IT Continuity Planning in Government

Released: April 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: February 2011 Transcript

Self-assessment conducted by the Ministry of Public Safety and Solicitor General

We support the recommendations contained in the report and find, in general, the recommendations are consistent with Business Continuity Core Policy and initiatives currently underway.

We do have some concern that the audit was conducted against a different standard than that used by Government to manage the Business Continuity Program.

The OAG used ISACA criteria for the review. Government uses methodology developed by the Disaster Recovery Institute; therefore the measurements of OAG are inconsistent with phraseologies, methodologies and criteria common to the BC Government Business Continuity Program and resulted in some confusion regarding terminology.

The terms: Disaster Recovery Plan, Business Continuity Plan and IT Continuity Plan were interchanged often without clarity of identity.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 1: Preparation of a business impact analysis and risk assessments annually, as outlined in government policy	Fully or substantially implemented

Actions taken, results and/or actions planned

To improve Ministry compliance, Emergency Management BC (EMBC) has:

- revised the Business Impact Analysis (BIA) template based on industry standards and Internal Audit recommendations;
- authored a corresponding BIA Guide and training materials;
- conducted BIA training with Ministry Business Continuity Advisors and Coordinators;
- communicated Ministry risk assessment requirements in Core Policy and at monthly BCP Advisory Committee Meetings; and
- created a new SharePoint site to make templates and training materials more accessible to Ministry Advisors.

Recommendation 2: Prioritization of the recovery of mission-critical applications at the ministry level and across government	Partially implemented

Actions taken, results and/or actions planned

1. Shared Services BC (SSBC) is engaged with ministries to determine mission critical sensitivities and priorities for servers and applications being migrated to the new data centre.
2. EMBC is reviewing and refreshing the cross government mission critical services list requirements with Ministry BCP Advisors.
3. The combined data will provide a sound technological and functional basis for the accurate planning and implementation of provincial recovery priorities.
4. EMBC will incorporate the captured critical applications information with regular Mission Critical Services list updates and share with SSBC.
5. EMBC and SSBC will host a series of information sessions Ministry Executives, BCP Advisors and Information Technology professionals to reinforce and expand existing knowledge of recovery processes, timelines and options.

IT Continuity Planning in Government

Released: April 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: February 2011 Transcript

Recommendations (cont.)

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 3: Establishment of realistic and achievable recovery timelines for shared systems and program applications	Partially implemented
Actions taken, results and/or actions planned 1. Ministries determine business function Recovery Time Objectives (RTOs) and choose a course of action. If IT RTOs cannot support business requirements, options include developing manual workarounds, investing in high availability Disaster Recovery solutions or seek sign-off from Executive for risk acceptance. 2. On April 1, 2010, SSBC published Service Bulletin #178 to assist ministries in understanding their options and provide processes to obtain enhanced IT. 3. SSBC and EMBC will promote Service Bulletin #178 by hosting a series of informational sessions for Ministry Executives, BCP Advisors and IT professionals designed to reinforce and expand existing knowledge of recovery processes, timelines and options.	
Recommendation 4: Assessment of risk associated with alternate arrangements being in the same geographical area as the primary operations and data centre facility, and feasibility of relocation	Fully or substantially implemented
Actions taken, results and/or actions planned SSBC has entered into an agreement with HP Advanced Solutions to provide two new Data Centres. The first came on line in September 2010 and is located in seismic zone 0. The second will be on line in April 2011 and is located in seismic zone 1. These Data Centres are geographically diverse and are state of the art with regard to security and survivability.	
Recommendation 5: Finalization of business continuity plans for all mission-critical business functions	Fully or substantially implemented
Actions taken, results and/or actions planned 1. All SSBC Mission Critical IT business units have approved Business Continuity Plans in place. 2. Revised Core Policy and Procedures Manual, Business Continuity Chapter 16, (on target for Spring 2011 amendments) specifically states Ministry IT recovery requirements. 3. EMBC has revised the provincial Business Continuity Management Program status reporting tool (the Scorecard) to support key internal audit recommendations, incorporate new performance measures and improve data granularity. This will provide enhanced visibility into Ministry business continuity program deliverables and maturity levels.	

IT Continuity Planning in Government

Released: April 2010
1st Follow-up: April 2011
Discussed by the Public Accounts Committee: February 2011 Transcript

Recommendations (cont.)

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 6: Preparation of disaster recovery plans to support the availability of significant operating environments and network infrastructures within the timelines required by ministry programs	Fully or substantially implemented

Actions taken, results and/or actions planned

1. The significant operating environments will be housed in the new Data Centres and will be covered by the vendor's Disaster Recovery Plans as required by the contract.
2. SSBC Network Services has started work to establish Disaster Recovery Planning for critical Network Infrastructure.

Recommendation 7: Inclusion, in contracts with third-party providers of critical services, of provisions regarding both the preparation and testing of business and IT continuity plans and the assessment of risks where inclusion of these provisions is not feasible	Fully or substantially implemented

Actions taken, results and/or actions planned

1. Revised Core Policy (Chapter 16) will require the inclusion of continuity provisions in formal agreements.
2. New contracts for IT services include requirements for the Service Provider to:
   - implement and annually test and update Business Continuity Plans, Disaster Recovery Plans and Operation Centre Plans;
   - conduct annual Business Impact Analysis and Security Risk Assessment to validate plans; and
   - provide detailed confirmation of compliance to the province.

Recommendation 8: Regular testing of continuity plans and restoration procedures for all mission-critical applications and supporting systems	Partially implemented

Actions taken, results and/or actions planned

1. Revised Core Policy (Chapter 16) will require regular testing of continuity plans and restoration procedures for Mission Critical systems and applications.
2. The new Service Provider contract includes obligations for the regular testing of continuity plans and restorations procedures.

Recommendation 9: Updating of business continuity plans for all mission-critical business functions annually	Fully or substantially implemented

Actions taken, results and/or actions planned

1. Revised Core Policy (Chapter 16) will reinforce minimum requirement for annual continuity plan maintenance.
2. The new Scorecard reflects revised policy, Internal Audit recommendations and industry best practice by asking Ministries to report on Business Continuity Plan review and maintenance.
3. The Scorecard semi-annual reporting deadlines (winter/summer) will help trigger Ministry action on maintenance cycles.