

Returning to the EDM03 management objective, we have selected the following governance components:

- Processes: EDM03.01 (*Assess*), EDM03.02 (*Lead*), EDM03.03 (*Monitor*)
- Services, infrastructure and applications
- Information
- People, skills and competencies
- Culture, Ethics and Behavior

These choices are justified by the fact that the CIUSSS must have a holistic approach to risk management. It is necessary that the CIUSSS and competent IT people be able to evaluate the potential risks incurred, but also to act accordingly. Furthermore, this risk culture must be known by all CIUSSS personnel so that each one can act at his or her own level.

Regarding governance objective DSS04, we selected the following governance components:

- Process (DSS04.02 *Maintain Enterprise Resilience*)
- Services, infrastructure and applications
- Information
- People, skills and competencies
- Culture, Ethics and Behavior

These choices are justified by the fact that the CIUSSS must maintain an appropriate level of availability, must analyze the impacts and continuity of services, and the risks in order to ensure the best availability. This will allow them to implement solutions following the risk analysis done upstream. In addition, the CIUSSS will have to host the main services (appointment scheduling, analyses) at an external host to have redundancy, guaranteeing continuity in its services. Speaking of redundancy, we also advise the CIUSSS to have redundancy in its precious data and to store them in different places (physical support, cloud...). Finally, the CIUSSS can set up a supervision system for critical services in order to act quickly and reduce unavailability.
To conclude our brief justification of our choice of governance objective, which is DSS04, we advise the CIUSSS to adopt a policy related to business continuity in order to put more emphasis on the importance of availability rates.

In conclusion, if CIUSSS respects and follows the above recommendations, it will no longer experience problems related to the unavailability of its services or will be able to react efficiently to any difficulties.