

Provincial Update on the Auditor General Recommendations  
Chief Information Office  
November 2011

The Chief Information Office understands the critical importance of security and risk mitigation and how it impacts responsible and effective management of government's information and technology assets. While our current IT Security program has enabled us to achieve good results, we recognize security is an ongoing matter that must be planned for, continually monitored, and managed to keep ahead of new and emerging threats. The Chief Information Office would like to thank the staff of the Auditor General for their courtesy and professionalism while conducting these audits, and will continue to make the recommendations resulting from the audits a priority.

**Recommendations assigned to the Chief Information Office:**

	Complete	Work In Progress	Action no Longer Required	Do not Intend to Implement	Total Recommendations
<b>Chief Information Office</b>					
<b>April 2009</b>					
Chapter 3: Government-wide: Information Technology Security	12	8	-	1	21
<b>November 2010</b>					
Chapter 4: Registry Systems	1	2	-	-	3
<b>May 2011</b>					
Chapter 8: Registry of Motor Vehicles Information and Technology	1	-	-	-	1
<b>Total</b>	<b>14</b>	<b>10</b>	<b>-</b>	<b>1</b>	<b>25</b>
Percentage	56%	40%	0%	4%	100%

**Recommendations in Detail:**

Month & Year	Chapter	Recommendation	Status	Brief summary of actions taken
April 2009	3	3.1	Complete	The Chief Information Office (CIO) was created in April 2009. The structure is complete, the management team is in place and all staff transitioned to their new positions.
April 2009	3	3.2	Complete	The Infrastructure Service Management (ISM) division of the Office of the Chief Information Officer (OCIO) has connected all departments to the government identity management system.

Provincial Update on the Auditor General Recommendations  
 Chief Information Office  
 November 2011

**Recommendations in Detail:**

Month & Year	Chapter	Recommendation	Status	Brief summary of actions taken
				The Wide Area Network (WAN) Security Policy standards were updated to include a requirement that all new applications must use the government identity management system for identification and authentication of internal users.
April 2009	3	3.3	Complete	An IT governance review was undertaken and a new governance model was created. Governance committees became functional in January 2011.
April 2009	3	3.4	Do not intend to implement	The Security Authority was transferred to the Chief Information Office and reports to the Executive Director, Corporate Information Strategies, who in turn reports to the Chief Information Officer. The IT Service Delivery components report to the Executive Director of Infrastructure Service Management, also reporting to the CIO. The CIO appreciates the need for separation of duties between Security and IT Operations. The risks will be balanced and managed through the governance model and through a dispute resolution process.
April 2009	3	3.5	Work in Progress	The resources required to effectively perform security monitoring and audit functions were reviewed in conjunction with the creation of the Infrastructure Service Management division of the Chief Information Office. Resources will be allocated to ensure a proper balance between operations and security functions.
April 2009	3	3.6	Complete	An IT governance review was undertaken and a new governance model has been proposed and accepted. Security oversight has been included in the Technology and Information governance framework. While all 3 of the Governance Committees have a roll in Security oversight, the

Provincial Update on the Auditor General Recommendations  
Chief Information Office  
November 2011

**Recommendations in Detail:**

Month & Year	Chapter	Recommendation	Status	Brief summary of actions taken
				Technology and Information Risk Committee is the lead committee.
April 2009	3	3.7	Work in Progress	A draft security charter was developed by the Security Authority (March 2011).
April 2009	3	3.8	Complete	The Security Authority and ISM collaborate to produce a security plan for each fiscal year (beginning in fiscal 2010-2011) which contains technical and governance activities to be implemented cooperatively between ISM and the Security Authority
April 2009	3	3.9	Complete	The Public Sector Classification Guidelines have been circulated and their use re-communicated to departments. Implementation of data classification standards must be done at the Program level (departmental responsibility).
April 2009	3	3.10	Complete	The Policy has been published in Management Manual 300.
April 2009	3	3.11	Complete	The Security Authority has adopted the Threat Risk Assessment Process developed by the Information Security Forum. The ISF process is regularly updated to remain current with new and existing threats.
April 2009	3	3.12	Complete	A Threat Risk Assessment (TRA) was conducted on the Wide Area Network in 2010-2011 by the Security Authority. The OCIO does not perform TRAs on Corporate Service Unit (CSU) operated applications, and any TRA would be the responsibility of the CSU.
April 2009	3	3.13	Work in Progress	Met with the PSC to discuss the need for updated guidelines and a potential policy.

Provincial Update on the Auditor General Recommendations  
Chief Information Office  
November 2011

**Recommendations in Detail:**

Month & Year	Chapter	Recommendation	Status	Brief summary of actions taken
April 2009	3	3.14	Work in Progress	The strategy is to address management training first. A security training course for management has been developed with the PSC and is delivered 4 times per year. The second phase of the strategy is to conduct employee training.
April 2009	3	3.15	Work in Progress	The pieces required to enact the certification section, are governance (now in place), Change Advisory Board (now in place), security (in place), documented architecture standards (currently being developed), and the architecture review board (role of the Standards Committee supported by CIO staff).
April 2009	3	3.16	Work in Progress	An external firm was contracted to conduct an independent security vulnerability assessment of the wide area network. Learnings from this process will be used to establish policy amendment details.
April 2009	3	3.17	Work in Progress	Policy options developed  Consulted with legal counsel and Public Service Commission.
April 2009	3	3.18	Complete	The WAN Security Policy Standards have been updated to include all mobile computing devices. The updated standards have been communicated to IT and security staff.
April 2009	3	3.19	Work in Progress	TCA funding (\$250k) and an FTE was approved in 2011-2012 for Intrusion/Detection hardware and software.
April 2009	3	3.20	Complete	The CERT process is now embedded with the functionality of ISM.
April	3	3.21	Complete	A secure and managed wireless service offering

Provincial Update on the Auditor General Recommendations  
 Chief Information Office  
 November 2011

**Recommendations in Detail:**

Month & Year	Chapter	Recommendation	Status	Brief summary of actions taken
2009				has been created and implemented in select government office to replace un-authorized and unmanaged devices. Connectivity to the devices is managed by username and password authentication through government's identity management solution
November 2010	4	4.10	Work in Progress	The Chief Information Office has worked in cooperation with the Provincial IT Security Authority to document and approve the standards based on industry best practices. Supporting processes and procedures have been established and will be implemented.
November 2010	4	4.12	Complete	The Chief Information Office has developed and implemented a process for assigning unique temporary passwords under the current support model.
November 2010	4	4.24	Work in Progress	An interim DRP (Disaster Recovery Plan) for all CIO services has been developed and implemented as part of the ISM transition. An interim DRP process has been implemented. New DRP/BCM positions have been approved and funded.
May 2011	8	8.13	Complete	A process for Oracle patching activities is documented and will be repeated as new patches are released.