Correctional Service Canada
Service correctionnel Canada

Safety, Respect
and Dignity
for All

La sécurité,
la dignité
et le respect
pour tous

Audit of IMS Disaster Recovery Plan

Internal Audit

378-1-615

April 29, 2009

Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background, Scope and Approach

In order to continue to meet its objectives and the requirements of the Government Security Policy (GSP), CSC developed, through Information Management Services (IMS), Disaster Recovery Plans (DRPs) for its applications identified as critical.

The objective of this audit is to provide reasonable assurance that the management control framework in place to support disaster recovery preparedness for information technology systems is adequate and effective. The audit also reviewed the progress made on the implementation of the DRP-related requirements of the TBS Operational Security Standard on Management of Information Technology Security (MITS) and improvements initiated as a result of a DRP tabletop exercise conducted by IMS in 2005.

The scope of the audit included the IMS DRPs for critical applications, the controls in place at National Headquarters (NHQ) and the Laval facility to support the timely implementation of the DRPs, and linkages of DRPs and Business Continuity Plans (BCPs), although BCPs themselves are outside the scope of the audit. While regions have recently started to develop DRPs, the regional offices have only recently been actively engaged in DRP activities in the context of the DRP tabletop exercises. The scope of the audit therefore included a review of regional DRPs, but on-site visits in each region were not deemed necessary considering the limited DRP-related control activities performed in the regions, and the fact that all critical applications identified are centrally managed at NHQ.

The critical applications, which were identified as critical during the Year 2000 project, and included within the scope of this audit are outlined below:

System/ Application	System Overview	Number of Users
Network	The CSC network infrastructure enables the interaction of CSC staff and partners with the various forms of electronic information stores and applications.	
CEDV2	Common Enterprise Desktop v2 (CEDV2) is the common operating system on all CSC user workstations delivering access to CSC applications.	13,000
Email	Electronic mail (email) is a key messaging system used within CSC.	14,000
OMS	The Offender Management System (OMS) is a computer based application developed for	10,000

	Correctional Service of Canada (CSC) and National Parole Board (NPB) to manage offender-related information. Through the OMS system, CSC is connected to the National Parole Board, RCMP, and CCRA (Immigration) to share relevant offender information.	
IAS	Inmate Accounting System (IAS) is an application used by CSC institution clerks to manage inmates pay and savings accounts (funds).	150
HRMS	The Human Resource Management System (HRMS) is an element of the PeopleSoft application. PeopleSoft is a Commercially Off-The-Shelf (COTS) application frequently used in private and public sectors. It offers a range of products such as Human Resource Management, Financial Management, Management of Materiel and scheduling of Time and Labour.	3,200
IFMMS	The Integrated Financial and Material Management System (IFMMS) is CSC's corporate financial system.	600
Online Pay	The Online Pay application (OLPS) is used by CSC to process payroll data.	
RADAR	RADAR (Reports of Automated Data Applied to Reintegration) is a suite of reports that allows CSC staff and managers to access OMS offender information in a user-friendly manner.	10,000

The approach and methodology used is consistent with the Internal Audit standards as outlined by the Institute of Internal Auditors, and is aligned with the Internal Audit Policy for the Government of Canada. Audit criteria was developed from COBIT 4.1 (www.isaca.org) DS4 requirements, and also include specific DRP-related requirements from the TBS Government Security Policy and supporting Management of IT Security Standard. The audit criteria are included in Annex A.

Conclusion

A number of key controls for the DRP program have been implemented. Namely, CSC has developed a DRP program for critical business applications which includes a dedicated resource, has been based on an established framework, plans for the resumption of critical application services are in place, the program makes use of off-site storage and recovery and also it has been subject to table top testing exercises.

Several areas for improvement to the current DRP program were identified. Formal Service Level Agreements detailing requirements for the availability of systems should be implemented between IMS and its clients, a formal Business Impact Analysis should be completed, a complete fail-over test for all critical applications should be performed, and current efforts to further implement and test DRPs in regions should continue.

Progress has been made on implementing improvements from MITS and the 2005 DRP tabletop exercise. However, further efforts are required to fully meet MITS requirements related to DRP revisions and testing.

Recommendations have been made in this report to address these areas for improvement. Management has reviewed and agrees with the findings contained in this report and a Management Action Plan has been developed to address the recommendations (see Annex C).

1.0 INTRODUCTION

As a federal government agency, Correctional Service Canada (CSC) is responsible for managing institutions of various security levels and supervising offenders under conditional release in the community. CSC is one component of the larger criminal justice system, and works closely with other partners in the Public Safety Canada portfolio, including the Royal Canadian Mounted Police and the National Parole Board, and with all police agencies.

In order to continue to meet its objectives and the requirements of the Government Security Policy (GSP), CSC developed, through Information Management Services (IMS), Disaster Recovery Plans (DRPs) for its applications identified as critical. Due to the importance of the DRP for CSC and the results of the 2006 preliminary risk assessment of the IT function by Internal Audit, the Audit Committee has approved an Audit of the Information Management Services DRP as part of the Internal Audit Branch audit plan for 2008-2009.

IMS has identified within its Security and Project Management Directorate (ITSEC) a Manager responsible for DRP, assigned a Senior Project Officer to DRPs on a full time basis, and has started to review all DRPs available and to conduct tabletop and failover tests to improve upon the current DRPs. While ITSEC is responsible for coordinating, monitoring, testing and standardizing disaster recovery activities, the Infrastructure Services and Operations (ISO) and Systems Development Directorates are responsible for the development and maintenance of DRPs related to IT operations and critical applications. All staff involved in Disaster Recovery (DR) activities centrally report up to IMS, but may be located at NHQ, the alternate processing site in Laval (Quebec), or within the regions or institution that they support.

Business Continuity Planning is the responsibility of the Departmental Security Officer, and he has requested business areas within CSC to develop Business Continuity Plans (BCPs). The BCPs should detail, among other things, the business area’s requirements in terms of IT resources required to ensure the continuity of their business area. IMS is responsible for developing DRPs that address these requirements for IT resources in the event of a disaster.

The critical applications, which were identified as critical during the Year 2000 project, and included within the scope of this audit are outlined below:

System/ Application	System Overview	Number of Users
Network	The CSC network infrastructure enables the interaction of CSC staff and partners with the various forms of electronic information stores and applications.	
CEDV2	Common Enterprise Desktop v2 (CEDV2) is the common operating system on all CSC user workstations delivering access to CSC applications.	13,000
Email	Electronic mail (email) is a key messaging system used within CSC.	14,000
OMS	The Offender Management System (OMS) is a computer based application developed for Correctional Service of Canada (CSC) and National Parole Board (NPB) to manage offender-related information. Through the OMS system, CSC is connected to the National Parole Board, RCMP, and CCRA (Immigration) to share relevant offender information.	10,000
IAS	Inmate Accounting System (IAS) is an application used by CSC institution clerks to manage inmates pay and savings accounts (funds).	150
HRMS	The Human Resource Management System (HRMS) is an element of the PeopleSoft application. PeopleSoft is a Commercially Off-The-Shelf (COTS) application frequently used in private and public sectors. It offers a range of products such as Human Resource Management, Financial Management, Management of Materiel and scheduling of Time and Labour.	3,200
IFMMS	The Integrated Financial and Material Management System (IFMMS) is CSC's corporate financial system.	600
Online Pay	The Online Pay application (OLPS) is used by CSC to process payroll data.	
RADAR	RADAR (Reports of Automated Data Applied to Reintegration) is a suite of reports that allows CSC staff and managers to access OMS offender information in a user-friendly manner.	10,000

2.0 AUDIT OBJECTIVES AND SCOPE

2.1 Audit Objectives

The objective of this audit is to provide reasonable assurance that the management control framework in place to support disaster recovery preparedness for information technology systems is adequate and effective. The audit also reviewed the progress made on the implementation of the DRP-related requirements of the TBS Operational Security Standard on Management of Information Technology Security (MITS) and improvements initiated as a result of a DRP tabletop exercise conducted by IMS in 2005.

2.2 Audit Scope

The scope of the audit was based on an initial risk assessment. As a result, it included the IMS DRPs for critical applications, and the controls in place at National Headquarters (NHQ) and the Laval facility to support the timely implementation of the DRPs. Considering risks identified, the audit also includes the linkages of DRPs and Business Continuity Plans (BCPs), although BCPs themselves are outside the scope of the audit. DRP controls were only tested for design and implementation (i.e. at a point in time) and were not tested for their operating effectiveness (i.e. over a period of time).

While regions have recently started to develop DRPs, the regional offices have only recently been actively engaged in DRP activities in the context of the DRP tabletop exercises. The scope of the DRP therefore included a review of regional DRPs, but on-site visits in each region were not deemed necessary considering the limited DRP-related control activities performed in the regions, and the fact that all critical applications are centrally managed at NHQ. The only on-site visit outside of the National Capital Region (NCR) was at the alternate processing facility in Laval.

3.0 AUDIT APPROACH AND METHODOLOGY

The approach and methodology used is consistent with the Internal Audit standards as outlined by the Institute of Internal Auditors, and is aligned with the Internal Audit Policy for the Government of Canada.

Following an analysis of potential control frameworks to use for the audit, a risk-based audit program was developed from COBIT 4.1 (www.isaca.org) DS4 requirements, and also include specific DRP-related requirements from the TBS Government Security Policy and supporting Management of IT Security Standard (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON-eng.asp). The audit criteria are included in Annex A.

Work was conducted in the NCR between September 2008 and December 2008, and included an on-site visit to the Laval alternate processing facility. Inquiries were held with numerous CSC representatives involved in DRP activities. Testing included a review of directives and guidelines, organizational structure, roles and responsibilities, and observing the tabletop testing exercise conducted for NHQ in November 2008. For NHQ, testing was conducted for the full lifecycle of the DRP; from initial development to testing, training, maintenance and updating. For regions, testing was limited to a review of the regional specific DRPs and a limited number of interviews.

Upon completing fieldwork, the team held a debriefing meeting at National Headquarters with the Chief Information Officer, Information Management Services and the Director, IT Security and Project Management.

4.0 AUDIT FINDINGS AND RECOMMENDATIONS

4.1 Management Control Framework for Disaster Recovery Planning

We assessed the extent to which the management control framework for DRP is in place.

4.1.1 DRP Framework (COBIT DS4.1)

We expected to find a framework that supports enterprise wide DR planning using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of the DRPs. The framework should address the organisational structure, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The DRPs should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

The DRP Framework is appropriately designed with regards to critical applications maintained at NHQ, but not fully implemented as a number of areas for improvement still exist. The framework is not yet sufficiently implemented within regions.

More specifically during our testing we made the following observations:

- *CSC has not formally assessed the adequacy of having only one resource dedicated to DRP activities, which increases the risk that the DRP program is under staffed.*
- *A standard template for regional DRPs and other related documents has not been developed and distributed to CSC Regions to ensure regional DRPs are comprehensive and consistent. For example, most regional DRPs do not identify*

the individuals assigned to various regional DRP responsibilities, and most of the regional DRPs are missing key information such as a listing of critical applications and related recovery time objectives. This lack of consistency increases the risk that recovery efforts will be more difficult to coordinate in the event of a disaster requiring multiple DRPs to be activated.

- *Internal Service Level Agreements detailing requirements for the availability of systems have not been implemented between IMS and its clients, which increases the risk that IMS may not be aware and able to respond to the availability requirements of the business areas.*
- *There is no evidence that any of the DRPs have been approved by senior management, which increases the risk that DRPs may not meet the needs of senior management.*

Recommendation #1:

The Chief Information Officer, Information Management Services should formally assess the adequacy of the level of resources currently assigned to the DRP program.

Recommendation #2:

The Chief Information Officer, Information Management Services should finalize a standard template for documenting, testing and distributing DRPs at a regional level within CSC.

Recommendation #3:

The Chief Information Officer, Information Management Services should ensure that formal Service Level Agreements detailing requirements for the availability of systems be implemented between IMS and its clients across CSC.

Recommendation #4:

The Chief Information Officer, Information Management Services should ensure that all current DRPs are appropriately reviewed and formally approved by the same parties that sign the internal Service Levels Agreements within which availability requirements will be specified. All significant changes to DRPs should also be subject to review and formal approval by management/application owners.

4.1.2 Disaster Recovery Plans, Critical Resources and Recovery & Resumption (COBIT DS4.2, 4.3 &4.8)

We expected to find DRPs based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach. The DRPs should focus attention on items specified as most critical and establish priorities in recovery situations. The DRPs should ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Lastly, we expected to find plans for the actions to be taken for the period when IT is recovering and resuming services.

DRPs have been appropriately designed with regards to critical applications maintained at NHQ, but not fully implemented as a number of areas for improvement still exist. DRPs have not yet sufficiently been implemented within regions.

More specifically during our testing we made the following observations:

- *As CSC relied on the list of critical applications identified for Y2K disaster recovery efforts, no Business Impact Analysis has been conducted, which increases the risk that all critical applications may not have been appropriately identified, and that defined recovery time objectives (RTOs) may not be appropriate. A Business Impact Analysis is typically conducted as part of the BCP process, which falls under the responsibility of the DSO at CSC.*
- *While the DRPs of NHQ critical applications are based on defined recovery time objectives (RTOs), it is not clear if all RTOs can be met, especially in a full disaster situation where all critical applications need to be recovered, which increases the risk that IT resources will not be recovered in time to meet the requirements of the business areas.*
- *There is no guidance available on the timeframe within which a disaster should be declared (RTOs only kick in once a disaster has been declared), which increases the risk that a disaster may not be declared in a timely manner in order to meet the requirements of the business areas.*
- *The DR role and training of staff located at the alternate processing facility (in Laval) has been minimized, and DRPs rely mostly on staff located at NHQ, which increases the risk of further delaying recovery efforts should NHQ staff be delayed in relocating to the alternate site.*
- *While the DRPs could leverage the Staff College located next to the alternate processing facility, the DRPs rely on the availability of rooms in nearby hotels to relocate DR resources from NHQ, which increases the risk of further delaying recovery efforts should NHQ staff be delayed in relocating to the alternate site.*

Recommendation #5:

The Departmental Security Officer (DSO) should ensure that a formal Business Impact Analysis is completed by the business/applications owners to confirm the identification of critical applications and to further confirm that the identified Recovery Time Objectives remain appropriate and relevant.

Recommendation #6:

The Chief Information Officer, Information Management Services should develop a DRP training program specifically aimed at increasing the DRP knowledge of the resources in the alternate processing facility in Laval as a means of expanding the availability of qualified DR resources in the event of a disaster.

4.1.3 Maintenance, Testing and Training of DRPs (COBIT DS4.4, 4.5 & 4.6)

We expected to find implemented change control procedures to ensure that the DRPs are kept up to date and continually reflect actual business requirements, and that changes in procedures and responsibilities are communicated clearly and in a timely manner. We also expected to find regular tests of the DRPs to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plans remain relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Lastly, we expected to find that all concerned parties are provided with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster.

A testing plan has been designed and partly implemented for critical applications and regions, consisting mostly of tabletop tests and limited failover tests. While the regular maintenance of DRPs has been implemented, it is not clear if these updates are addressing all lessons learned from testing performed.

More specifically during our testing we made the following observations:

- *While fail-over tests for three critical applications have been conducted, complete fail-over testing for all critical applications has not occurred, which increases the risk that the defined RTOs may not meet the needs of the business areas, and that current DPRs are missing important steps to permit the full recovery of critical applications.*
- *The capacity of the alternate processing facility to take over all critical applications has not been formally assessed, which increases the risk that critical applications may not be responsive when running at the alternate processing facility.*

- *DRPs are not always being updated on at least a yearly basis as required by IMS guidelines, which increases the risk that DRPs will be outdated and miss critical steps in the recovery of critical applications.*
- *Lessons learned and action plans from testing sessions have not been consistently documented, which increases the risk that problems raised during testing may not have been formally addressed or updated within the DRP. Of the twenty potential improvements identified in the 2005 DRP tabletop exercise, eleven have been implemented (55%), two have been partially implemented (10%), and seven have not yet been implemented (35%).*
- *A training plan does not formally exist. Training of DR resources is essentially accomplished through participation in tabletop testing exercises, but attendance is not mandatory. This increases the risk that staff may not always attend required DRP training.*

Recommendation #7:

The Chief Information Officer, Information Management Services should expand the current testing program and include annual testing of the processing capacity of the alternate processing facility.

Recommendation #8:

The Chief Information Officer, Information Management Services should ensure that all DRP documents are updated at least annually, or following a significant change. As part of the update, the Chief Information Officer should also ensure that the DRPs are formally reviewed and approved by application owners.

Recommendation #9:

The Chief Information Officer, Information Management Services should implement a process to ensure that lessons learned from DRP testing is consistently documented and proactively addressed.

4.1.4 Distribution of DRPs (COBIT DS4.7)

We expected to find that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorized interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.

A limited DRP distribution plan has been designed and implemented at NHQ, but not in the regions. DRPs are available in a central repository at NHQ, and replicated to the alternate processing facility on a daily basis, but areas for improvement exist for DRP distribution processes.

More specifically during our testing we made the following observations:

- *The DRPs do not currently include a comprehensive distribution plan listing all individuals that should have a copy of the most recent DRP and the method of distribution, which increases the risk that DRPs will not be readily available in the event of a disaster.*
- *When we performed our testing, staff located at the alternate processing facility with DR responsibilities could not readily access DR documents, which increases the risk that DRPs will not be readily available in the event of a disaster.*

Recommendation #10:

The Chief Information Officer, Information Management Services should ensure that DRPs include a comprehensive distribution plan listing all individuals that should have a copy of the most recent DRP and the method of distribution, and that staff located at the alternate processing facility has readily access to DR documents.

4.1.5 Offsite Backup Storage (COBIT DS4.9)

We expected to find offsite storage of all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Management of the offsite storage facility should respond to the data classification policy and the enterprise’s media storage practices. IT management should ensure that offsite arrangements are assessed for content, environmental protection and security. Compatibility of hardware and software to restore archived data, and periodically test and refresh archived data should also be ensured.

An offsite backup storage process has been designed and implemented. While some critical applications also rely on data replication to reduce risks of data loss, areas for improvement exist with backup storage processes.

More specifically during our testing we made the following observations:

- *Backup tapes for critical applications and regions are not encrypted, which increases the risk of unauthorized access to the data on the backup tapes, especially while the tapes are in transit from CSC to National Archives or the alternate processing facility.*

Recommendation #11:

The Chief Information Officer, Information Management Services should implement a solution that enables CSC to encrypt backup tapes for application data assessed as sensitive either from a security or from an access to information perspective.

4.1.6 Post-Resumption Review (COBIT DS4.10)

We expected to find that IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.

A post-resumption review process has not yet been formally designed and implemented.

More specifically during our testing we made the following observations:

- *Evidence could not be found that lessons learned from DRP testing and actual incidents and disasters are formally leveraged to make improvements to the DRPs, which increases the risk that DPRs are missing important steps to permit the full recovery of critical applications.*
- *DRPs do not currently include steps for the resumption of activities back to the primary processing facility, which increases the risk of further delaying the resumption to normal IT operations.*

Recommendation #12:

The Chief Information Officer, Information Management Services should ensure that, as part of the DRP, there is either a plan to restore resumptions of activities back to NHQ or a new DRP which would guide DR staff in the event of a disaster at the alternate processing facility (prior to resumption at NHQ).

CONCLUSION:

Overall, CSC has designed and implemented some key elements of the Management Framework for DRP. However, it will be important that CSC establishes Formal Service Level Agreements detailing requirements for the availability of systems between IMS and its clients. To enable the development of such agreements a formal Business Impact Analysis should be completed. In addition, a complete fail-over test for all critical applications should be performed, and current efforts to further implement and test DRPs in regions should continue.

4.2 Progress Made on MITS Implementation and Tabletop-initiated improvements

The second objective of the audit was to assess the progress made on the implementation of the DRP-related requirements of the TBS Operational Security Standard on Management of Information Technology Security (MITS) and improvements initiated as a result of a DRP tabletop exercise conducted by IMS in 2005.

4.2.1 Implementation of DRP-Related MITS Requirements

We expected to find evidence that CSC has formally implemented the DRP-related requirement of MITS, specifically:

- As part of their business continuity planning, departments must produce and routinely test and revise an IM continuity plan and an IT continuity plan. (MITS 12.8)
- Departments must restore essential capabilities within the time constraints and the availability requirements specified in the departmental Business Continuity Plan (MITS 18.5);
- Backup and recovery procedures exist and are documented (MITS 18.5); and,
- Backup data is created regularly and copies are maintained at an off-site location (MITS 18.5).

CSC has designed and implemented DRP-related requirements of MITS, with the exception of requirements related to DRP revisions and testing.

More specifically, during our testing we made the following observations:

- *DRPs have been produced for NHQ critical applications and for regions, but have not been consistently revised and tested, which increases the risk that the DRPs are missing critical steps in the recovery of critical regional applications.*
- *CSC has not comprehensively tested its capacity to restore all critical applications within the time constraints and the availability requirements specified in BCPs, which increases the risk that critical applications may not be recovered in a timely manner, or be operating at expected processing levels when running at the alternate processing facility.*
- *Backup and recovery procedures exist and are documented. Backup data is created regularly and copies are maintained at an off-site location*

These observations were previously noted in Section 4.1 and related recommendations were included as part of that section.

4.2.2 Implementation of Improvements

We expected to find evidence that CSC has formally implemented improvements initiated as a result of a DRP tabletop exercise conducted by IMS in 2005.

Of the twenty potential improvements identified in the 2005 DRP tabletop exercise, eleven have been implemented (55%), two have been partially implemented (10%), and seven have not yet been implemented (35%). The complete list of improvements and status is included in appendix B.

More specifically, during our testing we made the following observations:

- *DRPs do not specifically document who will be relocated to the alternate processing facility, how quickly they should relocate, where they will lodge and for how long. This increases the risk of further delaying recovery efforts in relocating NHQ staff to the alternate site.*
- *A process for the secure transportation of the backup tapes to the alternate processing facility has not been documented, which increases the risk of unauthorized access, loss or theft of backup tapes.*

These observations were previously noted in Section 4.1 and related recommendations were included as part of that section.

CONCLUSION:

Progress has been made on implementing improvements from MITS and the 2005 DRP tabletop exercise. However, further efforts are required to fully meet MITS requirements related to DRP revisions and testing.

Annex A

Audit Criteria

The audit criteria for the audit were developed from COBIT 4.1 (www.isaca.org) DS4 requirements, and also include specific DRP-related requirements from the TBS Government Security Policy and supporting Management of IT Security Standard (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON-eng.asp).

1. IT Continuity Framework:
Develop a framework for IT continuity to support enterprise wide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organizational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

2. IT Continuity Plans:
Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. They should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach.

3. Critical IT Resources:
Focus attention on items specified as most critical in the IT continuity plan to build in resilience and establish priorities in recovery situations. Avoid the distraction of recovering less-critical items and ensure response and recovery in line with prioritised business needs, while ensuring that costs are kept at an acceptable level and complying with regulatory and contractual requirements. Consider resilience, response and recovery requirements for different tiers, e.g., one to four hours, four to 24 hours, more than 24 hours and critical business operational periods.

4. Maintenance of the IT Continuity Plan:
Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner.

5. Testing of the IT Continuity Plan:
Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

6. IT Continuity Plan Training:
Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests.

7. Distribution of the IT Continuity Plan:
Determine that a defined and managed distribution strategy exists to ensure that plans are properly and securely distributed and available to appropriately authorised interested parties when and where needed. Attention should be paid to making the plans accessible under all disaster scenarios.

8. IT Services Recovery and Resumption:
Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs.

9. Offsite Backup Storage:
Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise’s media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data.

10. Post-resumption Review:

Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly.

Annex B

Action Items from Confident Recovery I

Ref:	Action Item / Lesson Learned / Comment:	Finding:	Status:
Alerte Phase			
i.	Time required for recovery teams to rendezvous for a meeting prior to deployment to recovery site needs to be taken into account	Time required is not indicated in any plans. During conversation with the DR Coordinator December 23, 2008, this cannot be documented. Onus is with recovery groups to meet RTO.	Not implemented
ii.	The contact list (call tree) was problematic. Lesson learned: team members should have all their team contact numbers and a fan out.	In the 2005 meeting, Bruno had the responsibility to call everyone. Changed for 2007 tabletop. Call plan is documented in the BCP.	Implemented
iii.	Lesson learned: provision should be made for senior management to hold meeting to discuss actions prior to a disaster declaration being made.	This was not included in the plan in 2005. The BCP in 2008 has the Emergency Operations Centre at 100 Metcalf street.	Implemented
iv.	Provision for notification process to inform the designated alternate contact that they are the primary when the original primary is on vacation.	In 2005 alternates were not identified. The 2008 BCP and DRP's have primes and alternates documented.	Implemented
Deployment Phase			
i	**Recovery Team**		
i.1	Rendezvous point needs to be clearly identified.	In 2005, the rendezvous point was not documented. The rendezvous point of Carlingwood Shopping Centre is documented in the BCP in 2008.	Implemented
i.2	Staff live all across Ottawa. These staff could be picked up en-route to Laval by bus	There is a single central rendezvous point.	Implemented
i.3	Initial deployment of all staff for 30 days is too long. After recovery, less NHQ staff needed at Laval site.	This is a comment. In 2005 the duration was not implemented. In 2008, the understanding is that people are needed until the site is functional. People are not needed on site for more than 3 days. This is not documented. Most staff are under the understanding	Not Implemented

Ref:	Action Item / Lesson Learned / Comment:	Finding:	Status:
		that they are not needed to be onsite. Their understanding is that they will be working via VPN.	
i.4	Aide-memoire should be created to remind team members what they should bring to recovery site.	This has not been created	Not implemented
i.5	No provision for contract staff to be paid past the 37.5 hours per week.	During December 23 meeting with Terry, noted that as contractor contracts come up for renewal, DRP availability clauses are being inserted into the contracts.	Partially Implemented
i.6	Designated manager responsible for arranging bus services should be made aware of this responsibility.	Mentioned in BCP. During meeting with Terry December 23, 2008, the recovery manager for BCP (Murray) has this responsibility. This was confirmed with Murray during his interview	Implemented
i.7	Other means of transportation should be examined.	During meeting with the DR Coordinator, this is his responsibility of the BCP recovery manager.	Not implemented
Right of Refusal			
ii.1	Recovery Team composition must be reviewed to include members with issues of being deployed to another site with a few hours notice.	The DR Coordinator states that although CSC cannot mandate that personnel must respond to a disaster, most primes understand they will be there. However, during interviews, most indicated they do not think they need to go to Laval	Not Implemented
ii.2	Mechanisms to handle team members who have health or family issues with relocation to recovery site.	Mechanism is the alternate contact. In 2005, alternates were not defined. Every prime and key member has an alternate.	Implemented
Physical Space			
iii.1	Recovery site physical space limited to 15 people. Many more than this are designated to go to recovery site.	Informal understanding that the Staff College in Laval can be used.	Partially Implemented
Backup Tapes			
iv.1	Discrepancy in plans that tapes are actually recovered from King	During interviews and process review, it is understood that tapes	Implemented

Ref:	Action Item / Lesson Learned / Comment:	Finding:	Status:
	Edward, not National Archives.	are stored at National Archives and King Edward (2 copies). Tapes will be recovered from National Archives.	
iv.2	Tape transportation – Treasury Board (TBS) Standard for physical security requires secure transport of tapes. Process must be in place that, in the event of an accident, would identify to police the fact that there is cargo in the vehicle and that the container should be safeguarded and not released to just anybody	Plans do not indicate secure transport.	Not implemented.
Lodging of staff in Laval			
v.1	Documents do not specify where staff would lodge while in Laval.	This is still outstanding. Informal arrangement that Normand Vermette in Laval makes arrangements for Lodging in the Laval area, or at the staff college. Formal agreements are not in place.	Not implemented
Recovery Phase			
i	Given the occasion and setting to sit down as a team, recovery teams relish the opportunity to review and revise their expected plans.	Tabletops occur yearly, and plans updated based on tabletop.	Implemented
ii	Service Desk did not have detailed recovery plan	Service desk has a detailed DRP. We observed Service Desk DR procedures during the tabletop	Implemented
iii	The DRP's do not call for the establishment of a "command centre (CC) or Command post (CP)"	In 2005 they did not have a command post. In 2007 they had 441 MacLean defined as command centre. In 2008 they have 100 Metcalfe.	Implemented

Annex C

Management Action Plan

Recommendation	Action Summary	OPI	Planned Completion Date
Recommendation #1: The Chief Information Officer, Information Management Services should formally assess the adequacy of the level of resources currently assigned to the DRP program.	1.) Business case will be developed jointly between ISO and ITSEC and submitted to CIO for review and approval.	The Chief Information Officer, Information Management Services	1.) June 2009
Recommendation #2: The Chief Information Officer, Information Management Services should finalize a standard template for documenting, testing and distributing DRPs at a regional level within CSC.	1.) Template was created in 2008. 2.) Template will be presented to Regional Administrators IMS for comments and implementation 3.) Plans were created for Regional DRP's FY07/08 Tabletop exercises were conducted in all regions including NHQ in FY 2008/2009 based on the templates.	The Chief Information Officer, Information Management Services	1.) Completed 2.) April 2009 3.) Completed
Recommendation #3: The Chief Information Officer, Information Management Services should ensure that formal Service Level Agreements detailing requirements for the availability of systems be implemented between IMS and its clients across CSC.	1.) SLA template to be developed by ISO. Template will include RPO/RTO from C&A evidence. 2.) ISO to create SLA's for all mission critical applications. 3.) Sign-off on SLAs	The Chief Information Officer, Information Management Services	1.) Completed 2.) April 2010 NOTE: SLAs will not be created for CED2 Engineering group and the Service (these will be outlined within individual SLAs for Desktop Support etc and within the IT Service Catalogue.) 3.) April 2010
Recommendation #4: The Chief Information Officer, Information Management Services should ensure that all current DRPs are appropriately reviewed and formally approved by the same parties that sign the internal Service Levels Agreements within which availability requirements will be specified. All	1.) DRP's will be reviewed by March 31, 2009. 2.) DR Coordinator will design a formal DRP review/approval process with annual updates. 3.) Process will be approved and implemented by CIO.	The Chief Information Officer, Information Management Services	1.) Completed 2.) June 2009 3.) July 2009

Recommendation	Action Summary	OPI	Planned Completion Date
significant changes to DRPs should also be subject to review and formal approval by management/application owners.	4.) Change Process Trigger: Class 1 Change and CAB Process document amended by ISO.		4.) Ongoing
Recommendation #5: The Departmental Security Officer (DSO) should ensure that a formal Business Impact Analysis is completed by the business/applications owners to confirm the identification of critical applications and to further confirm that the identified Recovery Time Objectives remain appropriate and relevant.	Departmental Security will undertake a Business Impact Analysis (BIA) for NHQ in the coming months. Included in this analysis will be a dialogue between Departmental Security, Information Technology Security as well as the business/application owners with a view to determining mission critical applications and their recovery time objectives. The committed involvement of all stakeholders will be crucial to ensure that the BIA is accurate, well-developed and relevant to the mission of CSC.	The Departmental Security Officer	October 2009
Recommendation #6: The Chief Information Officer, Information Management Services should develop a DRP training program specifically aimed at increasing the DRP knowledge of the resources in the alternate processing facility in Laval as a means of expanding the availability of qualified DR resources in the event of a disaster**.**	1.) ISO to develop and implement a cross training plan for DR activities/responsibilities in Laval including implementation dates.	The Chief Information Officer, Information Management Services	1.) June 2009
Recommendation #7: The Chief Information Officer, Information Management Services should expand the current testing program and include annual testing of the processing capacity of the alternate processing facility.	1.) Capacity/failover tests were conducted in DR site in 2008 on IFMMS, and HRMS applications. 2.) Capacity/failover tests will be run annually on mission critical applications.	The Chief Information Officer, Information Management Services	1.) Completed 2.) March 2010
Recommendation #8: The Chief Information Officer, Information Management Services should ensure that all DRP documents are updated at least annually, or following a significant change. As part of the update, the Chief Information Officer should also ensure that the DRPs are formally reviewed and approved by application owners.	1.) DR Coordinator will design a formal DRP review/approval process. Process will be approved and implemented by IMS CIO.	The Chief Information Officer, Information Management Services	1.) June 2009
Recommendation #9: The Chief Information Officer, Information Management Services should implement a process to ensure that lessons learned from DRP testing	1.) Action plan was created to address issues identified in2007/2008 Lesson Learned document. 2.) Process will be developed, approved	The Chief Information Officer, Information Management	1.) completed 2.) April 2010

Recommendation	Action Summary	OPI	Planned Completion Date
is consistently documented and proactively addressed.	and implemented by IMS CIO. Part of the process will include action plan to deal with lesson learned recommendations.	Services	
Recommendation #10: The Chief Information Officer, Information Management Services should ensure that DRPs include a comprehensive distribution plan listing all individuals that should have a copy of the most recent DRP and the method of distribution, and that staff located at the alternate processing facility has readily access to DR documents.	1.) Management/application owners to update DR plans to include distribution list, and maintain list. 2.) Laval staff already has access to all DR Plans.	The Chief Information Officer, Information Management Services	1.) June 2009 2.) Completed
Recommendation #11: The Chief Information Officer, Information Management Services should implement a solution that enables CSC to encrypt backup tapes for application data assessed as sensitive either from a security or from an access to information perspective	1.) ISO to develop and implement encryption solution for backup tapes or propose alternative solution. 2.) Deployment of solution	The Chief Information Officer, Information Management Services	1.) March 2010 2.) June 2010
Recommendation #12: The Chief Information Officer, Information Management Services should ensure that, as part of the DRP, there is either a plan to restore resumptions of activities back to NHQ or a new DRP which would guide DR staff in the event of a disaster at the alternate processing facility (prior to resumption at NHQ).	1.) IT Security will lead the development of the Resumption Plan in close consultation with ISO. 2.) Once accepted the NHQ resumption plan will be reviewed and approved by the CIO.	The Chief Information Officer, Information Management Services	1.) March 2010 2.) May 2010