Information Management Advice 35: Implementing Information Security
Part 1: A Step by Step Approach to your Agency Project

Introduction

This Advice provides an overview of the steps agencies need to take to implement the mandatory requirements of the Tasmanian Government Information Security Policy Manual. In particular it focuses on the establishment of a governance structure, developing an information security plan, and an information security policy for your agency.

Information Management Advice 35 consists of 4 parts:

- **Part 1: A Staged Approach to your Agency Project**
- **Part 2: A Step by Step approach to developing an Information Security Plan**
- **Part 3: Establishing Information Security Governance**
- **Part 4: Developing an Information Security Policy Framework**

This Advice - Part 1 provides an overview of the steps recommended to implement an information security project. Its primary focus is the project management activities required for implementation.

Overview

The steps described below are based on the Plan, Do, Check and Act (PDCA) model suggested by the International Standard 27001.

Plan: Establish Agency Information Security Management

Step 1: Assign Agency Responsibility for Information Security

Step 2: Establish Information Security Governance

Step 3: Perform a Gap Analysis

Step 4: Develop a Project Implementation Plan

Step 5: Identify and Classify Information Assets

Step 6: Identify and Assess Risks

Step 7: Plan for Risk Management

Step 8: Develop an Agency Information Security Plan

Step 9: Define Information Security Policy and Procedure Framework

Step 10: Develop Information Security Policies

Do: Implement and Operate Information security

Step 11: Implement Risk Mitigation Strategy

Step 12: Implement Agency Awareness Raising Program

Step 13: Prepare an Incident Response Plan

Step 14: Business Continuity and Disaster Recovery Plan

Check: Monitor and Review Information Security

Step 15: Monitor and Review Information Security

Act: Maintain and Improve Information Security Management

Step 16: Maintain Information Security Management and ensure continual improvement

Table 1: The Plan, Do, Check, Act (PDCA) model applied to Information Security Management System (ISMS) processes (Source International Standard 27001)

Plan **(establish the ISMS)**	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do **(implement and operate the ISMS)**	Implement and operate the ISMS policy, controls, processes and procedures.
Check **(monitor and review the ISMS)**	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act **(maintain and improve the ISMS)**	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Critical Success Factors

In addition to management commitment the successful implementation of information security within an agency will depend on several factors, notably:

- Information security policy, objectives and activities reflect business objectives.
- Recognition that information security is a business issue not an IT problem.

- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the agency culture and involves stakeholders.
- A realistic assessment of the security risks.
- Provision of resources for information security management.
- The existence and use of an agency security architecture.
- Effective promotion of information security to all managers, staff and other parties to achieve awareness.
- Appropriate awareness training and education to all staff.
- Establishing an effective information security incident management process.
- Processes to measure the ISMS, evaluate its performance and feed into the improvement process.

Indicators of an effective IS framework include:

- The Board or equivalent requires and receives regular reports about information security performance and events.
- Information security is a standing item on the agendas of risk management committees up to executive level.
- Information security risk levels are set by the executive level and reflect the agency's risk appetite.
- Business unit managers are responsible for the security of the information underpinning their operations.
- The inherent information risks in critical business processes are understood and documented.
- Individuals are held accountable for any security breaches in which they participate, whether intentional or accidental.
- Regular review of information security products and services to ensure they are cost effective.

There must be a regular review of information security arrangements to ensure continued relevance and continuous improvement.

Step 1: Assign Agency Responsibility for Information Security

Responsibility for implementing Information security needs to be assigned to staff at an appropriate level in the agency. They require a background in information management and experience in project management. The level of resourcing required will depend upon the size and complexity of the agency. For large agencies they will need a project manager assigned full time to the project for at least the Plan stage – Steps 1-10 and then part time to complete the remaining steps. Ongoing responsibilities for Information Security monitoring, reporting and review need to be assigned to an Information Security Officer or Manager (depending upon the complexity of the agency). For more details about roles and responsibilities in information security governance see Part 3 of this advice.

Step 2: Establish 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.

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.

Roles and responsibilities relating to information security within the agency should also be defined. The information security governing body should report through an appropriate Executive of the agency and should be responsible for:

- protecting the agency's information and information assets;
- managing vulnerabilities within the agency's ICT infrastructure;
- reviewing threats and incidents which adversely impact on the agency's information assets;
- assuring (through policy) the appropriate use of the agency's information assets; and
- educating staff about their information security and privacy protection responsibilities.
- Developing an information asset register

The governing body for information security within the agency will need to approve the project deliverables and approve (or request approval for) the funding of projects to implement the controls needed to reduce the risks to significant information assets.

If the agency does not yet have an effective structure for information security governance, it should review the structure and authority for information security governance within the agency and resolve any issues that arise.

For details on how to establish an IS Governance structure and definitions of roles and responsibilities see Part 3 of this advice.

Step 3: Perform a Gap Analysis

The gap analysis will assist you to determine your agency's current state of information security. The gap analysis process involves determining, documenting and obtaining management recognition of the difference between the mandatory requirements in the Whole of Government (WoG) IS Policy Manual and the agencies current information security program.

A gap analysis comprises a series of questions for each mandatory requirement and seeks to discover if there is a documented process in place that adequately addresses the intent of each requirement. Each question is answered 'Yes', 'Partly' or 'No' and must include justification for each response answered 'yes' and 'partly' along with planned mitigation actions for 'no' responses. The identified gaps provide management with insight into the areas within the information security program which need to be improved. Once the gaps are identified, a project plan can be developed which provides a foundation for setting priorities, assigning ownership and allocating investments of time and resources for implementing IS. See Attachment 1for a gap analysis template. The results of this step will be documented in the Agency Information Security Plan. The Checklist for Your Agency's Current Information Security Practices which accompanies TAHO Information Management Advice 32 can assist.

Step 4: Develop a Project Implementation Plan

The IS project requires planning. The project manager needs to develop a Project Plan to determine timeframes for implementation and roles and responsibilities. The Tasmanian Government Project Management Guidelines includes a template for a project plan. This is available from http://www.egovernment.tas.gov.au/project_management

Step 5: Identify and Classify Information Assets

If it hasn't already done so, the agency should develop a list of information assets. Significant information assets are those which are crucial to the achievement of the agency's mission. The identification of information assets is an essential prerequisite to the completion of the Risk Assessment. There is also a need for a good knowledge of the agency's overall inventory of information assets, including tools and utilities used for systems and network operations and management, which may potentially be used to compromise significant information assets.

If the agency does not have such an information asset register, or the inventory is out of date or otherwise inadequate, it will need to ensure that any deficiencies are identified and rectified before completing a risk assessment.

All information assets need to be identified including those information assets which may be used to compromise the security of significant information assets. A good question to ask is: 'Could this asset be used to bypass normal security and compromise sensitive information, and would the impact be High or Very High. If the answer is 'Yes', then this information asset must also be included in the Risk Assessment.

Examples of significant information assets could include:

- data centres which host agency systems;
- applications used for the delivery of agency services online, or through agency offices, or through downstream customer service organisations, etc.;
- applications containing information classified as PROTECTED; or
- networks that allow:
    - agency customers to communicate with the agency online, or by telephone, etc; or
    - agency offices or downstream customer service organisations to access significant agency applications.

Examples of other information assets which may be used to compromise the security of significant information assets are:

- Systems/network management tools which can be used by systems administrators to look at server information, network traffic, application databases, etc.

The results of this step will be documented in the Agency Information Security Plan. For more advice on developing an Information Asset Register See TAHO *Advice 39 Developing an Information Asset Register*.

Step 6: Identify and Assess Risks

Identifying and assessing Risks for IS Project needs to occur at two levels

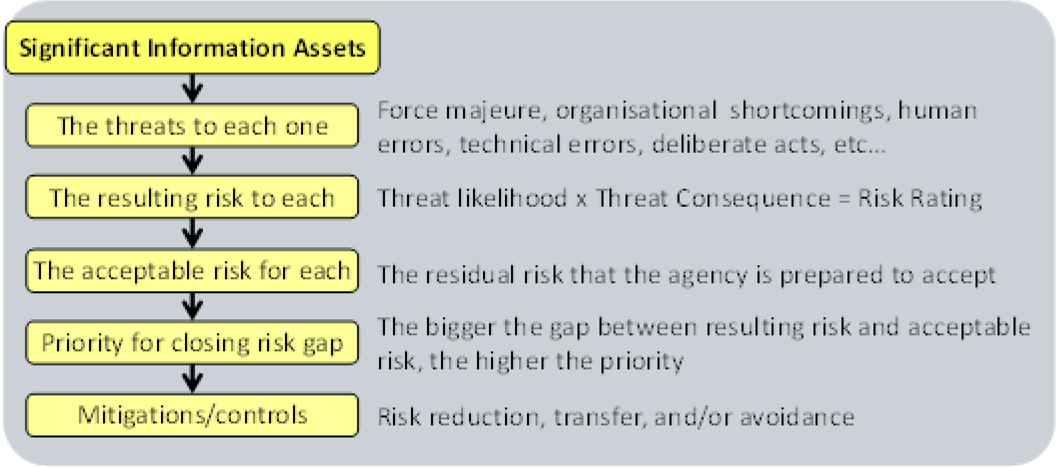
1. Assess IS risks to the agency
2. Assess IS risks against information assets

A risk assessment of IS risks the agency faces should be undertaken. This includes risks in areas of project failure, possible information security incidents etc.

A Risk Assessment of information assets is a high level self-assessment performed against the list of information assets within the agency. It reviews the high level risks to the portfolio of significant information assets, and develops high level risk mitigations to reduce the risks to an acceptable level. The Risk Assessment Report should not attempt to 're-invent the wheel'. Existing material which may be re-used to reduce the effort required includes;

- previously developed agency ICT risk assessments (e.g. within a Risk Management unit); and/ or
- an existing Risk Assessment Report ; and/ or
- previous assessments of agency information classifications; and/ or
- reports from third parties, including ICT shared services providers; and/ or
- other similar documents.

The threats to each of the significant information assets then inform the identification, analysis, and evaluation of risks.


Significant Information Assets
The threats to each one
Force majeure, organisational shortcomings, human errors, technical errors, deliberate acts, etc...
The resulting risk to each
Threat likelihood x Threat Consequence = Risk Rating
The acceptable risk for each
The residual risk that the agency is prepared to accept
Priority for closing risk gap
The bigger the gap between resulting risk and acceptable risk, the higher the priority
Mitigations/controls
Risk reduction, transfer, and/or avoidance

Establishing the risk assessment group

Completing Risk Assessment(s) requires multiple skills:

- experienced agency users or management who are familiar with agency services and processes and the related ICT risks the agency faces;
- information and physical security staff, who are familiar with the agency's security controls;
- ICT infrastructure or systems administration staff, who are familiar with the way the agency's ICT assets interconnect, the risks to systems and networks, and the existing information security controls; and
- agency or risk management staff, who may have performed risk assessments in the past.

Note the two different risk assessments may require different stakeholders to be involved.

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 utilise *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*. The results of this step will be documented in the Agency Information Security Plan.

Step 7: Plan for Risk Management

Options for risk management are based on cost benefit analysis of various options available to manage the risk. Broadly these are:

- Transfer the risk: For example, take a fire insurance policy and transfer the risk for fire to an insurance company.
- Avoidance of the risk: For example, if there is an old server which is malfunctioning, replacing it will avoid all the associated risk.
- Acceptance of the risk: You are aware of the risk but the solution to avoid the risk is too costly. You decide to live with the risk and face the consequences.
- Risk reduction: You decide to tackle the risk and plan to identify the security measures, which will reduce the risk to an acceptable level.

International standards *AS/NZS ISO/IEC 27001* and *27002*, available from http://www.egovernment.tas.gov.au, provide examples of controls, which can be deployed to reduce the risk. However, these controls are general in nature. Selection of specific controls should be based on threat and risk assessment performed in the earlier step. Also see *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines* available from http://www.egovernment.tas.gov.au

The following steps could be used to select appropriate controls:

- Define security policies
- Define Procedures
- Define Standards
- Identify Security products
- Undertake a cost benefit analysis of the options
- Prepare current state assessment and gap analysis: prepare a table of all the Threats /Risk and identify where these risks are being controlled in the current security set up. Identify all the gaps and inadequacies in the current set up and present it to the agency's senior executive with cost benefit analysis. The results of this step will be documented in the Agency Information Security Plan.

Step 8: Develop an Agency Information Security Plan

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 Attachment 1 of this advice for a Template for a Gap Analysis.

Step 9: Define Information Security Policy and Procedure Framework that will be developed for the agency

The IS project manager for the agency needs to define for the governance committee the IS policy and procedure framework that will be developed for the agency IS project. A security policy should fulfil many purposes. It should: protect people and information;

- set the rules for expected behaviour by users, system administrators, management, and security personnel;
- authorize security personnel to monitor, probe, and investigate;
- define and authorize the consequences of violation;
- define the agency consensus baseline stance on security;
- help minimize risk; and help track compliance with Whole of Government Policy, regulations and legislation.

The policy framework for the agency is the tool that implements IS throughout the agency. It supports change to agency procedures and day to day behaviours, thereby applying IS at an operational level.

Although the importance of information security for agencies is increasingly recognized, the complexity of issues involved means that the size and shape of information security policies may vary widely from agency to agency. This may depend on many factors, including the size of the agency, the sensitivity of the information they create and manage, and the numbers and types of information and computing systems they use. Another factor is the maturity of the policy development process currently in place. An agency which currently has no information security policy or only a very basic one may initially use a different strategy to an agency which already has a substantial policy framework in place, but wants to tighten it up and start to use policy for more complex purposes such as to track compliance with legislation.

It should be noted that there is no single method for developing a security policy or policies. For large agencies, developing a single policy document that speaks to all types of users within the agency and addresses all the information security issues necessary may prove impossible. A more effective concept is to develop a suite of policy documents to cover all information security bases; these can be targeted for specific audiences, making a more efficient process for everyone

When starting out it is a good idea to use a phased approach, starting with a basic policy framework, developing the major policies that are needed and then subsequently developing a larger number of policies, revising those that are already in place and adding to this through the development of accompanying procedure documents which will help support policy.

Part 4 of this advice examines the elements that need to be considered when developing and maintaining information security policy and goes on to present a design for a suite of information security policy documents and the accompanying development process.

Note that Part 4 of this advice presents a policy framework for a fairly mature, developed process, probably aligned to that possible in a large agency where policy development has been underway for several years. For smaller agencies or for those just starting to develop policy, it is possible to use this basic framework, but it may be helpful to begin with a smaller number of Technical Policies. Rather than trying to develop a large hierarchy all at once, it is more realistic to develop a Governing Policy and a small number of Technical Policies initially, and then increase the number of policies and supporting procedures, to support the ongoing development of the policies as you move forward.

In large agencies there will be several audiences for your policy, and you will want to cover many different topics on different levels. For this reason, a suite of policy documents rather than a single policy document will work better.. The hierarchical structure of the suite of security policy documents reflects the hierarchical structure of roles in a large agency. The proposed scheme provides for all levels of audience and for all topics by using two policy types supported by procedural documents:

- Governing Policy
- Technical Policies
- Procedures

Step 10: Develop Information Security Policies

An Information Security Policy is a high level document covering the principal information security objectives of the agency. It is informed by the Risk Analysis, and the guidelines and legal framework under which the agency operates. It demonstrates how compliance with the WoG IS Policy Manual is measured internally, and externally.

Security policy is the demonstration of management's intent and commitment for information security in the agency. This should be based on facts about the criticality of information for the agency as identified during risk analysis. Security policy statement(s) should strongly reflect the Executive's belief that if information is not secure, the agency will suffer. The policy should clearly address issues like:

- Why information is strategically important for the agency?
- What are business and legal requirements for information security for the agency?
- What are the agencies' contractual obligations towards security of the information pertaining to business processes, information collected from clients, employees etc.?
- What steps the agency will take to ensure information security?

A clear security policy will provide direction to the information security efforts of the agency as well as create confidence in the minds of various stakeholders.

The CEO/ Secretary of the agency should issue the security policy statement to build the momentum towards information security and set clear security goals and objectives.

Step 11: Implement Risk Mitigation Strategy

Implementation of risk mitigation strategy involves converting all the risk management plans into actions. As an outcome of the previous step you should have the following items ready for implementation:

- Detailed Security Policies
- Procedures and guidelines
- New security products
- Improvements for existing devices

The results of this step will be documented in the Agency Information Security Plan.

Step 12: Implement Agency Awareness Raising Program

Information security management involves each and every person who interacts with information. Broadly speaking, it will be everybody who ever touches the keyboard or mouse, or enters a government building. Each person has the capability of sabotaging information security through ignorance, or with malicious intent. Training should explain each individual's role in maintaining the information security and his/her responsibilities towards every information asset that they handle. Training each person on information security is similar to training the entire organization about fire prevention measures. Training should be comprehensive and adequate to ensure that each person clearly understands the security policies of the agency, various security risks and threats and finally consequences of not abiding by the security procedures. Agencies should implement the following:

- Information security training programs. These programs should be designed for all levels including senior management, general staff including volunteers, and contractors. The training programs should be relevant to the organization's security requirements, and as such, should be based on the security policy and risk assessment performed for the organization.
- Creating Information Security awareness - To ensure that information security measures do not become routine stuff and get ignored, create IS acceptable use agreements, and put regular reminders about staff obligations in newsletters to keep the interest in security topics alive. Also, give publicity to relevant security incidents. There will be increased awareness if the hypothetical threats are realised.

The development of IS awareness programs should be included in the project plan and IS Plan. IS awareness training for senior management and staff is currently being developed and will be available for use in your agency.

Step 13 Prepare Incident Response Plan

Your agency should already have a plan or policy for dealing with major information security incidents. At a minimum, the plan should include:

- what constitutes an information security incident (e.g. definitions and examples of major and minor security incidents to guide the level of response);
- the minimum level of security incident response, and investigation training for users and system administrators;
- the authority responsible for initiating investigations of information security incidents in the agency;
- the steps necessary to ensure the integrity of evidence supporting an investigation;
- the steps necessary to ensure that significant systems remain operational during the investigation of an incident; and
- how to report an information security incident.

Step 14: Business Continuity and Disaster Recovery

Agency business continuity plans should be reviewed and tested on a regular basis to ensure that all current business and ICT systems and infrastructure are accounted for. When developing the agency testing strategy, the importance of each system to the business operations and the ability to recover it within the time frames required by users should determine the extent of the testing. Business continuity plans should ensure that information security controls are maintained and this should be within scope of the testing strategy.

Agencies should also undertake a review of their plans and strategies after any significant disruption to information services or failure to ascertain the cause, assess the remedy and ensure procedures are adjusted to reduce the likelihood of any repeat occurrence. For further information, please refer to *Australian Standards HB:221:2004 Business continuity management.*

Disaster recovery

To ensure the availability of information, and ICT systems and services following a disaster, agencies need to document information and ICT disaster recovery plans. When documenting agency information and ICT disaster recovery arrangements, agencies should develop an ICT asset disaster recovery planning guideline. The plans should ensure that information security controls are recovered as part of the plan.

When developing information risk management strategies to assess the vulnerability of information and ICT assets and the impact on these assets as a result of a security failure or a disaster, agencies should consider adapting the *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*.

Agencies should establish an information and ICT asset disaster recovery register to assess and classify systems to determine their criticality. This register does not need to be a new register, agencies are free to utilise existing registers that they may have, provided that they assess and classify information and ICT assets to determine their criticality. See TAHO *Advice 26: Disaster Preparedness and Recovery.*

Step 15: Monitor and Review Information Security

Implementation of information security is not a one-time job. It needs to be constantly monitored and reviewed. Create the following mechanism for effectively monitoring and reviewing performance.

Information Security Reporting

Put procedures in place for the management and review of responding to security incidents and malfunctions. This may involve the following measures: reporting of security incidents, security weaknesses, software malfunctions and operator logs, and fault logs. Each of these controls will generate huge amount of information. Ensure that this information is properly recorded and stored for any analysis.

Review Mechanisms

The incident reports will be of no use if they are not reviewed regularly. The formation of security organization should include assigning specific responsibilities to teams or individuals to periodically review the logs and reports.

- Internal Audit - Periodic audit should be performed to review the performance of various controls and measures defined in the policy framework. Internal audit teams or external consultants may perform the audit. The audit findings should be documented and all nonconformities must be corrected and reported within a specific time frame.
- Management Review - The Security Steering Committee should conduct management review of the performance of ISMS at least once a year. This review should be based on various reports submitted by incident reporting and review processes, and internal audit reports.

Step 16: Maintain Information Security Management and Ensure Continual Improvement

Implementing IS will not ensure sudden improvement in the information security stance of the organization. It provides an opportunity to monitor the security in an organized manner and ensure continual improvement. You can ensure that the continual improvement actually takes place by having the following measures in place:

Management review and follow-up

Management review should ensure that appropriate actions are taken on various security lapses reported through the following mechanisms:

- Incident response reports
- Internal audit reports
- External audit reports
- Learning from incidents
- Disciplinary process

Each such report and the actions taken to improve the security should be followed up in subsequent meetings until a measurable improvement is shown.

New Business Requirements

New business requirements will require deployment of new and untested technologies. These could expose the information systems to new threats. In such cases, a fresh risk assessment may be necessary before making changes.

Identification of New Threats

New threats may be identified in existing implementations. Periodic risk assessment should be done to evaluate the impact of new threats on the existing security implementation.

Internal and/ or external auditor

During the initial audit, the auditors may check any aspect of your IS implementation. They may check how the controls have been decided, i.e. evaluating your risk assessment methodology, how the controls have been implemented and how these are being maintained. The auditors may test a few controls at random. They may interview a few end-users to check their understanding of the security. They may review the business continuity plan and how often it is being tested and revised. Statement of applicability will be analysed and your approach will be verified. You should also be ready with all the minutes of various review meetings, including the Security Steering committee minutes.

Resources

- AS/NZS ISO 31000:2009 Risk management – Principles and guidelines available from http://www.egovernment.tas.gov.au
- Standards Australia HB 231:2004 Information security risk management guidelines available from http://www.egovernment.tas.gov.au
- Standards Australia HB 327:2010 Communicating and consulting about risk (Companion to AS/NZS ISO 31000:2009)Available from http://www.egovernment.tas.gov.au
- AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management available from http://www.egovernment.tas.gov.au
- Standards Australia HB 221:2004 Business Continuity Management available from http://www.egovernment.tas.gov.au

Acknowledgements

- Information Standard 18: Information Security – Implementation Guideline, 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
- ISMF Implementation Guideline, Department of Treasury and Finance, Victorian Government

- Information Security Policy –A Development Guide for Large and Small Companies SANS Institute http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331?show=information-security-policy-development-guide-large-small-companies-1331&cat=policyissues (Accessed October 2013)
- Implementation Methodology for Information Security Management System (to comply with BS7799 Requirements) SANS Institute, Avinash Kadam, http://www.giac.org/paper/gsec/2693/implementation-methodology-information-security-management-system-to-comply-bs-7799-requi/104600 (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

Attachment 1: Gap Analysis Template

Imagine that you've just been asked to implement information security Policy for your agency.

You already have some possible solutions in mind. However, before you choose a best solution, you need to identify what needs to be done to meet this project's objectives.

This is where Gap Analysis is useful. This simple tool helps you identify the gap between your current situation and the future state that you want to reach, along with the tasks that you need to complete to close this gap.

Gap Analysis is useful at the beginning of a project when developing a Business Case, and it's essential when you're identifying the tasks that you need to complete to deliver your project successfully.

Using Gap Analysis

To conduct a Gap Analysis for your project, follow these three steps:

1. Identify Your Future State

First, identify the objectives that you need to achieve. This gives you your future state - the "place" where you want to be once you've completed your project.

Simple example:

Future State	**Current Situation**	**Next Actions/Proposals**
Implement Information Security Policy		

2. Analyse Your Current Situation

For each of your objectives, analyse your **current situation**. To do this, consider the following questions:

- Who has the knowledge that you need? Who will you need to speak with to get a good picture of your current situation?
- Is the information in people's heads, or is it documented somewhere?
- What's the best way to get this information? By using brainstorming workshops? Through one-to-one interviews? By reviewing documents? By observing project activities such as design workshops? Or in some other way?

Simple example:

Future State	**Current Situation**	**Next Actions/Proposals**
Implement Information Security Policy	Agency **does not have**: • Information Security Policy	

	- Information Security Plan - Information Security Framework - Information Security Governance Committee - Up to date Information Asset Register	

3. Identify How You'll Bridge the Gap

Once you know your future state and your current situation, you can think about what you need to do to bridge the gap and reach your project's objectives.

Simple example:

Future State	**Current Situation**	**Next Actions/Proposals**
Implement Information Security Policy	Agency **does not have**: - Information Security Policy - Information Security Plan - Information Security Framework - Information Security Governance Committee - Up to date Information Asset Register	1. Identify Project Owner and Sponsor 2. Develop an Information Asset Register 3. Undertake a IS risk Assessment 4. Draft Information Security Plan 5. Decide an Information Security Policy Framework 6. Develop IS Policies 7. Develop IS Procedures

Tips:

Pitch your Gap Analysis to provide an appropriate amount of detail. If you present too much detail, people will be overwhelmed, but if you don't give enough detail, you won't tell them what they need to know to sign the project off.

When you analyse your future situation and current state, use metrics where information can be quantified (such as "Salary costs account for 50 percent of the cost of the product"), and general statements when metrics aren't available (such as "Creativity is valued within the organization")

Also remember that your assessment of the current situation and the desired future state can be both quantitative and qualitative.

For instance:

	Current Situation	Future State
Quantitative	Total costs are $100 per unit.	Total costs will be $80 per unit.
Qualitative	Team members work in isolation.	Team members will work collaboratively.

Note:

While this example illustrates a very simple use of Gap Analysis, this approach can be very extensive and complex, for example, when it is used to identify software modifications needed as part of IT projects. Don't underestimate how much work your Gap Analysis may involve!

Key Points

Gap Analysis compares your current situation with the future state that you want to achieve once your project is complete. By conducting a Gap Analysis, you can identify what you need to do to "bridge the gap" and make your project a success. You can use Gap Analysis at any stage of a project to analyse your progress, but it's most useful at the beginning.

To carry out a Gap Analysis, first identify your project's objectives - this is your "future state." Then analyse your current situation, making sure that you gather information from the right sources.

Finally, identify how you'll bridge the gap between your current situation and the desired future state.