Information Management Advice 35: Part 3 Information Security Governance

Information governance is the system by which the current and future use of information and its management is directed and controlled through a system of policies, procedures, standards and guidelines. Information security governance is specifically those activities related to the governance, authorisation and auditing of information security arrangements within an agency. Roles and responsibilities relating to information security within the agency should also be defined. The Tasmanian Government Information Security Policy states that the head of each agency MUST convene an Information Security Committee composed of senior management, or assign the role to an existing senior management committee. This Committee is responsible for ensuring the Policy is applied. This advice expands on the introduction provided in Step 2 Part 1 of this advice.

Management Commitment

A key factor for successful information security in any agency is the:

visible support and commitment from all levels of management

This will not guarantee success but **lack** of it will guarantee failure.

Executive management direction on, and commitment to, information security can influence the culture of the agency. Executive management interest helps ensure that information security is taken seriously at lower agency levels.

Management's commitment to information security can be demonstrated by ensuring that:

- Effective and functioning governance arrangements originate at the highest level of the agency.
- The IS management plan establishes detailed agency, management responsibilities and accountabilities and has executive level endorsement.
- An IS Framework is established, implemented and maintained.
- Adequate resources are allocated to information security.
- The performance of the IS Project is reported to executive management for review and as a basis for improvement, taking into account any regulatory reporting requirements.

Management commitment can be developed and sustained by providing regular reports and status information.

Below is an overview of the roles and responsibilities of a governance body for the implementation of an Information Security Project. Information Security is an aspect of Information management, which is generally implemented with its own governance arrangements. This advice does not therefore, specifically cover information management related governance.

Information Security Governance Body Membership

Membership of the information security governance body should reflect the size, geography and complexity of the agency. Membership should include:

- Agency Information Security Officer/Manager
- representative/s from information security administration
- representatives from across the agency with relevant roles and responsibilities (e.g. protective security, business areas, ICT, auditors, legal, human resources, risk management, business planning, information management)

Chair

It is the responsibility of the Chair of the information security governance body to:

- lead and direct the activities of the information security governance body
- ensure that the information security governance body operates effectively including setting meeting agendas and conducting meetings and business
- ensure adequate induction of new members
- determine performance standards and a program of work for the information security governance body
- fulfil the reporting requirements of the information security governance body (see suggestions below).

Role

The role of the information security governance body is to:

- direct the preparation and implementation of information security policies and processes
- evaluate and direct information security plans and initiatives
- review and monitor conformance to obligations and performance
- develop and promote information security capability within the agency.

Responsibilities

The information security governance body fulfils this role by meeting the management and coordination responsibilities detailed in this section.

Direct the Preparation and Implementation of Information Security Policies and Processes

It is a role of the information security body to direct the preparation and implementation of the information security policies and processes. In order to fulfil this role, the following management responsibilities should be met:

- direct the preparation of, review and approve the agency information security policy.

- ensure that the information security policy meets both compliance obligations and agency requirements and is integrated into processes.

In addition to these management responsibilities, the following coordination responsibilities should be met:

- ensure that the implementation of information security controls is coordinated across the agency
- identify how to manage non-compliance with information security policy
- review and approve methodologies and processes for information security
- develop processes that ensure that internal and/or external audit are consulted when implementing new or significant changes to financial or critical business information systems
- assign responsibility for and oversee the management of information security registers (including register of information security classified information and systems, and a disaster recovery register)

Ensure that policies and processes are in place to:

- determine business need for external party access arrangements to the agency's information and ICT environment
- identify risks related to external party access to the agency's information and ICT environment
- establish and define controls in agreement with external parties and ensure that they are documented in contract and service agreements

Evaluate and Direct Information Security Plans and Initiatives

It is a role of the information security governance body to evaluate and provide direction for information security initiatives. In order to fulfil this role, the following management responsibilities should be met:

- direct the preparation of, review and approve the agency's information security plan ensuring that the plan identifies the agency's information security goals and meets agency requirements
- direct the preparation of, review and approve the agency's disaster recovery plans that integrate with the agency's business continuity plan
- provide input into agency general security plans and business continuity plans
- direct the preparation of, review and approve the agency's overarching disaster recovery plan
- direct the preparation of, review and approve the agency's information security awareness plan
- provide clear direction and project board support for significant information security initiatives

Review and Monitor Conformance to Obligations and Performance

It is a role of the information security body to review and monitor conformance to information security obligations and performance.

In order to fulfil this role, the following management responsibilities should be met:

- review the effectiveness of the implementation of the information security policy, this could be achieved by reviewing:

    - the completed Information Security Compliance Checklist (see TAHO website).
    - information security incidents and escalating where appropriate to the senior executive management group or other in accordance with local procedures
    - information security incident reports
    - the results of exceptions from technical checks, and approve/endorse recommendations for corrective action
    - the results of business continuity and disaster recovery tests, and approve recommendations on corrective actions
- monitor external party arrangements for compliance, this includes:
    - confirming that related risks have been identified, and appropriate controls agreed and documented
    - ensuring that arrangements are being executed in compliance with documented agreements

In addition to these management responsibilities, the following coordination responsibilities should be met:

- assign responsibility for completing the agency's annual self-assessment against the Information Security Checklist for your Agency's current IS Practices
- ensure that networks and systems are subjected to regular technical checks for compliance with the information security policy
- identify significant threat changes, and exposure of information and information processing facilities to threats
- assess the adequacy and coordinate the implementation of information security controls
- monitoring, reviewing and evaluation of information received from information security incidents, and endorsing appropriate corrective actions in response to information security incidents or shortcomings
- in the case of deliberate violations and breaches, assist with formal disciplinary processes where required.

Develop Information Security Capability

It is a role of the information security governance body to develop information security capability. In order to fulfil this role, the following management responsibilities should be met:

- provide the resources needed for information security
- assign specific roles and responsibilities for information security across the agency

In addition to these management responsibilities, the following co-ordination responsibilities should be met:

- effectively promote information security education, training and awareness throughout the agency. This should be conducted in accordance with the information security awareness plan

Authority

The information security governance body must have the requisite authority to fulfil its role and responsibilities as identified in its terms of reference, See attachment 1. This should be coupled with clear reporting lines to the agency senior executive management group.

Suggested Reporting Requirements

The following are suggested reporting requirements, organised by role. It includes the intended audience for the report and the frequency of reporting or due date.

Role	Reporting requirement	Audience	Frequency/Date
Provide leadership in, and direct the preparation and implementation of the information security policies and processes	Submit information security policy for approval.	Senior executive management group	Ad hoc
Evaluate and direct information security initiatives	Submit information security plans for approval.	Senior executive management group	Annually
	Submit overarching information and ICT asset disaster recovery plan/s for approval.	Senior executive management group	Annually
	Submit information security awareness plan for approval.	Senior executive management group	Annually
	Endorse and submit information security initiatives for approval.	Senior executive management group	Ad hoc
Monitor conformance and performance	Submit the completed information security compliance checklist	Senior executive management group	DD Month each year as of YYYY
		Office of eGovernment	30 June each year as of 2013
	Endorse and submit information security incident reports	Senior executive management group	At least quarterly
	Report on key performance indicators for information security plans	Senior executive management group	Quarterly
	Provide annual report on the information security governance body's performance.	Senior executive management group	Annual

Role	Reporting requirement	Audience	Frequency/Date
Develop information security capability	Report on the agency's information security maturity level.	Senior executive management group	Annual

Delegation

Responsibility for specific aspects of information security governance may be delegated. However, accountability for information security governance resides with the information security governance body and ultimately the agency Secretary/CEO.

Operation

The information security governance body should convene at least every three months. The timing of these meetings should complement both agency planning cycle requirements and ongoing review processes.

Review

The information security governance body should identify indicators of its own performance and conduct an annual performance review against these. This should culminate in an annual report to the senior executive management group which identifies issues and makes recommendations on corrective actions.

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 Internal Governance Guideline, Queensland Government ICT Policy and Coordination Office, Department of Public Works
- Information Steering Committee Terms of Reference, Queensland Government ICT Policy and Coordination Office, Department of Public Works
- 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

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

Attachment 1 Information Steering Committee Terms of Reference

1. Membership (Example membership)

- Deputy Secretary Corporate Services
- Director, Finance
- Director, Information Technology and Management
- Director, Planning
- Director, Human Resources
- Business Unit Managers/directors
- Manager Internal Audit
- External Representative
- E-Business Representative

2. Roles

The Departmental Information Security Steering Committee has responsibility for ensuring:

- the Department's deployment of information technology is directed at the effective and efficient management of the Department's information resource; and
- that appropriate security measures are developed, endorsed, instituted and monitored.

The role of the Departmental Information Security Steering Committee includes, but is not necessarily limited to, the following functions:

- define the mission and goals of the information functions within the mission statement of the Department;
- identify strategic services with cross-department involvement
- authorise and direct the development of a IS resources plan for the Department;
- recommend a departmental IS resources plan

Plan to the Director Corporate Services for endorsement;

- review and approve the IS resources plans which are developed by the business areas of the Department;
- monitor progress against the departmental IS resources plan;
- review, approve and monitor information and information technology policy and standards for the Department;
- maintain an ongoing representative on the WoG Information Managers Group reporting status of Departmental progress towards compliance throughout the agency with relevant Government Information Standards;

3. Reporting Relationships

The Departmental Information Security Steering Committee reports to the xxx (executive management committee or like).

4. Matters For Consideration

These issues are examples which could be considered by the Committee:

- Departmental progress against implementation of the WoG Policy;
- Major IS implementation activities;
- Major Projects with IS implications

(While the Information Security Steering Committee does not necessarily have the power to approve or otherwise a major business unit project, the Department's Project Management Standards should probably specify any projects should report on the IS status to the committee.

Prior to project initiation, the Committee may:

- consider the intention of the project and its consistency with the Departmental IS Resources Plan;
- consider the opportunities for leveraging off the initiative;
- help to identify possible issues/duplication;
- help to qualify the business case for the project;

During the project the Committee may:

- consider issues arising which may impact the Department or the implementing Business Unit, with a view to assisting with resolution;

On completion of the project, the Committee may:

- consider the implementation review;
- leverage off positive outcomes;
- learn from negative outcomes;
- understand positive / negative impacts on the Department; and
- make this information readily available throughout the Department.
- Relevance and completeness of Departmental Information Policy development
- Compliance with Departmental Information Policy
- Business Area Information Steering Committee issues referred to this committee
- Issues arising out of IT Managers meeting;
- Consideration of recommendations of the IT Managers on IT project documents or other project deliverables submitted for acceptance or endorsement;
- Issues referred by other Departmental Committees

5. Induction Processes

New members must familiarise themselves with the Departmental Advisory Committee structure and the terms of reference for each committee.

6. Information Requirements

At each Information Security Steering Committee meeting the following could be used as examples for issues to be discussed:

- Information on major IS projects milestones
- New / revised Information Policy/Procedures/Plans
- Business area Information Security issues
- Issues arising out of IT / IM Managers meeting
- Issues referred by other Departmental Committees

7. Reporting Requirements

A quarterly report must be presented to xxx (for example the executive)

The report is to summarise the matters considered by the Information Security Committee during that quarter, highlighting key issues related to strategy, projects progress and policy.

8. Procedures

8.1 Meeting Frequency

8.2 Submissions

8.3 Presentations to the Committee

8.4 Agenda

8.5 Minutes

8.6 Responsibility for Actions and Communication

8.7 Maintenance of Records