Information Management Advice 35: Part 2
A Step by Step Approach to Developing an Information Security Plan

Agencies need to develop and document an Information Security Plan and use it to generate annual tactical plans that, when executed, move the overall maturity of the security program forward. Agencies need to develop a process to review and refine the plan annually via their information security governance structure. This advice provides a step by step approach to developing an IS Plan which was introduced in Step 8 of Part 1 of this advice.

The level of detail contained in the agency's information security plan should be commensurate with the complexity of the agency's information environment, its business functions and the information security risks that it faces. The suggested approach for the development of the plan is to:

- develop an overarching information security plan, which outlines the security program for the agency as a whole
- support this information security plan with a number of detailed plans for each separate entity/agency portfolio and/or significant or high risk agency information systems and processes.

Regardless of the development or format of the plan, information security planning should be integrated into the agency's culture through its strategic and agency plans and operational practices. Security considerations should be incorporated into the agency corporate planning process and ICT strategic resource planning, to ensure that the agency information security plan meets the business and operational needs of the agency and its clients.

An information security plan should include, at a minimum, an assessment of the current state of the program, a defined target state that is achievable within a 3 year planning window, and a gap analysis and plan for closing the gaps. (See advice 35 Part 1 Attachment 1 for a Template for a Gap Analysis).

Suggested Steps for Developing an Information Security Plan

There are a number of steps which should be used to develop the agency information security plan.

Step 1: Identify Agency Goals and Objectives for Information Security

Identify linkages between the agency information security policy and all agency corporate plans, strategies, goals and objectives to establish the key areas which may impact on the current or future information security environment of the agency.

Step 2: Identify Major Information Assets and Business Critical ICT Assets

This information may be sourced from the agency's disaster recovery plan. See TAHO *Advice 39 Developing an Information Asset Register* and related Template.

Step 3: Conduct a Risk Assessment

Conduct a risk assessment on the major information assets with the assigned owners of these assets, on an annual basis or after any significant change has occurred (e.g. machinery-of-Government changes).

The process or methodology used by the agency to assess security risks should be based on the agency's preferred risk management processes. In the absence of an agency risk methodology, agencies are encouraged to use *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*. Agencies can access a copy of this Standard from Office of e-Government website.

Step 4: Current Situation

Gather information regarding existing agency security policies, procedures and controls and map these against the:

- data obtained from the risk assessment process
- mandatory requirements of the Tasmanian Government Information Security Policy Manual and any other security standards that the agency uses
- agency's security architecture targets.

Step 5: Analysis of any Gaps and the Effectiveness of Existing Controls

Conduct an assessment of the effectiveness of the existing controls, and an analysis of any gaps, against the information obtained from step 4 above. See Attachment 1 for a Gap Analysis Template.

Step 6: Develop Recommendations and Strategies

Develop and document recommended controls, a prioritised plan of actions/strategies which need to be implemented or maintained to achieve the desired level of agency security, how this is to be achieved and who is responsible. Information security plans should provide for treatments that are both cost-effective and appropriate to the level of risk. Where agencies identify a high level of risk in their information environment (based on the information security classification of information assets in its care) it is suggested that it consult with specialist information security agencies or industry professional bodies for advice or technical assistance in developing their strategies and plans.

Step 7: Identify Outstanding/Residual Risks that will not be Treated

Document any ongoing risks that will remain untreated or are assessed as acceptable risks.

Step 8: Obtain Agreement on risks and Strategies

To ensure that the information security plan meets the requirements of the business, it is important to gain agreement from the information asset owners. This will ensure that the strategies and plan adequately reflects the protection of the assets from a business perspective and will also inform the prioritisation process for treatment.

Step 9: Develop Actions and Timetable

Document and develop a detailed plan of activities and actions along with timeframes for implementing the controls and strategies agreed on.

Step 10: Determine Resourcing

Document and detail the resourcing requirements for the implementation of the controls and strategies including the personnel, materials and budget for its implementation.

Step 11: Endorsement and Publishing of the Information Security Plan

Gain endorsement of the information security plan from the appropriate governance body and senior executive on an annual basis.

Step 12: Implementation of the Information Security Plan

To facilitate a systematic and co-ordinated approach to security and risk management, agencies should establish a structure or framework to help develop and implement the agency information security plan. The Tasmanian Government Project Management Guidelines include templates for project plans available from http://www.egovernment.tas.gov.au/project_management

Step 13: Ongoing Monitoring and Review

To ensure that security controls in the agency continue to remain relevant to the agency goals, objectives and operational and business environments, the agency's information security plan should be reviewed, monitored and reported on, on an ongoing basis. The information gained from these activities is used to inform future agency security plans and strategies.

It is suggested that agencies review their security plan at least annually to identify changes to the risk profile and to assess the effectiveness of existing controls. Further to this, the agency should ensure that security planning becomes an integral component of all agency management, projects and activities rather than an isolated and once a year planning activity.

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email gisu@education.tas.gov.au

Acknowledgements

- Information Standard 18: Information Security – Implementation Guideline, Queensland Government ICT Policy and Coordination Office, Department of Public Works
- Information Security Guideline NSW Government
- AS/NZS ISO/IEC 27001:2006 Information technology – Security Techniques – Information security management systems – Requirements
- ISO/IEC27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary
- Peltier, Thomas, R. "Information Security Fundamentals." 2002. URL: http://www.cse.hcmut.edu.vn/~ttqnguyet/download%20ebook%20here!!!/ISSReferences/IS06_Information_Security_Fundamentals.pdf (Accessed October 2013)

Information security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
1.0	November 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
		This is the first release of this document.

Issued: November 2013

Ross Latham
State Archivist