Employment and Social Development Canada
Emploi et Développement social Canada

Unclassified

Audit of Information Technology Continuity Planning

Report

March 2022

Internal Audit Services

Audit of Information Technology Continuity Planning

This publication is available for download at canada.ca/publicentre-ESDC.

It is also available upon request in multiple formats (large print, Braille,
audio cassette, audio CD, e-text diskette, e-text CD, or DAISY),
by contacting 1 800 O-Canada (1-800-622-6232).
By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No. Em20-158/2022E-PDF
ISBN: 978-0-660-43640-1

TABLE OF CONTENTS

1. Background

1.1 Context

The audit of Information Technology (IT) Continuity Planning was included in the 2019-20 departmental Risk-Based Audit Plan.

Employment and Social Development Canada (ESDC) delivered over $120 billion in benefits last year through a wide range of programs and services including Old Age Security (OAS), Canada Pension Plan (CPP), Employment Insurance (EI) and Canada Student Loans. The rise of the COVID-19 pandemic has resulted in the deployment of additional wide-reaching benefit programs, such as Canada Emergency Response Benefit, Canada Emergency Wage Subsidy and Canada Emergency Student Benefit.

These mission critical programs and services run on IT solutions implemented, operated and maintained by the Innovation, Information and Technology Branch (IITB) (application and database-level) with support from Shared Services Canada (SSC) (platform and infrastructure-level).

At ESDC, the practices and activities that ensure restoration of IT solutions are referred to as Disaster Recovery (DR) activities supported by technical recovery plans. These activities and related plans are managed by the Business Operations Sustainability Directorate's Techinical Debt Management/IT Continuity Division within IITB.

The Emergency Management and Business Continuity group led by the Chief Security Officer within the Integrity Services Branch (ISB) coordinates business continuity management activities (e.g., development of business continuity strategies) with branches and regions to ensure individual and overall departmental readiness for continuous operations in the event of a disruption or disaster. While IT Continuity planning is explicitly linked to the Business Continuity Strategy within each departmental program or service, it is a key subset of business continuity planning (BCP).

1.2 Audit Objective

The objective of this audit was to assess governance, risk management and program management activities related to IT continuity planning that address continuous availability of critical applications for departmental programs and services.

1.3 Scope

Of the 19 technical recovery plans in place covering over 122 solutions supporting departmental mission critical programs, the audit team selected four (4) plans for assessment, which cover 89 solutions supporting high impact operations. This sample was deemed most representative as it included plans covering a high number of internal users, external users and solutions. The technical recovery plans in scope are:

- CPP Technical Recovery Plan of Pension Workload Systems (PWS)
- Technical Recovery Plan of Job Bank
- EI Program Technical Recovery Plan of Enterprise Cyber Authentication Services (ECAS), My Service Canada Account (MSCA), My Service Canada Business Account (MSCBA) and Record of Employment (ROE) Web Automated Claims Processing (ACP)
- EI Program Technical Recovery Plan of Unisys Mainframe

The audit was conducted between September 2021 and October 2021.

The audit excluded areas under the responsibility of SSC (e.g., recovery of infrastructure where solutions are hosted, data centres). As well, the audit excluded BCP as this assessment was performed as part of a previous audit.

1.4 Methodology

With assistance from contracted professionals, the audit was conducted using the following methodologies:

- Documentation review and analysis
- Interviews with IITB and ISB

IT continuity planning components were assessed based on a collection of known and recommended tools and resources such as:

- Treasury Board Secretariat’s 2019 Policy on Government Security
- The United States Department of Homeland Security’s Federal Emergency Management Agency (FEMA)
- Public Safety’s 2017 Emergency Management Framework for Canada
- Information System Audit and Control Association (ISACA®) guidance including IT Governance Institute® (ITGI™) framework’s Control Objectives for Information and related Technology (COBIT®) version 4.1.

2. Audit Findings

2.1 IT Continuity Framework

An IT continuity framework is a subset of the enterprise-wide business continuity management process. The framework requires that a Business Impact Analysis (BIA) is completed and technical recovery plans are developed. As well, the framework establishes a strategy to enable the Department to respond to incidents and disruptions in order to continue operation of critical program processes in order to maintain availability of services and information at an acceptable level.

A defined strategic framework that outlines the departmental roadmap on IT continuity activities does not exist

ESDC's business continuity management directive is aligned with the Treasury Board Secretariat's directive on Security Management and provides an overview of the governance, roles and responsibilities. However, a defined strategic framework for IT continuity is not in place.

Without a completed and signed off IT continuity strategy, there is a risk that technical recovery plans and the BCP may be inconsistent and misaligned resulting in the inability of the Department to respond to incidents and disruption in a comprehensive, effective and repeatable manner.

Processes on the creation, maintenance and testing of technical recovery plans lack maturity

While there is evidence that most elements required by an IT continuity framework exist (for example, creation of technical recovery plans, testing of infrastructure or platforms hosting ESDC's solutions), the audit found that processes are ad hoc rather than being defined.

In addition, the audit found that technical recovery plans do not follow a common and structured approach in both content and scope. For instance, certain plans covered single solutions while others covered up to 70 solutions.

There is a risk that controls are either missing or not adequately documented which may hinder the organization's ability to consistently conduct and evaluate the effectiveness of DR activities and make adjustments where required.

Since the IT continuity team was put in place in 2019, there is no evidence that technical recovery plans were presented at governance committees

While progress on DR activities is being reported to governance bodies such as the Architecture Review Committee and the Directors General Advisory Committee, the audit found that presentations were focused on infrastructure and technical debt complexities rather than the continuity of departmental solutions.

Without formal tabling, review and approval of technical recovery plans by governance, the understanding and acceptance of the activities, processes, roles and responsibilities may lack and pose a risk to the effective implementation of the framework. In addition, there is a risk that without a governance review of technical recovery plans, any oversight and decision-making that may be required to address incidents or disruptions may be unclear and difficult to execute.

Recommendations

1. IITB should define a departmental strategic plan on IT continuity based on departmental business continuity planning requirements and document processes related to the framework.
2. IITB should include the IT continuity framework and plans at governance committees for approval as well as to confirm alignment between Business Impact Analysis outputs and technical recovery plans and the enterprise-wide Business Continuity Management, key departmental priorities and strategic initiatives.

Management Response

1. *IITB agrees. Actions are expected to be completed by March 2023.*
2. *IITB agrees. Actions are expected to be completed by September 2022.*

2.2 Risk Management

A BIA identifies the consequences of disruption of a business function or process and gathers information needed to develop recovery strategies. Potential loss scenarios are identified during the assessment of risks. BIA is an assessment that focuses on business impact and determines the recovery time objective (RTO) to provide guidelines for the time required to restore or provide interim services, and recovery point objective (RPO) to provide guidelines on the maximum tolerable data disruption/loss.

There are currently separate business and technical BIAs being created for each program or technical recovery plan

The audit found that IITB acknowledges that there are currently two processes for the development of BIAs and that RTOs and RPOs are determined in two places: IT BIA and program BIA. According to IITB, IT BIAs were initially developed to address the absence of Program BIAs. As this shortfall has now been addressed and ISB is creating program BIAs as part of a repeatable process, IITB will no longer be producing them.

Until a complete review and removal of IT BIA is performed, there is a risk that having two BIAs in place may lead to inconsistencies, misalignment and delays in arriving at one RTO and RPO figure.

BIA documents are not consistently updated

Regarding IT BIA activities, out of the four technical recovery plans sampled which cover 89 critical solutions, only one critical solution has undergone a BIA. However, with regards to the program BIAs, the audit team was able to obtain BIAs that are program specific related to the critical solutions in scope and those reviewed are complete and up to date. IITB is planning to discontinue the practice of conducting IT BIAs, so long as the Program BIA is already available. This would mitigate the risk of developing duplicate BIAs which may lead to inconsistencies, misalignment and delays in arriving at one RTO and RPO figure.

Recommendation

3. IITB should leverage a single up-to-date assessment of business impact that takes into consideration RTOs and RPOs to all critical solutions.

Management Response

3. IITB agrees. Actions are expected to be completed by March 2023.

2.3 Technical Recovery Plans

It is expected that IITB develops plans as part of the IT continuity framework to address the business continuity requirements defined in the departmental BCP. It is also expected that IITB maintains IT continuity plans to reflect solutions and systems changes and modifications within the departmental BCP. Also the plans should be tested periodically, including a comprehensive verification of continuity processes and situational drills to verify the assumptions and alternate procedures outlined within the plans.

Technical Recovery Plans are missing key elements

The audit found that, overall, 11% of the technical recovery plans in place do not have contact details for the technical resources which may affect the ability to reach out to personnel in the event of a service disruption. Furthermore, some plans (e.g., plans covering the Employment History File—EHF, and Corporate Payment Management System—CPMS solutions) are missing critical components (e.g., recovery strategy, architectural diagrams, etc.) which may result in an extended outage in the event of incidents or disruptions.

Plans are not being maintained in a timely manner

The audit found that of the full population of technical recovery plans, 89% are expired, the oldest expiry date being 2018. IITB has developed a schedule to update the outdated technical recovery plans that is linked to DR testing activities currently underway or planned.

Outdated plans may result in a risk of not being able to reach personnel as well as inaccurate reference to technical services resulting in extended operation disruptions.

Testing activities are not up to date

The audit found that there is a process in place for testing solutions as part of infrastructure continuity plan testing conducted by SSC. When a test is scheduled (including tabletop exercises), a change request is submitted for approval by both the technical and business stakeholders at the Director General level.

Interviewees revealed that recent testing activities were conducted on a few solutions, for example the recent functional testing undertaken on CPP and OAS mainframe solutions. In addition, interviewees revealed that lessons learned are being produced for tested solutions and being used to enhance future testing activities.

A schedule that highlights future plans on testing has been developed. Evidence was provided that demonstrates that business owners have been engaged to communicate blackout dates and approve testing time windows. However, no key performance indicators are established to enable reporting on testing effectiveness.

Recommendations

4. IITB should confirm that technical recovery plans:
    a. include roles, responsibilities and accountabilities;
    b. are defined, documented, communicated, and periodically reviewed;
    c. holistically encompass internal and external parties including partners and vendors;
    d. ensure validity of the details (services, solutions, contact details, etc.); and
    e. are reviewed for completeness and include key sections like recovery strategy and architectural diagrams.
5. IITB should expand the scope of testing to include the whole solution (Functional Tests, Production Tests, and Tabletop exercises) to better enable program readiness in a case of a disaster and result in test scenarios that mirror a real-world recovery scenario.
6. IITB should establish key performance indicators to report on the adequacy of testing.

Management Response

4. IITB agrees. Actions are expected to be completed by July 2022.

5. IITB partially agrees, IITB's existing IT Continuity Test Methodology provides the framework for whole solution testing where possible. However, limitations exist in the legacy data centre environments that prevent whole solution production testing. Actions are expected to be completed by March 2023.

6. IITB agrees. Actions are expected to be completed by September 2022.

3. Conclusion

The audit concluded that, overall, without testing the technical recovery plans, it is not clear whether plans will function as expected in the event of a disruption or disaster.

At the governance level, various DR activities are being reported to governance bodies. However, reporting requirements and mechanisms of technical recovery plans within a defined IT continuity framework do not exist and are not adequate to allow for oversight and timely approval of processes.

From a risk management perspective, there is an opportunity to streamline the BIA process to ensure consistency and alignment with the overall BCP program.

There is room for improving the management of the technical recovery plans currently in place. More specifically, maintenance of the plans through a routine review is not in place. IITB is moving in the right direction as they developed a plan maintenance schedule that is linked to the DR testing activities underway.

4. Statement of Assurance

In our professional judgment, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the audit of IT Continuity Planning. The evidence was gathered in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practice of Internal Auditing*.

Appendix A: Audit Criteria Assessment

It was expected that IITB:	Rating
Line of Enquiry A: Governance	
A1 Develops a program/framework for IT continuity to support enterprise-wide business continuity management, including :	
• The mission statement and goals of the IT continuity planning team are in alignment with the Government of Canada and the Department's policies addressing business continuity.	●
• Roles, responsibilities and accountabilities are defined, adequate and communicated to concerned parties including internal and external stakeholders and partners.	◉
• Reporting requirements and mechanisms for IT Continuity Planning exist and are adequate to allow for oversight and timely approval of processes.	○
Line of Enquiry B: Risk Management	
B1 Ensures that the framework requires reliance on risk assessments and Business Impact Analysis (BIA) to determine critical resource requirements, alternative processing strategies and recovery approaches.	◉
B2 Ensures that IT continuity plans contain risk assessment and BIA results to establish business interruption exposures, their probability and impact, and mitigation alternatives.	◉
B3 RTOs have been established to provide guidelines for the time required to restore or provide interim services and RPOs have been established to provide guidelines on the maximum tolerable data disruption/loss.	◉
Line of Enquiry C: Program Management	
C1 Develops plans as part of the IT Continuity Planning program/framework to address the business continuity requirements defined in the departmental BCP, including:	
• Critical applications and supporting platforms have been identified and the required software and data are available for interim processing and restoration, and are in alignment with the departmental BCP.	◉
• Data recovery procedures have been established to ensure availability of data.	◉
• Staff responsibilities, notification, substitution and access procedures are in place to permit the timely assembly of staff and the commencement of interim and/or restoration procedures.	◉
• The recovery plan contains adequate details to permit external IT professionals to implement the plan if staff members are not available.	◉
• Third-party vendors are included in the IT continuity plans.	◉
• Plans are distributed on a need-to-know basis, are securely stored and can be obtained from multiple locations in the event that the primary storage location is compromised.	◉
C2 Maintains IT continuity plans to reflect applications and systems changes and modifications to the departmental BCP, including :	

• Plans are maintained through routine review of plans' components, testing results and linkage to departmental BCP reviews and enhancements.	○
• Plans are reviewed as part of applications and systems enhancements.	⦿
C3 Tests plans periodically including a comprehensive verification of continuity processes and situational drills to test the assumptions and alternate procedures within the plans.	⦿

✪ Best practice
● Sufficiently controlled; low-risk exposure
⦿ Controlled, but should be strengthened; medium-risk exposure
○ Missing key controls; high-risk exposure

Appendix B: Glossary

BCP	Business Continuity Planning
BIA	Business Impact Analysis
ESDC	Employment and Social Development Canada
IITB	Innovation, Information and Technology Branch
ISB	Integrity Services Branch
IT	Information Technology
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SSC	Shared Services Canada