## Information Security Management: An Audit of How Well Government is Identifying and Assessing Its Risks (*Summary Report*)

Released: December 2010
1st Follow-up: March 2012
Discussed by the Public Accounts Committee: February 9, 2011

**Self-assessment conducted by the Office of the Chief Information Officer**

The Ministry of Citizens' Services supports and appreciates the ongoing efforts of the Auditor General of BC in auditing the Security HealthCheck process and ministry responses. The Government of British Columbia places a high priority on the protection of information. The progress in implementing the recommendations will contribute to our ongoing efforts to protect information and technology resources.

The Government Chief Information Officer is pleased to report that many of the recommendations listed in the report have been addressed, or a plan is in place to address them.

### Recommendations

| RECOMMENDATION AND SUMMARY OF PROGRESS | SELF-ASSESSED STATUS |
|---|---|
| **Recommendation 1:** Develop more detailed guidance for ministries to follow in gathering appropriate support at each scoring level in their annual security review self-assessments. | **Fully or substantially implemented** |

**Actions taken, results and/or actions planned**

Work has been conducted by the Office of the Chief Information Officer (OCIO) to develop an Information Security Annual Compliance Review WIKI to provide ministry's with guidance on how to answer the ISO27001 control statements posed in their annual compliance review scorecard. The Wiki also provides an effective avenue to obtain feedback from ministries.

The OCIO Information Security Branch has created a web page for Compliance, which: hosts information pertaining to the Annual Government's Information Security Compliance Assessment; provides access to the iSMART application; provides elearning for the iSMART tool; and provides documentation on what is required in completing an assessment.

The OCIO Information Security Branch also provided a workshop on January 19th, 2012 attended by Ministry Inforamation Security officers and security analysts, to review the process and requirements for completing the annual information security compliance assessment.

| RECOMMENDATION AND SUMMARY OF PROGRESS | SELF-ASSESSED STATUS |
|---|---|
| **Recommendation 2:** Establish an audit process to ensure ministry assessment levels are reasonable and supported with Fully or substantially implemented sufficient and appropriate documentation. | **Fully or substantially implemented** |

**Actions taken, results and/or actions planned**

Work has been conducted by the Office of the Chief Information Officer to develop an audit program to review ministry compliance results. Within the program the audit plan has been created, with two audits completed, and one audit set to be launched.

## Recommendations (Cont.)

**Recommendation 3:** Develop a process that will identify causes of fluctuations in ministry compliance results, and develop specific action plans to deal with those causes.

**Fully or substantially implemented**

**Actions taken, results and/or actions planned**

Work has been conducted by the Office of the Chief Information Officer to work with ministries in achieving a better understanding of the causes of fluctuations in their compliance results. The identification of causes in fluctuation of results will be brought forward through the audit program, ministries review of issues and subsequent action plans and through the compliance results generated from the assessments.

**Recommendation 4:** Require all ministries to complete a ministry-wide Security HealthCheck assessment regardless of whether a particular application is selected for a more detailed assessment.

**Fully or substantially implemented**

**Actions taken, results and/or actions planned**

Direction has been provided by the Office of the Chief Information Officer to ministries requiring them to provide a ministry wide assessment.

**Recommendation 5:** Work with ministries to develop compliance performance targets suited for each ministry.

**Partially implemented**

**Actions taken, results and/or actions planned**

Work is proceeding by the Office of the Chief Information Officer to work with ministries to define ministry specific compliance performance targets. A framework for this initiative has been completed.

Work has been conducted to obtain an independant analysis of the minisitres 2010/11 annual information security compliance assessments, as well as individual meetings conducted with each Ministry Information Security officer to obtain their feedback on the value of the annual reviews. Ongoing work with the Ministry Chief Information Officers will assist in determining the value of continuing with these annual reviews and setting targets or determining an appropriate alternate solution.

**Recommendation 6:** Ensure that all ministries use the same assessment tool for their information security self-assessments.

**Fully or substantially implemented**

**Actions taken, results and/or actions planned**

A standard has been implemented by the Office of the Chief Information Officer that defines the Information Security Management and Risk Tool (iSMART) as the standard risk and compliance assessment tool for government.