Health Canada and the Public Health Agency of Canada
Santé Canada et l'Agence de la santé publique du Canada

Final Report

Audit of Information Technology Continuity Planning for Mission Critical Systems/Applications at Health Canada and the Public Health Agency of Canada

September 2016

Canada

Table of Contents

Executive summary

The audit focused on mission critical systems/applications (MCA) in Health Canada (HC) and the Public Health Agency of Canada (PHAC). All critical services delivered by HC and PHAC depend on one or more MCA being available during a disruption in operations. Information technology (IT) continuity planning is a key part of business continuity planning. The delivery of critical services could be seriously compromised or may not be performed if MCAs are not available during a business disruption or a disaster. IT continuity plans (commonly known as disaster recovery plans) and business continuity plans are vital to the delivery of critical services for HC and PHAC.

The objective of the audit was to assess the management control framework in place to enable IT continuity planning at HC and PHAC for MCAs supporting the delivery of critical services to Canadians. The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada and the International Standards for the Professional Practice of Internal Audit. Sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion.

While there is a governance structure in place for business continuity planning, HC and PHAC would be better served by integrating IT continuity planning for MCAs into the business continuity planning governance structure. Roles and responsibilities are well defined for business continuity planning; however, the roles and responsibilities of all key stakeholders involved in IT continuity planning should be more clearly defined and communicated.

The requirement to identify and maintain a list of MCAs is one of the most important elements to IT continuity planning because it has a significant impact on determining priorities and resource allocations. HC and PHAC are currently updating the list of MCAs. This exercise, led by the Director of the National Business Continuity Management Directorate, needs to be fully documented and requires improvement so that all MCAs are properly identified and have an IT continuity plan in place.

None of the 11 MCAs (seven from HC and four from PHAC) examined during the audit had a comprehensive IT continuity plan in place. More effort is required to integrate IT continuity planning into the Business Continuity Planning Program. Several key documents required for the development of IT continuity plans were missing, outdated or incomplete. The Branch or Departmental Business Continuity Coordinators need to challenge or verify the existence and completeness of the required documents.

IT continuity planning needs to be identified as a risk for HC and PHAC, even though it has been identified as a risk in several MCA threat and risk assessments and in HC's and PHAC's self-assessment of the Management of IT Security. With the exception of one MCA, action plans need to be prepared to ensure that risks have been mitigated. The IT Plans and the IT and Information Management Strategic Plan for HC and PHAC need to take into account IT continuity planning risks.

Although there is a business arrangement in place between HC and PHAC and Shared Services Canada, the audit found that service levels need to be specified with respect to the restoration of MCAs, thus providing formal assurance to business owners that MCAs can be restored within the predetermined time frame after a disruption or a disaster has occurred.

Management action is required to:

- Integrate IT continuity planning for mission critical systems/applications into the business continuity planning governance structure, including clearly defining and communicating the roles and responsibilities for IT continuity planning;
- Further assess risks related to IT continuity planning;
- Ensure that up-to-date threat and risk assessments exist for all mission critical systems/applications and action plans;
- Complete and document the process for identifying and approving the list of mission critical systems/applications;
- Ensure that a service level agreement or other formal business arrangement is in place with service providers, describing service levels for the restoration of mission critical systems/applications; and
- Ensure that a comprehensive IT continuity plan exists for all mission critical systems/applications.

Management agrees with the six recommendations and has provided an action plan that will strengthen the management control framework over IT continuity planning for mission critical systems/applications.

A - Introduction

1. Background

The Treasury Board of Canada (TB) *Policy on Government Security* (2009) defines mission critical services as a service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the effective functioning of the government.

Health Canada (HC) and the Public Health Agency of Canada (PHAC) provide seven critical services to Canadians, as follows:

- Managing risks and coordinating a national response associated with specific substances (for example, chemical, biological, radiological and nuclear) and emergencies;
- Ensuring the safety of consumer health products, drugs, drinking water and food;
- Providing essential primary health care, public health protection and health benefits to First Nations and Inuit, consistent with the existing federal role;
- Providing timely health advice and access to emergency health services for the travelling public, internationally protected persons in Canada and provincial and territorial departments of Health;
- Managing controlled substances services (for example, medical marijuana and methadone);
- Providing crisis and strategic communications (for example, public warnings and advisories in times of crisis); and
- Ensuring emergency preparedness and response against infectious disease.

HC and PHAC rely heavily on information technology (IT) systems to deliver critical services to Canadians. Increasingly, business processes are being automated and integrated, with complex and highly efficient IT systems. In most cases, IT systems are an essential business enabler and alternate delivery methods that include manual workarounds are not possible. The flipside of this reliance on IT is the associated risks and the tremendous impact if the risks were ever to materialize. To counter the threats associated with such risks, organizations are progressively evolving and adapting business continuity plans (BCP) to include IT continuity plans to meet their respective business requirements.

A **business continuity plan (BCP)** is part of the departmental security program that will ensure the availability of critical services in an emergency situation. It is the plan to recover from a disruption or disaster, so that normal business operations may be resumed within the predetermined maximum allowable downtime (MAD).

In accordance with section 5.2 of the TB *Policy on Government Security*, departments and agencies are responsible for ensuring the continuity of government operations and services in the presence of security incidents, disruptions or emergencies. Supporting this policy is the Treasury Board of Canada Secretariat (TBS) Operational Security

Standard: Business Continuity Planning. Section 3.1 of this operational standard requires departments and agencies to establish a Business Continuity Planning Program.

The TBS Operational Security Standard: Management of Information Technology Security states that IT continuity planning is an integral part of business continuity planning. One of the objectives of IT continuity planning is to ensure that few or no interruptions occur in the availability of critical IT services and assets referred to as mission critical systems/ applications (MCA). This operational standard also requires departments and agencies to create an IT continuity plan, also known as a disaster recovery plan (DRP).

An **IT continuity plan** covers the restoration, in the event of a disruption or disaster, of IT systems that are essential to the provision of critical services. It provides the capability to restore mission critical systems/ applications within the recovery time objective (RTO) The RTO is the length of time a business can be without data processing availability.

The requirement to identify and manage a list of mission critical systems/applications is one of the most important elements of IT continuity planning. This list has a significant impact on determining priorities and resource allocations important to the development of the IT continuity plans.

The IT continuity plan should outline system and resource priorities, detail recovery procedures and identify information, equipment and personnel requirements, including roles and responsibilities, necessary to restore the MCAs at HC and PHAC that are essential for the delivery of critical services. MCAs are the IT systems or applications that are essential for the delivery of critical services and for which no alternative method of delivery exists; in other words, they are the systems and applications that would cause the most harm to HC and PHAC if they were to become unavailable.

2. Audit objective

The objective of the audit was to assess the management control framework in place to enable IT continuity planning at HC and PHAC for mission critical systems/applications supporting critical services for Canadians.

3. Audit scope

The audit examined the governance, risk management and control practices of the business continuity planning and IT continuity planning function for mission critical systems/applications, in both HC and PHAC, against a set of pre-defined audit criteria (see Appendix A) agreed to prior to the commencement of the examination phase of the audit. The audit included an examination of the validity of the methods used to identify and assess critical services and corresponding systems. In addition, the audit included information technology mitigation strategies supporting critical services and systems, to ensure adequate systems contingency and disaster recovery. Finally, the scope focused on MCAs for all program branches and regions, whether these systems are maintained internally or through contracts or service agreements.

The period under review is from January 2014 to August 2015. However, documents pertinent to the period under audit were reviewed as far back as 2006. Subsequently, the report was also adjusted to reflect events that occurred between August and December 2015.

4. Audit approach

The audit approach included a review of documentation, policies, standards, guidelines, frameworks and business processes. Interviews were conducted in key program areas responsible for providing critical services, as well as with the Departmental Security Officer (DSO), the Business Continuity Planning Coordinator (BCP Coordinator) for HC and PHAC and officials from the Information Management Services Directorate.

HC and PHAC identified and approved 28 mission critical systems/applications (19 for HC and nine for PHAC) in 2011-12[1]. All but five MCAs (see Appendix D) are managed out of the National Capital Region. Of the 28 MCAs, a sample of 11 MCAs in the National Capital Region and in the Manitoba Region was examined to confirm that a comprehensive IT continuity plan was in place. Among the 11 MCAs examined, six reside on the Shared Services Canada IT infrastructure, four on HC/PHAC IT infrastructure and one on a third-party service provider’s IT infrastructure. It should be noted that in total, 23 of the 28 MCAs reside on Shared Services Canada IT infrastructure.

The audit reviewed the roles, responsibilities and accountabilities for key business activities as they relate to business continuity and IT continuity planning. These are illustrated in the RACI (Responsible, Accountable, Consulted and Informed) Chart developed by the audit team for HC and PHAC (see Appendix C).

5. Statement of conformance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion are based on a comparison of the conditions that existed as of the date of the audit, against established criteria that were agreed upon with management. Further, the evidence was gathered in accordance with the Internal Auditing Standards for the Government of Canada and the International Standards for the Professional Practice of Internal Auditing. The audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

[1] At the time of writing this report, the list of MCAs is being updated by HC and PHAC.

B - Findings, recommendations and management responses

1. Governance

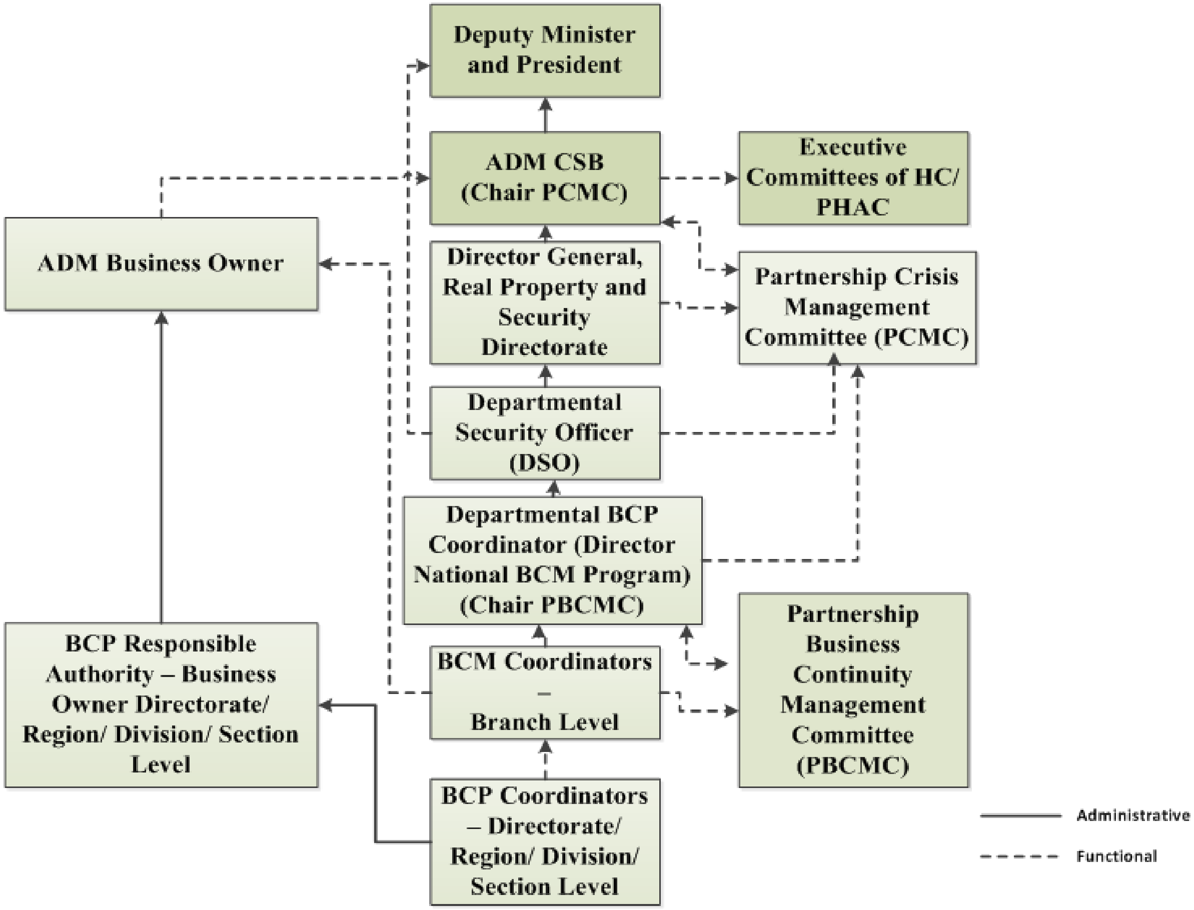
1.1 Governance structure

Audit criterion: A governance structure is in place for IT continuity planning for mission critical systems/applications.

A governance structure to support both business continuity and IT continuity planning for Health Canada (HC) and the Public Health Agency of Canada (PHAC) is essential for the restoration of mission critical systems/applications (MCA) in the event of a disruption or a disaster. The Treasury Board of Canada Secretariat (TBS) has recognized the importance of IT continuity planning. The TBS Operational Security Standard: Management of IT Security (MITS) states that in order to ensure minimal or no interruption in the availability of critical IT services and assets, departments must produce and routinely test and revise an IT continuity plan for each MCA. The TBS Operational Security Standard: Business Continuity Planning Program requires that the Departmental Business Continuity Planning Coordinator provide for regular training, review, testing and audit of MCAs, liaise with other departments and agencies as necessary and collaborate with the IT Security Coordinator throughout the business continuity planning process.

In the last few years, HC and PHAC have made progress in improving their business continuity planning program. As Figure 1 illustrates, HC and PHAC have put in place a governance structure for business continuity planning that covers normal operations but also provides for when there is a business disruption or a crisis situation.

Figure 1: Business continuity planning governance structure


Deputy Minister and President
ADM CSB (Chair PCMC)
Executive Committees of HC/ PHAC
ADM Business Owner
Director General, Real Property and Security Directorate
Partnership Crisis Management Committee (PCMC)
Departmental Security Officer (DSO)
Departmental BCP Coordinator (Director National BCM Program) (Chair PBCMC)
BCP Responsible Authority – Business Owner Directorate/ Region/ Division/ Section Level
BCM Coordinators – Branch Level
Partnership Business Continuity Management Committee (PBCMC)
BCP Coordinators – Directorate/ Region/ Division/ Section Level
Administrative
Functional

The audit focused particularly on two key committees within the business continuity planning governance structure. The Partnership Crisis Management Committee, chaired by the Assistant Deputy Minister (ADM), Corporate Services Branch (CSB), is responsible for the management and governance of the operational response and recovery, as well as the liaison and coordination of interactions within HC and PHAC. The Partnership Business Continuity Management Committee, chaired by the Director of the National Business Continuity Management Program, ensures that all branches and equivalent entities are prepared for business disruptions.

IT continuity planning is a key component of the business continuity program, but it is not well identified or described in the context of the business continuity planning governance structure. Based on a review of documentation (such as minutes and agendas from committee meetings and terms of reference for committees), the audit found few references to IT continuity planning. A review of the past year's agendas and records of decisions for the two key committees highlighted that although meetings were held at the prescribed frequency, the composition of the primary and alternate members was not at the prescribed level and some branches were not represented at the meetings. Although both committees held discussions on the government-wide review of the listing of MCAs led by TBS and Shared Services Canada, the committees did not discuss IT continuity for MCAs.

The audit concluded that a governance structure is in place for business continuity planning; however, improvements are needed so that IT continuity planning for MCAs is integrated into the business continuity planning governance structure and is included as a regular agenda item at the Partnership Business Continuity Management Committee.

Recommendation 1

It is recommended that the Assistant Deputy Minister, Corporate Services Branch, integrate information technology continuity planning into the business continuity planning governance structure, including clearly defining and communicating roles and responsibilities.

Management response

Management agrees with the recommendation.

CSB will clearly define roles and responsibilities for IT continuity planning, incorporate them into the governance structure and communicate them to the Health Partnership business continuity management committees.

1.2 Roles and responsibilities

Audit criterion: Roles and responsibilities are defined, communicated and carried out for IT continuity planning for mission critical systems/applications.

In accordance with the TB *Policy on Government Security*, the continued delivery of government services must be assured through baseline security requirements identified during business continuity planning, including IT continuity planning and continuous risk management. Clear roles and responsibilities are essential for an effective business continuity planning program.

The roles and responsibilities are well defined for business continuity planning in HC and PHAC’s draft Business Continuity Management (BCM) Roles and Responsibilities. However, the roles and responsibilities of the key stakeholders for IT continuity planning are not clearly defined or understood. The key stakeholders are the business owners, the Departmental Security Officer (DSO), the departmental and branch business continuity planning coordinators (BCP coordinator), the Chief Information Officer (CIO) and the Departmental IT Security Coordinator (DITSC). The DSO is responsible for ensuring that business continuity, including IT continuity, is integrated into the broader security program for HC and PHAC. The CIO has a key role to play by working closely with the DSO and the BCP coordinators by ensuring that there is effective IT continuity across HC and PHAC.

A RACI (Responsible, Accountable, Consulted, Informed) chart was developed by the audit team at the beginning of the audit, based on internationally recognized best practices in the field of IT continuity planning. The purpose of the RACI chart is to identify and clarify accountabilities and roles and responsibilities of the key stakeholders for business and IT continuity planning. The RACI chart was shared with the Director of the National Business Continuity Management Program, the DSO, the DITSC, the CIO and other officials from the Information Management Services Directorate (IMSD). Numerous comments were received, and the chart in Appendix C represents the consensus reached in regards to accountabilities and responsibilities for IT continuity planning.

The HC and PHAC IT Security Directive clearly identifies that the DITSC is required to play a key role in continuity planning at HC and PHAC. This role is important to help bridge the current gap, namely the lack of integration between business continuity planning and IT continuity planning at HC and PHAC. The audit noted that the role of the DITSC has not been included in the draft Business Continuity Management Roles and Responsibilities. The DITSC's responsibilities should include the development of IT continuity plan standards, guidelines, models, processes and tools, supporting the Business Continuity Management (BCM) Program, providing training to support the IT continuity plan and maintaining a database of completed IT continuity plans. These roles and responsibilities are not currently carried out by the DITSC or anyone else at HC or PHAC.

In conclusion, although roles and responsibilities for business continuity planning are well defined, IT continuity planning roles and responsibilities for all key stakeholders are not clearly defined and communicated (see Recommendation 1).

1.3 IT continuity planning alignment with business continuity planning

Audit criterion: IT continuity planning for mission critical systems/applications is integrated with business continuity planning.

The TBS Management of Information Technology Security (MITS) Standard specifies that IT continuity planning is an integral element of business continuity planning. The draft HC/PHAC *Business Continuity Management Policy* specifies that the Chief of the National Business Continuity Management Program (NBCMP) is responsible for ensuring that IT continuity plans and arrangements are fully integrated into the NBCMP.

The audit noted the absence of integration between IT continuity planning and business continuity planning. The branch and departmental BCP coordinators have not confirmed the existence of an IT continuity plan for each MCA once the business continuity plan (BCP) and the business impact analysis (BIA) has identified a system or application as being essential for the delivery of a critical service. Interviews with business owners confirmed that they were not asked to validate the existence of an IT continuity plan for each of their MCAs included in the BCP and BIA.

A review of the annual report to the Assistant Deputy Minister, Corporate Services Branch, identifies the BCP completion rate for HC and PHAC, although the report does not mention the percentage of completion for the IT continuity plans. The reporting process was established to ensure continued operations and availability of critical services to Canadians during a period of disruption or disaster. However, if IT continuity plans are not in place and this information is not included in the report, senior management is thus provided with an incomplete picture of HC's and PHAC's ability to deliver critical services in the event of a disruption or disaster.

Interviews with Branch Business Continuity Coordinators, the Director of the NBCMP, the DSO and officials from IMSD indicated that there was no challenge function in place to ensure that IT continuity planning is integrated with the business continuity planning. For example, the BCP template has a section entitled "Alternate Site". This information is required for those systems and applications deemed mission critical. However, only in a few instances is information provided in this section. A review of several BIAs and BCPs revealed that they do not clearly identify the critical dependencies, including mission critical systems and applications, which act as a means to identify the need for an IT continuity plan.

More effort is required to integrate IT continuity planning with business continuity planning, so that all MCAs are properly identified and have an IT continuity plan (see Recommendation 1**)**.

1.4 IT continuity strategy

Audit criterion: A departmental IT continuity strategy is in place and aligned with the overall Business Continuity Management program.

An IT continuity strategy aligned with the overall Business Continuity Management (BCM) program and the enterprise view (Government of Canada) of disaster recovery by Shared Services Canada would provide guidance and direction to business owners in the event of a major disruption or disaster. This strategy could include to the following, among others: an analysis of continuity requirements, to identify possible strategic business and technical options; a list of who should be providing approval to selected strategic options; the conditions and owners of key decisions that will cause the IT continuity plans to be invoked; the resource requirements and costs for each strategic technical option and strategic recommendation; plans for transitioning HC and PHAC back to a normal state after recovery; and a review of business continuity and IT continuity plans to ensure that they are aligned with changes in people, processes, technology and the overall operating environment.

The IT Security Directive for HC and PHAC indicates that IT continuity planning should be integrated with business continuity planning, but there is no IT continuity strategy describing how this could be achieved. HC and PHAC IT Plans (2015-18) and the IM/IT Strategic Plan (2013-15) were reviewed and interviews with the Departmental Security Officer and the Director of NBCMP confirmed that no overall IT continuity strategy exists for HC and PHAC. Several business owners interviewed indicated that a departmental IT continuity stand-alone strategy, or one that is integrated in HC and PHAC IT Plans or the IM/IT Strategic Plan, would be useful for establishing departmental priorities, resource allocations, direction and guidance in the event of a major disruption to operations. Business owners are looking to IMSD for more direction and guidance in this area. The CIO is best positioned to

develop the overall IT continuity strategy for HC and PHAC because of the subject matter expertise; however, business owners should be consulted in the process.
While an IT continuity strategy is not a TB requirement for HC and PHAC, it would be beneficial for the two organizations to identify priorities, set direction and provide guidance to business owners in the event of a crisis.

2. Risk management

2.1 Risk management

Audit criterion: Risks related to IT continuity planning for mission critical systems/applications are identified, assessed and mitigated.

The TB *Policy on Government Security* includes continuous risk management as an essential element of IT continuity planning. The TBS Framework for the Management of Risk indicates that deputy heads are responsible for monitoring risk management practices in their organization, as well as considering risks that arise when partnering with organizations within and external to the federal government.

The lack of an IT continuity plan, as noted in many of the threat and risk assessments examined, has been identified as a risk for several of the MCAs. The audit found no evidence to indicate that this risk was considered at the organizational level. In 2012-13, HC and PHAC prepared a self-assessment against the TBS Management of IT Security Standard. The assessment identified some gaps with respect to business continuity planning and IT continuity planning, noting the development and maintenance of IT continuity plans as being partially compliant and stating that although BCPs exist, plans for the recovery of systems have not yet been fully developed or are not regularly tested.

In addition, a review of the Corporate Risk Profile, IT Plans and IM/IT Strategic Plan for HC and PHAC found no reference to risks related to IT continuity planning for MCAs. As well, many MCA business owners have identified a critical dependency on Shared Services Canada (SSC) as a risk. SSC now manages the IT infrastructure supporting most of the MCAs, which had previously been managed by the business owners.

Lastly, several interviews with key stakeholders indicated the lack of resources, the transfer of the IT infrastructure to SSC and other competing priorities as the most common reasons why risks related to IT continuity planning have not been addressed.

While IT continuity planning for MCAs has been identified and documented as a risk by several stakeholders, this risk is not recognized in either the IT Plan or the IM/IT Strategic Plan for HC and PHAC.

Recommendation 2

It is recommended that the Assistant Deputy Minister, Corporate Services Branch, ensure that risks related to information technology continuity planning be further assessed and included in the information technology plans for HC and PHAC.

Management response

Management agrees with the recommendation.

CSB will further assess risks associated with IT continuity planning and record them in the IT plans for HC and PHAC.

2.2 Threat and risk assessments

Audit criterion: Complete and up-to-date threat and risk assessments exist for all mission critical systems/applications.

The TBS Operational Security Standard: Management of Information Technology Security requires that departments have their systems certified and accredited before approving them for operation. An up-to-date threat and risk assessment (TRA) provides key certification evidence for a system to receive:

- Full authorization – no restrictions to operate;
- Interim authority to operate (IAO) – time-limited authority for a business owner to address a medium to high risk either update the existing TRA or develop a new TRA;
- No Authorization to operate.

A TRA assesses the risks associated with the system and makes suitable recommendations to address the risks. The Security Assessment and Authorization Report, signed by the DITSC, the CIO and the business owner, confirms acceptance of any residual risk associated with the system.

The audit noted that in the majority of cases examines, the TRAs for MCAs do not exist or are not up-to-date. A TRA is considered outdated when significant changes have occurred to the infrastructure of the system since it was conducted. In addition, the majority of the TRAs sampled identified IT continuity as a medium or high risk. The audit also noted that nine of the eleven MCAs examined were granted an IAO with the proviso that the business owners mitigate the medium and high risks or update the TRA. In addition, it was noted that for most of the TRAs, there were no action plans to mitigate risks, particularly those risks rated as medium and high.

While it is the responsibility of each business owner to have an up-to-date TRA for each of their systems and applications, IMSD has a plan to update all TRAs for mission critical applications by December 31, 2015, prior to the expiry of the IAOs. IMSD is working to move all of HC and PHAC MCAs into a state where each system has a valid and full authorization to operate. Among the drivers for this initiative are compliance requirements with the TBS Operational Security Standard: Management of Information Technology Security and the current Security Management Accountability Framework, which focuses on full authorization for MCAs.

In conclusion, TRAs exist for all MCAs but they are not up-to-date. Further, there are few action plans to mitigate the risks identified in the TRAs.

Recommendation 3

It is recommended that the Assistant Deputy Minister, Corporate Services Branch:

- **Communicate to other branches the requirement for up-to-date threat and risk assessments and action plans for all mission critical systems/applications;**
- **Ensure that the Departmental Information Technology Security Coordinator monitor compliance with the requirement and report on the results at least annually; and**
- **Ensure that no new mission critical applications be released for production without an authority to operate.**

Management response

Management agrees with the recommendation.

As part of the annual validation process, CSB will communicate to branches the requirement for up-to-date threat and risk assessments (TRA) for all mission critical systems and applications (MCA).

CSB will monitor compliance for all TRAs for MCAs and report the results at least annually to HC and PHAC Executive Committees.

Branch ADM owners of MCAs will ensure that an up-to-date TRA is completed for each approved MCA under their responsibility.

CSB will implement a process whereby the Chief Information Officer (CIO) approves the Security Assessment and Authorization Report (SAAR) prior to an MCA moving into production.

3. Internal controls

3.1 Identification of mission critical systems/applications

Audit criterion: Systems and procedures are in place to identify and manage mission critical systems/applications.

The requirement to identify and manage a list of MCAs is one of the most important elements of IT continuity planning because it has a significant impact on determining priorities and resource allocations. There should be a formal process in place to identify, manage and approve MCAs at HC and PHAC. This process should include but not be limited to the following: a mapping of systems and applications to critical services; identification of dependencies for critical services; verification and validation of recovery time objectives (RTO) established by business owners; the identification of alternate service delivery methods; and the existence of an IT continuity plan. One of the key outputs of the business continuity process is to help produce the list of MCAs to be approved by senior management. The list of MCAs should be updated regularly to reflect changes in technology, legislation and business processes.

The current official list of 28 MCAs (19 for HC and nine for PHAC) was approved in 2011-12 by HC and PHAC (see Appendix D). The audit noted that a number of these MCAs do not meet the definition of an MCA and should not have been included on the list. HC and PHAC could not provide the audit team with the process that was followed to develop the 2011-12 list; the documentation could not be located and staff involved in the process are no longer available. The audit found that there is a lack of understanding of what constitutes an MCA. As well, there is a tendency among business owners to over-rate the criticality of their systems or applications in the belief that they will receive more attention in the event of a disruption, without realizing the resource requirements that are triggered when an application is deemed to be mission critical. The various lists that have been produced and circulated by HC and PHAC since 2011-12, with the number of MCAs ranging from 21 to 94, illustrate this lack of understanding.

An exercise to update the list of MCAs at HC and PHAC is currently underway, but it had not been completed by the end of the audit examination phase. As of August 2015, the list of MCAs was reduced from 28 to 21 (14 for HC and seven for PHAC), pending approval from senior management. The audit team was provided with some elements that were used in the current exercise to update the list of MCAs. However, there is little documentation to support the revised list of MCAs because as noted earlier, this exercise is still in progress.

The audit noted some concerns about the current exercise to update the list of MCAs.

- Several business owners confirmed that while they were asked to update their list of MCAs, there was little discussion or validation as to why some MCAs were not included in the revised list.

- In one case, the BIA identified an application as being mission critical, but it was not included in the revised list of 21 MCAs. On several occasions, the business owner of the Radiation Surveillance Division Science Network system asked that this application be added to the list of MCAs. The business owner believes it is an MCA and has no intention of modifying the BIA.

- The current exercise was conducted in an iterative and ad hoc manner and is not fully documented at this time.

Unless the process is formalized, it is unlikely that the current exercise will result in a process that is repeatable and can be used to produce timely updates to the list of MCAs.

In conclusion, the systems and procedures to identify and manage MCAs are not fully documented.

Recommendation 4

It is recommended that the Assistant Deputy Minister, Corporate Services Branch, document the process for identifying and approving the list of mission critical systems/applications at HC and PHAC.

Management response

Management agrees with the recommendation.

CSB will document a process for identifying and approving MCAs at HC and PHAC.

3.2 Service level agreements

Audit criterion: Service level agreements or other formal business arrangements are in place and describe the expected service levels to which MCAs will be restored in the event of a disruption or disaster.

The TBS Guideline on Service Agreements – Essential Elements strongly recommends that departments establish service level agreements for any type of client or service provider or collaborative service relationship. Service agreements serve three primary functions:

- Articulate the expectations of the parties to the agreement;
- Provide a mechanism for governance and issue resolution; and
- Act as a scorecard against which to examine performance and results.

Service level agreements between HC, PHAC and third-party service providers, including Shared Services Canada (SSC), should be in place for the IT continuity of MCAs.

The audit noted that separate business arrangements are in place between SSC and PHAC and SSC and HC. The purpose of these business arrangements is to describe, in general terms, the ongoing business relationship between SSC and partner organizations. Its aim is to ensure that accountabilities related to the ongoing delivery of common infrastructure services for all organizations are clear and that the expectations and commitments of both SSC and partner organizations are well understood and documented. Although the business arrangement does mention business continuity and disaster recovery, it does not mention service levels, thereby leaving recipients with uncertain expectation levels. The audit noted that only PHAC and SSC have signed the business arrangement.

It should also be noted that even if systems or applications do not reside on the HC or PHAC IT infrastructure, there is still a dependence on SSC for approvals related to system upgrades, replacement of equipment, security software and other IT-related requirements. The audit did not review the timeliness of approvals in these circumstances.

In February 2015, SSC developed an Operations Service Management Manual – Incident Management. Included in this document are key performance indicators related to target resolution times for critical and high priorities. However, the business arrangement and the SSC Operations Manual do not provide assurance that MCAs will be restored within the prescribed RTOs specified by application business owners. For example, business owners of the Sexually Transmitted Infectious (STI) and Medical Records Chart (MRC) databases, whose systems reside on the SSC IT infrastructure, indicated that their systems were unavailable for periods greater than the RTOs specified in the BIA. The STI database was unavailable for seven weeks in July 2014 due to the Windows 7 configuration upgrade and the MRC database was unavailable for one week in December 2014 for reasons unknown to the business owner. Both of these MCAs have RTOs of less than 24 hours. The business owners confirmed that SSC did not restore these MCAs within the RTOs.

Lastly, it should be noted that 23 of the 28 mission critical systems and applications (18 MCAs for HC and five MCAs for PHAC) reside on the SSC IT infrastructure. Therefore, HC and PHAC are highly dependent on SSC to restore these critical systems and applications.

In conclusion, without a service level agreement in place that defines and clarifies expected service levels, business owners have no assurance that their MCAs can be restored as per the stated RTO in the event of a disruption or disaster, thus leaving some uncertainty for business owners that they can deliver critical services.

Recommendation 5

It is recommended that the Assistant Deputy Minister, Corporate Services Branch, in collaboration with the business owners, ensure that a service level agreement or other formal business arrangement be put in place with service providers, describing service levels for the restoration of mission critical systems and applications.

Management response

Management agrees with the recommendation.

CSB will work with branches to identify service providers, to ensure that service level agreements (SLA) or other formal business arrangements are in place for the restoration of MCAs.

3.3 Preparation and maintenance of IT continuity plans

Audit criterion: A comprehensive IT continuity plan reflecting current business needs and technology exists for each mission critical system/application.

The TBS Operational Security Standard: Management of Information Technology Security recognizes that IT continuity planning is an integral element of business continuity planning. As well, the TBS Operational Security Standard: Business Continuity Planning Program requires that IT continuity plans be fully integrated into the business continuity planning program. Neither TBS nor HC or PHAC has developed a guide for the development of IT continuity plans. Public Safety Canada is responsible for developing an approach for emergency management for the Government of Canada. It has developed a Guide to Business Continuity Planning, which provides information on creating a business continuity plan. The guide does not include IT continuity planning. In the absence of TBS or departmental guidance regarding what should be included in an IT continuity plan, the audit used internationally recognized best practices to establish what constitutes a comprehensive IT continuity plan. Thus, each MCA should include the following key elements:

- A plan objective based on risk and an understanding of potential business impact;
- Standard operating procedures for recovery and restoration;
- Roles and responsibilities for the disaster recovery team;
- A contact list of individuals responsible for recovery and restoration;
- Testing of the IT continuity plan, including documentation of results;
- Maintenance and update of the IT continuity plan on a regular basis;
- Training of individuals responsible for implementing the IT continuity plan; and
- An alternate processing site.

Of the eleven MCAs examined (six for HC and five for PHAC), only one has an IT continuity plan. It was noted that a majority of the key documents necessary for the preparation of an IT continuity plan are missing, obsolete or incomplete**.** This observation is based on a review of key documents that are essential to the development of an IT continuity plan, such as business continuity plans, a business impact analysis, the statement of sensitivity, the threat and risk assessment and the security assessment and authorization report.

Figure 2 summarizes what was found for the 11 mission critical applications that were reviewed. Appendix E provides a brief description of each MCA.

Figure 2: Mission critical systems/applications reviewed

	Mission Critical Systems/Applications	BCP	BIA	SOS	TRA	SAAR	DRP
1	Health Canada Internet	🟡	🔴	🔴	🔴	🟢	🔴
2	PHAC Internet	🟡	🔴	🔴	🔴	🟢	🔴
3	Medical Records Chart (MRC) Index	🔴	🔴	🟡	🔴	🟢	🔴
4	Sexually Transmitted Infections (STI) database	🔴	🔴	🟢	🔴	🟢	🔴
5	Federal Nuclear Emergency Plan (FNEP) System	🟢	🟢	🟢	🟡	🟢	🟡
6	Drug Products Database (DPD) and DPD Online Query	🟡	🟡	🟡	🟡	🟢	🔴
7	Medical Devices System (MDS)	🟡	🟡	🟡	🔴	🟢	🔴
8	Global Public Health Intelligence Network (GPHIN)	🔴	🔴	🟡	🔴	🟢	🟡
9	Laboratory Information Management System (LIMS)	🔴	🔴	🟢	🟢	🟢	🟡
10	Canadian Network for Public Health Intelligence (CNPHI)	🔴	🟡	🟢	🟡	🟢	🟡
11	Bionumerics	🔴	🔴	🟢	🟢	🟢	🟡

🟢 Criteria met. Document exists, is up-to date and is mostly complete.

🟡 Criteria is partically met. Document exists, but it is not up-to-date or is missing some key elements

🔴 Criteria not met. Document does not exist, is very out-of date or is mostly incomplete

Legend: BCP – Business continuity plan; BIA – Business impact analysis; SOS – Statement of sensitivity; TRA – Threat and risk assessment; SAAR – Security assessment and authorization report; DRP – Disaster recovery plan

Of the reviewed 11 MCAs, four were managed internally by the client, one was managed through a third-party service provider and six resided on the SSC IT infrastructure. Only one application tested, the Federal Nuclear Emergency Plan system, had a document entitled IT continuity plan; however, the plan was not signed and did not include all of the elements of an IT continuity plan such as data recovery procedures, emergency contact list and a continual update of the IT continuity plan based on test results. Similarly, elements such as data recovery procedures were found in a separate stand-alone document entitled Standard Operating Procedures. Other MCAs tested, such as the Global Public Health Intelligence Network, the Laboratory Information Management System, the Canadian Network for Public Health Intelligence and Bionumerics, also had stand-alone documents for recovery procedures. The remaining six applications and systems identified as mission critical had neither an IT continuity plan nor even elements of an IT continuity plan.

Of note, the departmental Business Continuity Planning Database, which could be used for identifying MCAs, is not up-to-date, nor does it provide sufficient information to determine the existence of an IT continuity plan. A review of the documents in the database revealed that they were either out-of-date and in many cases, the required documents were missing. In addition, business owners found that working with the database was difficult. The National Business Continuity Management Directorate has recognized the problems with the database and has a plan to address these issues.

Finally, for the MCAs residing on the SSC IT infrastructure, HC and PHAC have not received assurance from SSC that a comprehensive IT continuity plan exists and that MCAs can be restored within the predetermined RTO. While some elements of an IT continuity plan exist for a few MCAs, comprehensive IT continuity plans have not been developed for the sample of MCAs tested.

Recommendation 6

It is recommended that the Assistant Deputy Minister, Corporate Services Branch:

- **Communicate to business owners the requirement for a comprehensive IT continuity plan for all mission critical systems/applications; and**
- **Monitor compliance with the requirement and report on the results at least annually.**

Management response

Management agrees with the recommendation.

CSB will develop requirements for IT continuity plans for all MCAs, communicate them to business owners, monitor compliance and report on them annually.

IT continuity plans for each MCA to be reviewed, updated and exercised on an annual basis by the branch ADM owners of the MCAs.

C - Conclusion

The audit concluded that IT continuity planning for MCAs requires improvement in order to ensure that critical services are available in the event of a disruption or disaster.

Improvements are required to integrate IT continuity planning into the business continuity planning governance structure; to define and communicate more clearly the roles and responsibilities of key stakeholders involved with IT continuity planning; to assess and mitigate further the IT continuity planning risk; to ensure that threat and risk assessments are up-to-date for all MCAs; to document and approve the process for identifying MCAs; to put in place a service level agreement between Shared Services Canada and Health Canada (HC) and the Public Health Agency of Canada (PHAC) that identifies service levels and commitments for the restoration of MCAs; and to develop comprehensive IT continuity plans for all MCAs.

Improvements in these key areas will serve to strengthen IT continuity planning and prepare HC and PHAC in the event of a disruption to operations.

Appendix A – Lines of enquiry and criteria

Audit of IT Continuity Planning for Mission Critical Systems/Applications		
Criteria Title		**Audit criteria**
Line of enquiry 1: Governance		
1.1	Governance structure[2,4,10]	A governance structure is in place for IT continuity planning for mission critical systems/applications.
1.2	Roles and responsibilities[2,4,10]	Roles and responsibilities are defined, communicated and carried out for IT continuity planning for mission critical systems/ applications.
1.3	IT continuity planning alignment with business continuity planning[2,3,4]	IT continuity planning for mission critical systems/applications is integrated with business continuity planning.
1.4	IT continuity strategy[2,4]	A departmental IT continuity strategy is in place and aligned with the overall Business Continuity Management program.
Line of enquiry 2: Risk management		
2.1	Risk management[3,4,7]	Risks related to IT continuity planning for mission critical systems/applications are identified, assessed and mitigated.
2.2	Threat and risk assessments[3,4]	Complete and up-to-date threat and risk assessments exist for all mission critical systems/applications.
Line of enquiry 3: Internal controls		
3.1	Identification of mission critical systems/ applications[1,4]	Systems and procedures are in place to identify and manage mission critical systems/applications.
3.2	Service level agreements[4,6]	Service level agreements or other formal business arrangements are in place and describe the expected service levels to which MCAs will be restored in the event of a disruption or disaster.
3.3	Preparation and maintenance of IT continuity plans [2,3,4,8,9,11]	A comprehensive IT continuity plan reflecting current business needs and technology exists for each mission critical system/application.

[1] TB *Policy on Government Security*
[2] TBS Operational Security Standard – Business Continuity Planning Program
[3] TBS Operational Security Standard – Management of Information Technology Security (MITS)
[4] COBIT 5 – ISACA
[5] Shared Services Canada – Integrated Business Plan
[6] TBS Guideline on Service Agreements – Essential Elements
[7] TBS Integrated Risk Management Framework
[8] Draft HC/PHAC Business Continuity Management Roles and Responsibilities
[9] HC/PHAC Business Continuity Management – Business Impact Analysis – User Guide
[10] HC/PHAC IT Security Directive
[11] Public Safety Canada - Guide to Business Continuity Planning

Appendix B – Scorecard

Audit of IT Continuity Planning for Mission Critical Systems/Applications

Criterion	Rating	Conclusion	Rec #
Governance			
1.1 Governance structure	🟨	While there is a governance structure in place for business continuity planning, HC and PHAC would be better served by integrating IT continuity planning for mission critical systems/applications (MCA) into the business continuity planning governance structure.	1
1.2 Roles and responsibilities	🟧	Roles and responsibilities for business continuity planning are well defined; however, IT continuity planning roles and responsibilities for all key stakeholders should be more clearly defined and communicated.	Ref. 1
1.3 IT continuity planning alignment with business continuity planning	🟧	More effort is required to integrate IT continuity planning into business continuity planning, so that all MCAs are properly identified and have an IT continuity plan in place.	Ref. 1
1.4 IT continuity strategy	🟢	While an IT continuity strategy is not a Treasury Board of Canada requirement, it would be beneficial for the two organizations to identify priorities, set direction and provide guidance to business owners in the event of a crisis.	-
Risk management			
2.1 Risk management	🟨	While IT continuity planning for MCAs has been identified and documented as a risk by several stakeholders, it needs to be identified in the IT Plan and the IM/IT Strategic Plan for HC and PHAC.	2
2.2 Threat and risk assessments	🟧	Threat and risk assessments (TRA) exist for all MCAs but they are not up-to-date. Further, there are few action plans to mitigate the risks identified in the TRAs.	3
Internal controls			
3.1 Identification of mission critical systems/applications	🟧	The systems and procedures to identify and manage mission critical systems/applications are not fully documented.	4
3.2 Service level agreements	🟨	There is no service level agreement in place with Shared Services Canada that defines and clarifies expected service levels for the restoration of MCAs. Business owners have received no assurance that their MCAs can be restored as per the stated recovery time objective in the event of a disruption or disaster.	5
3.3 Preparation and maintenance of IT continuity plans	🟧	While some elements of an IT continuity plan exist for a few MCAs, comprehensive IT continuity plans have not been developed for most MCAs.	6

🟩	🟢	🟨	🟧	🟥	⬜
Satisfactory	Needs Minor Improvement	Needs Moderate Improvement	Needs Improvement	Unsatisfactory	Unknown; Cannot Be Measured

Appendix C – RACI Chart (Responsible, Accountable, Consulted, Informed)

Information Continuity Planning for Mission Critical Systems/Applications
RACI Chart (Responsible, Accountable, Consulted, Informed)

	Key Management Practices	HC Deputy Minister/ PHAC President	EC Committees - Health Canada and PHAC	ADM Corporate Services Branch	ADM Business Owner	Responsible Business Authority - Business Owner	Departmental Security Officer	Partnership Crisis Management Committee (PCMC)	Departmental BCP Coordinator - NBCMP	BCP Coordinator - Directorate/Division/Section Level	Chief Information Officer	IT Security Coordinator (ITSC)	TBS Chief Information Officer Branch (CIOB)	Shared Services Canada
1	Define the Business Continuity Planning Standard for the Government of Canada (GOC)	I		I	I	I	I	I	I		I	I	R&A	C
2	Develop an enterprise (i.e. GOC) view of Disaster Recovery and Business Continuity	I			I	I	I	I	I		C		C	R&A
3	Define and manage a Dept/Agency business continuity planning program	I	I	A	I	I	R	I	R	C	C	C	I	
4	Develop an IT continuity strategy for the Dept/Agency	I	I	A	I	I	C	I	C	I	R	I	I	
5	Prepare and maintain BCP's and BIA's			I	A	R	I	I	C	C		C	I	I
6	Prepare and maintain a list of Mission Critical Applications (MCA) for the Dept/Agency	I	A	I	C	C	C		R		C	C	I	I
7	Prepare an IT Continuity Plan/ Disaster Recovery Plan (DRP) for each mission critical application	I	I	I	A	R	C	I	C	I	C	C	I	R*or C
8	Train personnel, test and review the IT Continuity Plan for each MCA				A	R	I	I	I	C	C	I		R*

*: Only for the SSC IT Infrastructure

R:	**R**esponsible: person who performs an activity or does the work.
A:	**A**ccountable: the person who has overall accountability for getting the task done and has Yes/No/Veto
C:	**C**onsulted: the person who provides input to the activity.
I:	**I**nformed: the person who is receiving the information and needs to know of the decision or action.

Source: Developed by the Office of Audit and Evaluation and agreed to by the Corporate Services Branch.

Appendix D – List of mission critical systems/applications as of 2011-12

Legend:

CPAB	-	Communications and Public Affairs Branch
CSB	-	Corporate Services Branch
FNIHB	-	First Nations and Inuit Health Branch
HECSB	-	Healthy Environments and Consumer Safety Branch
HPFB	-	Health Products and Food Branch
HSIB	-	Health Security Infrastructure Branch
IDPCB	-	Infectious Disease Prevention and Control Branch
IMSD	-	Information Management Services Directorate
NML	-	National Microbiology Laboratory
SSC	-	Shared Services Canada

Health Canada				**CRITERIA FOR MEETING MISSION SERVICES****				
No.	**Mission Critical System / Application**	**Client Branch**	**IT Support**	**Health of Canadians**	**Safety of Canadians**	**Security of Canadians**	**Economic Well Being of Canadians**	**Effective Functioning of Government of Canada**
Critical Service 1: Managing risks and coordinating a national response associated with specific substances (for example, chemical, biological, radiological, nuclear) and with emergencies.								
1	Centre and Systems in support of the Federal Nuclear Emergency Plan (FNEP)	HECSB	Client	Yes	Yes	No	Yes	Yes
2	Joint Emergency Preparedness Committee (sub-Committee on Chemical Emergencies); Chemical Emergency Response Unit Inventory; Chemical Emergency Response Unit Incident Report Log	HECSB	SSC/IMSD	Yes	Yes	No	Yes	Yes
3	Labview HCIL/MITES (Health Canada Inhalation Laboratory/ Mobile Inhalation Toxicology Exposure System)	HECSB	SSC/Client	Yes	Yes	Yes	No	Yes
Critical Service 2: Safety of consumer health products, drugs, drinking water and food.								
4	Drug Products Database (DPD) and DPD Online Query	HPFB	SSC/IMSD	Yes	Yes	No	No	Yes

Health Canada				**CRITERIA FOR MEETING MISSION SERVICES****				
No.	**Mission Critical System / Application**	**Client Branch**	**IT Support**	**Health of Canadians**	**Safety of Canadians**	**Security of Canadians**	**Economic Well Being of Canadians**	**Effective Functioning of Government of Canada**
5	Medical Devices System	HPFB	SSC/IMSD	Yes	Yes	No	No	Yes
6	*LIMS-HPFB-HBFBI (LIMS instance for the Health Products and Food Branch Inspectorate)	HPFB	SSC/IMSD	Yes	Yes	Yes	No	No
7	Canadian Adverse Drug Reaction Information System - Canada Vigilance (CADRIS – CVP)	HPFB	SSC/IMSD	Yes	Yes	No	No	Yes
8	Special Access Programme (eSAP)	HPFB	SSC/IMSD	Yes	Yes	Yes	Yes	Yes
9	Emergency Veterinary Drug Release (LIMS-HPFB-VDD-EDR)	HPFB	SSC/Client	Yes	Yes	Yes	No	No
10	*LIMS-HPFB-BGTD (LIMS instance for the Biologics and Genetic Therapies Directories)	HPFB	SSC/Client	Yes	Yes	Yes	No	No
11	Amega Monitoring System	HPFB	SSC/Client	Yes	Yes	Yes	No	Yes
12	Inspection Reporting System (IRS)	HPFB	SSC/IMSD	Yes	Yes	Yes	No	No
Critical Service 3: Essential primary health care, public health protection and health benefits to First Nations and Inuit, consistent with the existing federal role.								
13	Medical Records Chart (MRC) Index (Manitoba Region)	FNIHB	SSC/Client	Yes	Yes	Yes	No	No
14	Sexually Transmitted Infections (STI) database (Manitoba Region)	FNIHB	SSC/Client	Yes	Yes	Yes	No	No
15	Medical Transportation Record System (MTRS)	FNIHB	SSC/IMSD	Yes	Yes	Yes	Yes	Yes
16	Medical Transportation Data Store (MTDS)	FNIHB	SSC/IMSD	Yes	Yes	Yes	No	Yes
Critical Service 5: Manage controlled substances services (for example, medical marihuana and methadone).								
17	SAMM II (Secure Access for Medical Marihuana)	HECSB	SSC/IMSD	Yes	Yes	No	No	Yes
Critical Service 6: Crisis and strategic communications (for example, public warnings and advisories in times of crisis).								
18	Physical Emergency Preparedness and Response ***(application has been decommissioned)***	HECSB	SSC/IMSD					
19	Health Canada Internet Website	CPAB	SSC/CPAB	Yes	Yes	No	No	No

Public Health Agency of Canada				**CRITERIA FOR MEETING CRITICAL SERVICES****				
No.	**Mission Critical System / Application**	**Client Branch**	**IT Support**	**Health of Canadians**	**Safety of Canadians**	**Security of Canadians**	**Economic Well Being of Canadians**	**Effective Functioning of Government of Canada**
Critical Service 2: Safety of consumer health products, drugs, drinking water and food.								
1	Vocera	CSB	SSC/IMSD	Yes	Yes	Yes	No	No
Critical Service 4: Timely health advice and access to emergency health services for the travelling public, internationally protected persons in Canada and P/T Departments of Health.								
2	ES Medical Indent Register	HSIB	SSC/IMSD	Yes	Yes	Yes	Yes	Yes
Critical Service 6: Crisis and strategic communications (for example, public warnings and advisories in times of crisis).								
3	Agency Internet Website	CPAB	SSC/CPAB	Yes	Yes	No	No	No
Critical Service 7: Emergency preparedness and response against infectious disease.								
4	CEPR Drug Rotation Database	HSIB	SSC/IMSD	Yes	Yes	Yes	Yes	Yes
5	Global Public Health Intelligence Network (GPHIN)	HSIB	Third-party IT service provider (Einstein)	Yes	Yes	Yes	No	Yes
6	Integrated Suite of Tools for Operational Processes (iSTOP)	HSIB	SSC/IMSD	Yes	Yes	Yes	Yes	Yes
7	Laboratory Information Management System (LIMS) - Winnipeg	IDPCB	NML- Science Network	Yes	Yes	Yes	No	No
8	Canadian Network for Public Health Intelligence (CNPHI)	IDPCB	NML- Science Network	Yes	Yes	Yes	No	No
9	Bionumerics	IDPCB	NML – Science Network	Yes	Yes	Yes	Yes	Yes

<u>Source of information</u>: IT Security and Solutions Centre IMSD.

*NOTE: Client has advised that there are two references to LIMS because these are two distinct instances of LIMS, with unique datasets.
**The business owners have deemed the system/application supporting the critical service to be mission critical.

Appendix E – Description of mission critical systems/applications tested

No.	Mission Critical System/Application	Description
1 and 2	HC/PHAC Internet Websites	HC and PHAC's Internet and MySource Intranet websites are focal points for strategic advice, planning and implementation of both internal and external communications. In the case of a business disruption, they would play a key role in ensuring that both employees and the Canadian public remain well-informed.
3	Medical Records Chart (MRC) Index	MRC Index is a database used to retrieve patient paper charts at the Percy E. Moore hospital in Manitoba.
4	Sexually Transmitted Infections (STI) Database	The STI database is populated by laboratory results from Manitoba Health where the residence of the client is listed as a First Nations community. It is an Access database that can provide reports as requested, necessary or appropriate.
5	Federal Nuclear Emergency Plan (FNEP) Science Network	The FNEP Science Network is a consolidation of equipment and applications for the preparedness for and response to a radiological event. The FNEP Science Network has three core IT platforms: ARGOS, ArcGIS and SharePoint. ARGOS is used for modelling atmospheric dispersion of radiological substances and dose calculation. ArcGIS is a platform for analyzing, presenting and sharing geospatial data. SharePoint is used as a collaborative platform for sharing information with partners.
6	Drug Products Database (DPD)	DPD is the departmental repository for human pharmaceutical, biological and veterinary drugs, as well as disinfectant products. The database provides information on a number of drugs approved for sale and sold in Canada. The DPD Online Query is a web application that contains information about drugs in Canada accessible on the Internet.
7	Medical Devices System (MDS)	MDS is a database designed to support the Medical Devices Regulations and to ensure that medical devices offered for sale in Canada are safe, effective and of high quality. The system consists of several integrated modules to administer special access to unlicensed products, investigational testing, quality systems certificate validity, authorized importers/distributors and post-market enforcement.
8	Global Public Health Intelligence Network (GPHIN)	GPHIN is a secure, Internet-based "early warning" system that gathers preliminary reports of public health significance in nine languages on a real-time, 24/7 basis.
9	Laboratory Information Management System (LIMS) – National Microbiology Laboratory (NML)	LIMS is used extensively by laboratory technicians, managers, directors and senior executives to capture, analyze and report on all forms of data generated by the diagnostic and research laboratories at the NML in Winnipeg.
10	Canadian Network for Public Health Intelligence (CNPHI) –NML	CNPHI is managed by the NML; it provides a suite of online tools that enable laboratory and epidemiologic collaboration on a range of public health topics.

11	Bionumerics – NML	Bionumerics is the software that is used by PulseNet for the surveillance and investigation of foodborne illness outbreaks (e.g., E. coli and salmonella) that were previously difficult to detect. Through PulseNet, outbreaks and their causes can be identified in a matter of hours rather than days.

Appendix F – List of acronyms and definitions

BCM	Business continuity management
BCP	Business continuity plan
BCP Coordinator	Business continuity planning coordinator
BIA	Business impact analysis
CSB	Corporate Services Branch
DITSC	Departmental IT Security Coordinator
DSO	Departmental Security Officer
DRP	Disaster recovery plan
HC	Health Canada
IAO	Interim authority to operate
IMSD	Information Management Services Division
IT	Information technology
MAD	Maximum allowable downtime
MCA	Mission critical system/application
NBCMP	National Business Continuity Management Program
PBCMC	Partnership Business Continuity Management Committee
PCMC	Partnership Crisis Management Committee
PHAC	Public Health Agency of Canada
RACI	Responsible, Accountable, Consulted and Informed (chart)
RTO	Recovery time objective
SSC	Shared Services Canada
SOS	Statement of sensitivity
SAAR	Security assessment and authorization report
TB	Treasury Board of Canada
TBS	Treasury Board of Canada Secretariat
TRA	Threat and risk assessment

Business continuity planning: the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets.

Business impact analysis (BIA): identifies the organization's mandate and critical services or products; ranks the order of priority of services or products for continuous delivery or rapid recovery; and identifies internal and external impacts of disruptions.

Critical activities: support critical services and whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or the effective functioning of the Government of Canada.

Critical assets: functions that are directly linked to the delivery of a critical service including, but not limited to, IT applications network systems, real property and multimedia.

Critical dependency: service requirement that is necessary to ensure the delivery of a critical service.

Critical service: service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or the effective functioning of the Government of Canada.

Deferred activities: (Level 3 or 4) support deferred services and whose compromise in terms of availability or integrity would result in some loss of business, financial or other losses, but for which most or all activities can be deferred without serious or any consequences.

Disaster recovery plan (DRP): an element of the Business Continuity Planning Program that includes the development of plans, measures, procedures and arrangements (using the business continuity planning methodology) to ensure minimal or no interruption to the availability of critical IT services and assets.

Enablers: internal functions that may support the delivery of a critical activity or a critical asset and could cause serious harm if unavailable. These can be Levels 1 through 4.

Interim authority to operate (IAO): provides authorization that a system/application can remain in service for a determined period of time, pending mitigation of residual risks.

Maximum allowable downtime (MAD): the longest period of time for which a service can be unavailable or degraded before a high degree of injury results.

Mission critical system/application (MCA): information technology system or application that is essential for the delivery of a critical service and for which no alternative method of delivery exists; the systems and applications that would cause the most harm to HC and PHAC if they were to become unavailable.

Recovery time objective (RTO): the duration of time and the service level to which a business process must be restored after a disruption or disaster.

Statement of sensitivity (SOS): identifies and categorizes relevant assets according to their confidentiality, integrity and availability values, based on injuries that may reasonably be expected in the event of a system/application compromise.

Security assessment and authorization report (SAAR): documents the residual levels of risk; the signatories authorize the information system for operation.

Threat and risk assessment (TRA): assesses the threats and system vulnerabilities that could affect the delivery of a program or service; determines the level of risk, based on current safeguards and system vulnerabilities; recommends safeguards to mitigate risk to an acceptable level.