Consolidated Management Action Plan
Corporate Services, Human Resources and Communications Branch (CSHRC), Corporate Emergency Preparedness with Information Technology Services Branch (ITSB)
Audit Survey Report 2003-726 "Audit of IT Infrastructure Component of the Corporate Business Continuity Plans"

Recommendation	Office of Principal Interest (OPI)	Implementation Actions	Action Implementation Dates
1. A complete process for identifying and approving the list of critical services and their associated Business Continuity Plans (BCP) needs to be defined, planned and coordinated	◆ ADM, Corporate Services, Human Resources and Communications Branch is the Office of Primary Interest. ◆ Director General, Health Safety Security Emergencies Administration is accountable for ensuring obligations have been fulfilled. ◆ ADM's/CEOs all Branches. ◆ Other Key Stakeholders, including Public Safety and Emergency Preparedness Canada,	Revisit and update PWGSCs high-level critical services list with all Branches using Business Impact Analysis. Expand to include prioritization (through maximum allowable downtime) and associated IT assets (applications and supporting IT infrastructure). Roll up and review all Branch submissions. Seek DM approval.	**a)** Presentation to Operations Committee 10 November 2004. Background briefing and approval of approach. **b)** Update to Operations Committee detailing next steps 19 January 2005. **c)** Brief Branch BCP Coordinators and roll out of software for Business Impact Analysis 21 February 2005. **d)** Meet separately with each Branch/SOA BCP Coordinator to identify specific needs and approach for Branch. Prepare Branch Management Committees' presentations specific for each Branch. Begin March 2005. Complete June 2005. **e)** Establish Regional BCP Working Group. First teleconference March 2005. Completed 23 March 2005. **f)** Visit each Branch Management Committee to brief on BCP process and process to identify Branch critical services and associated IT assets. Begin March 2005. Complete July 31 2005.

	will be acknowledged and engaged as required.		**g)** Each Branch completes their Business Impact Analyses using Living Disaster Recovery Planning System (LDRPS) software and submits to Corporate Emergency Preparedness Directorate. Begin March 2005. Complete October 31 2005. **h)** Branch roll ups are consolidated into a department-wide critical services list. Interim returns from Branches will be conveyed to ITSB when obtained. Begin upon receipt from Branches. Complete November 30 2005. **i)** Present first iteration of prioritized critical services list to Operations Committee December 2005. Reporting will be done against all "Implementation Actions" to be taken, on a quarterly basis. Milestones will be identified, and reported on when proposed, communicated and agreed upon by key stakeholders.

Recommendation	Office of Principal Interest (OPI)	Implementation Actions	Action Implementation Date(s)
2. Linkages between the list of critical services, business units and the IT Infrastructure components of BPCs required to ensure availability, needs to be established, and a risk management process be included for prioritization of these services.	◆ OPI: ADM CSHRC/ADM ITSB ◆ OSI: ADMs All Branches, DG Strategic and Client Services; DG Standards, Engineering and Project Management ◆ Other Key Stakeholders will be acknowledged and engaged as required.	**a)** *ITSB to implement a Branch BCP Committee with membership from key sectors including the Chief Information Officer's (CIO), the Business Continuity / Recovery Services sector, Application Maintenance Services, IT Security Directorate and regions. The committee's mandate will be to ensure a* ***co-ordinated approach*** *to the continuity of branch critical services and assets which support both PWGSC and OGD clients.*	
		◆ Solicit ITSB Director Generals and Regional Directors to appoint members to participate in ITSB BCP Committee	January 21, 2005
		◆ Develop Terms of Reference for ITSB BCP Committee	Draft version of the TOR for ITSB BCP Committee completed
		◆ Kick-off meeting to be held for the BCP Committee	June 30, 2005
		b) ITSB will appoint key employees to participate in the Department's BCP Governance which provides for representation from all business units and whereby a co-ordinated approach to the continuity of Departmental critical services and assets will be addressed.	

		◆ Establish a meeting with Corporate Emergency Preparedness to identify roles and responsibilities of ITSB within the Departmental governance/committee structure.	July 31, 2005
		◆ Solicit ITSB Director Generals to appoint members to participate in Departmental governance/commitee structure.	September 30, 2005
		◆ Provide training and awareness to participants on their respective roles and responsibilities.	October 31, 2005
		c) Define a framework within ITSB, involving key stakeholders, to review and assess Departmental Business Continuity Plans for IT Infrastructure recovery options which will provide for the continued availability of critical services.	
		◆ Arrange a meeting with ITSB stakeholders to confirm roles and responsibilities with regards to reviewing Departmental BCPs.	September 30, 2005
		◆ Develop the framework and obtain approval from ITSB Senior Management.	September 30, 2005
		◆ Ensure that Corporate Emergency Preparedness are aware of ITSB's framework.	September 30, 2005
		◆ Distribute the framework to all Departmental BCP Coordinators.	October 31, 2005

		d) To further strengthen the link ITSB will update its IT Security Risk Management Framework to be compliant with the new Government Security Policy (GSP) and the Operational Security Standard - Management of Information Technology Security (MITS) to include linkages to business continuity planning. As well, MITS mandates that a Certification and Accreditation (C&A) process be applied which will assist business units in identifying safeguards that will ensure for the continued availability of the IT component of critical services.	In progress and will be completed by July 31, 2005
		◆ Business units are invited to attend training sessions at each project kick-off phase of the C&A process.	
		◆ PWGSC Information Technology Security Officers (ITSO) who are Branch IT security representatives will be briefed at the ITSO Conference.	May 6, 2005
		◆ There is a C&A awareness session offered every Monday afternoon by the IT Security Directorate.	Every Monday
		e) Re-establish the IT Security Advisory Group (ITSAG) whose mandate is to advise the Departmental Security Committee on ITS matters including ITS Certification & Accreditation and	July 2005

		ITS Training and Awareness. This committee has representatives from all Branches. **f)** Upon confirmation of a first iteration of Departmental critical services (Aug. 2005), CSHRC and ITSB will conduct an assessment to determine any key vulnerabilities that might impede the Department's ability to sustain delivery of these services. As well, an investment strategy will be developed and presented to the Department's Operations Committee for prioritization/funding.	 March 2006