Whole-of-Victorian Government Information Security Management Framework

Victorian Auditor-General's Report

Tabled 27 November 2013

Audit context and background

- Information communication technology (ICT) is now fundamental to nearly all service delivery and internal management by the public sector and government
  - Not a 'back room' activity – ICT is being used by citizens and public officials 24/7
- ICT systems have inherent and significant security risks:
  - Breaches can occur due to software, hardware and/or people
- The cyber threat is real, escalating and without borders:

According to the Cyber Security Operations Centre (CSOC) Cyber Intrusion Activity Report – Australian State and Territory Governments: January–June 2013:

> 'Between January and June 2013, there were approximately 40 cyber security incidents affecting state and territory governments. (...) The networks of the Victorian and West Australian state governments accounted for the highest proportion of cyber security incidents responded to by the CSOC between January and June 2013.'

- Previous audits that are relevant to this topic:
  - *Preparedness to Respond to Terrorism Incidents: Essential Services and Critical Infrastructure (January 2009)*
  - *Maintaining the Integrity and Confidentiality of Personal Information (November 2009)*

Audit objectives

To assess the effectiveness of ICT security policy, standards and protection mechanisms.

The audit examined whether:

- appropriate information security policy direction and guidance provided consistent protection to public sector ICT systems and data
- central agencies have oversight of, and coordinate responses to, Whole-of-Victorian government (WoVG) information and system threats
- selected agencies have established and complied with information security policy, standards and processes.

Audit scope – audited agencies

- Departments (all are inner WoVG)
  - Department of Premier and Cabinet (DPC)
  - Department of State Development, Business and Innovation (DSDBI)
  - Department of Treasury and Finance (DTF)
  - Department of Justice
  - Department of Human Services
- Shared services provider of ICT infrastructure to most departments
  - CenITex – (inner WoVG)
- Public financial corporations
  - State Revenue Office (inner WoVG)
  - Treasury Corporation of Victoria (outer WoVG)
  - Victorian Funds Management Corporation (outer WoVG)
  - WorkSafe Victoria (outer WoVG)
  - Transport Accident Commission (outer WoVG)

Findings – information security management framework

page
ix

- DTF has developed information security policy and standards following recommendations made by our previous audit.
- Inner WoVG agencies must develop an information security management framework (ISMF) and report annually on the status of information security.
- DSDBI is required to oversee the implementation of agencies' ISMF, but there is little evidence of this oversight.
- No specific information security guidance for outer WoVG agencies, despite recommendations previously accepted by DTF and DPC.
- The four outer WoVG agencies we reviewed are less advanced with their information security policies and frameworks—only one had considered the guidance developed by government.

Findings – no coordinated view of cyber threats

- No central view of the overall Victorian cyber threat situation.
- No arrangements in place to brief government in the event of a multi-agency or sustained cyber attack.
- Emergency Management Bill 2013, introduced into Parliament on 31 October 2013, may address these issues:
  - formalises establishment of the State Crisis and Resilience Council (SCRC), chaired by the Secretary of DPC and comprised of departmental secretaries.
  - DSDBI to brief SCRC on cyber threats
  - SCRC to recommend briefings for ministers as appropriate.
- Overall, there is an unsatisfactory awareness of how ICT systems would perform while under cyber attack.
- Closer central agency involvement will be critical in managing this knowledge gap.

Findings – top four strategies for cyber intrusions

- Agencies are required to implement the Australian Signals Directorate's *Top 4 Strategies to Mitigate Targeted Cyber Intrusions.*
  - poorly implemented within inner and outer WoVG agencies.

- All agencies had undertaken penetration testing, however:
  - little evidence that the agencies tested ICT systems across the whole enterprise
  - multiple instances of testing being too narrowly scoped
  - inadequate maintenance of software patches
  - continued operation of unsupported and vulnerable systems.

Actions in management letters agreed with agencies

	Recommended actions					
Agency[a]	**Critical level risk[b]**	**Medium level risk[c]**	**Total**	**Agreed with agency**	**Critical level completed by agency**	**Medium level completed by agency**
Agency 1	–	11	**11**	11	–	2
Agency 2	3	12	**15**	15	3	4
Agency 3	–	14	**14**	14	–	6
Agency 4	3	9	**12**	12	3	3
Agency 5	6	35	**41**	35	2	2
Agency 6	–	18	**18**	12	–	–
Total	**12**	**99**	**111**	**99**	**8**	**17**

(a) A critical level risk is a high information security risk which requires an urgent assessment of the risk and implementation of mitigating controls.

(b) A medium level risk is a moderate or long term information security risk which should be assessed and mitigating controls implemented as soon as possible.

Source: Victorian Auditor-General's Office.

Recommendations

The Department of State Development, Business and Innovation should:	Accept
1. send information security management policy to government for formal consideration	✓
2. amend information security policy and standards to include those outer WoVG agencies operating ICT systems that are critical to state revenue, public safety, or are holding sensitive personal data	✓
3. require WoVG agencies to report any variations between the information security standards and their agency ISMFs, that have been approved by their agency head, as part of the annual ISMF self-assessment reporting process	✓
4. require that each agency ISMF self-assessment report includes a statement of compliance addressing all self-assessment report deficiencies	✓
5. develop processes for outer WoVG agencies to be included in relevant briefings and information security forums, and to be provided with advice and assistance outside of the WoVG Chief Information Officers Council	✓
6. improve the current ISMF self-assessment report template to ensure a more comprehensive outcome.	✓

Recommendations – *continued*

Departments and agencies included in this audit should:		Accept
7.	take a more rigorous approach to completing their annual information security management framework self-assessment report	✓
8.	make sure their annual self-assessment reports reflect the true status and risk to agency business from any third party service provider they may use.	✓
DPC and DSDBI should:		
9.	confirm their respective roles and responsibilities for information security once the Emergency Management Bill 2013 is enacted	✓
10.	confirm that briefings on cyber threats will be made to the SCRC by DSDBI as the agency with primary responsibility for WoVG ICT, and that the SCRC will in turn recommend briefings for ministers as appropriate	✓

Recommendations – *continued*

DSDBI should:		Accept
11.	arrange for a cyber alert subscription service to be available to every government agency from a suitable provider	✓
12.	develop and implement a process for maintaining a register of all IP addresses in use by public sector departments and agencies.	✓
Departments and agencies included in this audit should:		**Accept**
13.	implement appropriate action to maintain the accuracy of their IP address information with the Asia-Pacific National Internet Centre.	✓

VAGO

Victorian Auditor-General's Office

Recommendations – *continued*

	All public sector agencies in Victoria should:	Accept
14.	review the Australian Signals Directorate *Top 4 Strategies to Mitigate Targeted Cyber Intrusions*, and implement these practices as a matter of urgency	✓
15.	retain responsibility for managing and allocating passwords if third party service providers are used	✓
16.	review the patching guidelines published on the Australian Signals Directorate's website and develop, implement or review their patching strategy.	✓

Contact details

For further information on this presentation please contact:

Victorian Auditor-General’s Office
[p] 8601 7000
[w] www.audit.vic.gov.au/about_us/contact_us.aspx