

## Management Response and Action Plan

### A - For inclusion in the report

The findings and recommendations of the audit were presented to the Corporate Management Sector (CMS) – Corporate Facilities and Security Branch and the Chief Information Office Sector (CIO). Management has agreed with the findings included in this report and will take actions to address the recommendations by March 2017.

*Include a brief summary of the management actions including key or significant elements of the detailed management action plan where appropriate.*

### B - For follow-up purposes - Detailed actions to address the recommendations in the report

Recommendation	Planned Action on the Recommendation	Responsible Official (position)	Target completion date
<p><b>Recommendation 1:</b></p> <p>In order to enhance the ability to have a prioritized departmental view of business functions/services, CMS should:</p> <p>a) Review and amend the BIA template and guide to better assist branches/sectors in providing additional information and rationale to support the criticality assessments and improve consistency across the department; and</p> <p>b) Provide a more rigorous challenge function to ensure consistency and alignment of</p>	<ul style="list-style-type: none"> <li>• CMS will review and amend the Business Impact Analysis (BIA) Template to ensure users provide the additional information and rationale to support the criticality assessment.</li> <li>• CMS will review and update BIA Guide to align with changes made to the BIA Template.</li> <li>• CMS will present to the BCP working group (BCPWG) the findings identified in the audit report to address during the BIA update this fall.</li> <li>• Sectors and Branches will ensure that information provided in BIAs aligns with</li> </ul>	<p>Director of Security CMS</p> <p>Director of Security CMS</p> <p>Director of Security CMS</p> <p>Sectors and Branches</p>	<p>Completed</p> <p>Completed</p> <p>Completed</p> <p>Completed</p>

Recommendation	Planned Action on the Recommendation	Responsible Official (position)	Target completion date
the branches/sectors' BIAs with current guidance.	<p>guidance.</p> <ul style="list-style-type: none"> <li>• CMS will review BIAs to ensure that Sectors and Branches follow guidance provided in the BIA Guide.</li> </ul>	Director of Security CMS	Completed
<p><b>Recommendation 2:</b> Sectors/branches should ensure that stakeholders responsible for the provision of services defined in BIAs, including CIO, have been consulted for validation.</p>	<ul style="list-style-type: none"> <li>• CMS will modify the BIA process to include a step of submitting draft BIAs to Departmental BCP Coordinator for review and validation, followed by a review and challenge by Facilities Management (FM) representative(s) and CIO representative(s) prior to submitting to Sector/Branch head and ADM for approval.</li> </ul>	Director of Security CMS	Completed

Recommendation	Planned Action on the Recommendation	Responsible Official (position)	Target completion date
<p><b>Recommendation 3:</b></p> <p>Sectors/branches, in collaboration with CMS, should ensure that BCPs address all of the OSS-BCP requirements. As well, it should ensure that recovery plans, resource requirements, measures and procedures respond to a range of disruptions of varied severity.</p>	<ul style="list-style-type: none"> <li>• CMS will modify BCP Template to include all OSS-BCP requirements. Training will be provided to BCPWG members to ensure that changes are captured in all Sector/Branch BCPs.</li> <li>• Under the direction of CMS, Sectors and Branches are to ensure changes are captured in their BCPs.</li> <li>• CIO is finalizing an “IT Service Continuity Management Program Framework” and an “Implementation Plan” that align with the OSS-BCP.</li> <li>• Subsequently, the CIO will implement the program.</li> <li>• CMS will discuss protocols with Public Safety for an NCR disruption and the CIO for disruptions to IT systems, and will develop procedures and measures if needed, including updating the BCP Template to reflect the additional information.</li> <li>• CMS will inform BCPWG Members of changes made to template and requirements.</li> </ul>	<p>Director of Security CMS</p> <p>Sectors and Branches</p> <p>CIO</p> <p>CIO</p> <p>Director of Security CMS</p> <p>Director of Security CMS</p>	<p>Completed</p> <p>March/April 2015</p> <p>May 2015</p> <p>March 2017</p> <p>Completed</p> <p>Completed</p>

Recommendation	Planned Action on the Recommendation	Responsible Official (position)	Target completion date
<p><b>Recommendation 4:</b></p> <p>Sector/branch management, with the assistance of CMS, should assess whether additional training is needed for employees with BCP responsibilities. If the assessment reveals that there is a common training need across sectors/branches, CMS should coordinate the provision of the training.</p>	<ul style="list-style-type: none"> <li>• Sector/branch management, with the assistance of CMS, will assess whether additional training is required for employees with BCP responsibilities and will continue the provision of such training if required.</li> <li>• CMS will formalize training requirements for BCPWG members by including requirement for training in the terms of reference of the working group.</li> <li>• CMS will provide BCPWG members with information for Incident Command System group training.</li> </ul>	<p>Sectors, Branches and Director of Security CMS</p> <p>Director of Security</p> <p>Director of Security</p>	<p>May 2015</p> <p>May 2015</p> <p>May 2015</p>
<p><b>Recommendation 5:</b></p> <p>CMS should develop and document a testing approach which outlines an appropriate frequency and complexity of testing, along with testing of key dependencies.</p>	<ul style="list-style-type: none"> <li>• CMS will formally document, in the BCP template, the testing approach that varies in complexity along with the testing of dependencies for Sectors/Branches responsible for critical operations.</li> <li>• Furthermore, CMS will develop an annual testing schedule aligned with the documented approach.</li> </ul>	<p>Director of Security CMS</p>	<p>Completed</p>

Recommendation	Planned Action on the Recommendation	Responsible Official (position)	Target completion date
<p><b>Recommendation 6:</b></p> <p>Sectors/branches should:</p> <p>a) Share lessons learned with all BCPWG members via the departmental BCP coordinator ; and</p> <p>b) Ensure action items following from lessons learned are addressed in order for BCP processes and practices to be improved.</p>	<ul style="list-style-type: none"> <li>• CMS will develop templates for Sectors and Branches to use to identify and report on lessons learned from tabletop exercises and real events.</li> <li>• Sectors and Branches will be responsible for reporting on lessons learned to BCPWG members when applicable.</li> <li>• CMS will develop an action plan template for implementing lessons learned.</li> <li>• Sectors and Branches will be responsible for implementing lessons learned into BCPs.</li> </ul>	<p>Director of Security CMS</p> <p>Sectors and Branches</p> <p>Director of Security CMS</p> <p>Sectors and Branches</p>	<p>Completed</p> <p>Implemented</p> <p>Completed</p> <p>Implemented</p>