Australian Government

Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements

July 2013

Version 1.0

Contact us

Inquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General's Department
3-5 National Cct
BARTON ACT 2600

Telephone: (02) 6141 6666

copyright@ag.gov.au

Document details	
Security classification	Unclassified
Dissemination limiting marking	None
Date of security classification review	Not applicable
Authority	The Attorney-General
Author	Attorney-General's Department
Document status	Approved 5 July 2013

Contents

Amendments

No.	Location	Amendment

1. Policy

Based on a sliding scale of risk and community expectations, this policy establishes a whole-of-government approach to how different categories of information are treated when considering offshore or outsourced ICT arrangements; and maintains agency head responsibility for managing agency information with appropriate ministerial oversight. The policy and guidelines apply to agencies which implement the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

Most Australian Government information is unclassified and has been provided to the Government by citizens and businesses. In many instances the provision of such information is required by law. As such, the community expects the Government to protect information from unauthorised access or inadvertent public release. Where there are risks to personal information that may lead to widespread loss of public confidence and trust in Government, Ministers should be made aware and agree to the controls.

Under existing policy frameworks, such as the PSPF and the ISM, agency heads are required to adopt a risk-based approach to assessing the risk and sensitivity of various categories of information when making ICT design decisions. The objective of a risk-based approach is to ensure the level of protection afforded to Australian Government information is consistent with its value. As part of these arrangements, agencies have obligations regarding the storage and processing of Government information in outsourced or offshore ICT arrangements. Under this policy detailed in Table 1, and the existing obligations under the PSPF and ISM, agency heads:

- are to apply a risk-based approach
- are to document that they have calculated and accepted the associated security risks, where applicable, in accordance with these guidelines
- are not to enter into arrangements where risk of outsourcing or offshoring Australian Government information cannot be quantified due to insufficient information or because the risks are too complex to be calculated
- can enter into outsourced and offshore arrangements for unclassified information (both publicly and not publicly available) if the risks can be appropriately managed, with the exception of personal information (as defined in the *Privacy Act 1988*), which may require additional approvals (see next)
- who intend to hold personal information (as defined in the *Privacy Act 1988*) in offshore or in outsourced onshore public cloud arrangements are to have ministerial approval (both the relevant agency's Minister and the Attorney-General as the minister responsible for privacy and protective security)
- are to ensure security classified information is handled in accordance with existing policies and guidance including the PSPF and the ISM, and
- cannot enter into arrangements for the storage or processing of classified information in outsourced – domestically hosted (onshore) public cloud or offshore arrangements. The exception to this is where information is covered under international information sharing arrangements or is held in formally accredited classified systems, such as in Australian embassies.

Figure 1 provides an alternate representation of the policy, describing the classes of information and controls. A decision tree has also been developed (see Figure 2) to assist agencies determine their responsibilities under the policy.

Table 1: *Policy for the Storage and Processing of Australian Government information in Outsourced or Offshore Arrangements*

ICT Arrangement	Unclassified information that is publicly available	Other unclassified information that is not publicly available	All information requiring privacy protections[1]	Security classified information
Offshore and **Outsourced - Domestically hosted (onshore) public cloud**	Agencies can enter into these arrangements following a risk assessment. The handling, storage, transmission, transportation and disposal of information in these arrangements should be done in accordance with the *Australian Government Information security management protocol*.	Agencies can enter into these arrangements following a risk assessment. Agency heads must also document that they have calculated and accept the associated security risks as per the guidelines developed by the Attorney-General's Department.[2]	Agencies cannot enter into these arrangements, unless: 1) relevant portfolio Minister agrees that sufficient technological or other measures have been implemented to mitigate the risk of unauthorised access, and 2) there has been consultation with, and agreement from, the Minister responsible for privacy and the security of Government information (the Attorney-General).	These guidelines do not focus on the controls for Australian Government security classified information which are detailed in the *Australian Government Information security management protocol* and Information Security Manual
Outsourced – Domestically hosted (onshore) private, internal or community cloud	Agencies can enter into these arrangements following a risk assessment. The handling, storage, transmission, transportation and disposal of information in these arrangements should be done in accordance with the *Australian Government Information security management protocol*.			

1.1 Definitions

Unclassified - Not publicly available information: this comprises information that is unclassified, but potentially sensitive such as:

- information on the functioning of Government
- commercial arrangements and certain Government procurements
- documents relating to policy development, and
- advice to Government.

[1] Personal information as defined by the *Privacy Act 1988*.

[2] Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements (these guidelines).

Unclassified - Information subject to the *Privacy Act 1988:* this comprises information that is subject to the *Privacy Act 1988* and includes both 'Personal' and 'Sensitive' information.

- 'Personal information' means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

- 'Sensitive information' means (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information.
- Agencies can consider seeking information from the Office of the Australian Information Commissioner on whether information is likely to be personal or sensitive information.

Unclassified - Publicly available information: this comprises information that the Australian Government makes publicly available. For example,

- Hansard and Government publications

- certain Government procurement

- community engagement and service delivery, and

- press releases.

Security classified information: this comprises information which is security classified at PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET.

Offshore arrangements: information is stored or processed in equipment that is located outside of Australia. The mere transit of information is not considered 'storage' or 'processing' for the purposes of this policy.

Onshore arrangements: information is stored or processed in equipment that is located within Australia.

Domestically hosted public cloud: information is stored or processed in equipment which is located in Australia, offers services to the public, and is not under the direct control of the Australian Government. It involves an organisation using a vendor's cloud infrastructure which is shared via the Internet with many other organisations and members of the public. For example, a multi-tenant data centre located in Australia.

Domestically hosted private cloud: information is stored or processed in equipment which is located in Australia and is restricted to a single or small class of tenants. The facility can be under the direct control of the Australian Government. It involves an organisation's exclusive use of cloud infrastructure and services located at the organisation's premises or offsite, and managed by the organisation or a vendor. For example, a data centre shared between multiple agencies, or a data centre operated by the private sector for use by the Government.

Community Cloud: involves a private cloud that is shared by several organisations with similar security requirements and a need to store or process data of similar sensitivity.

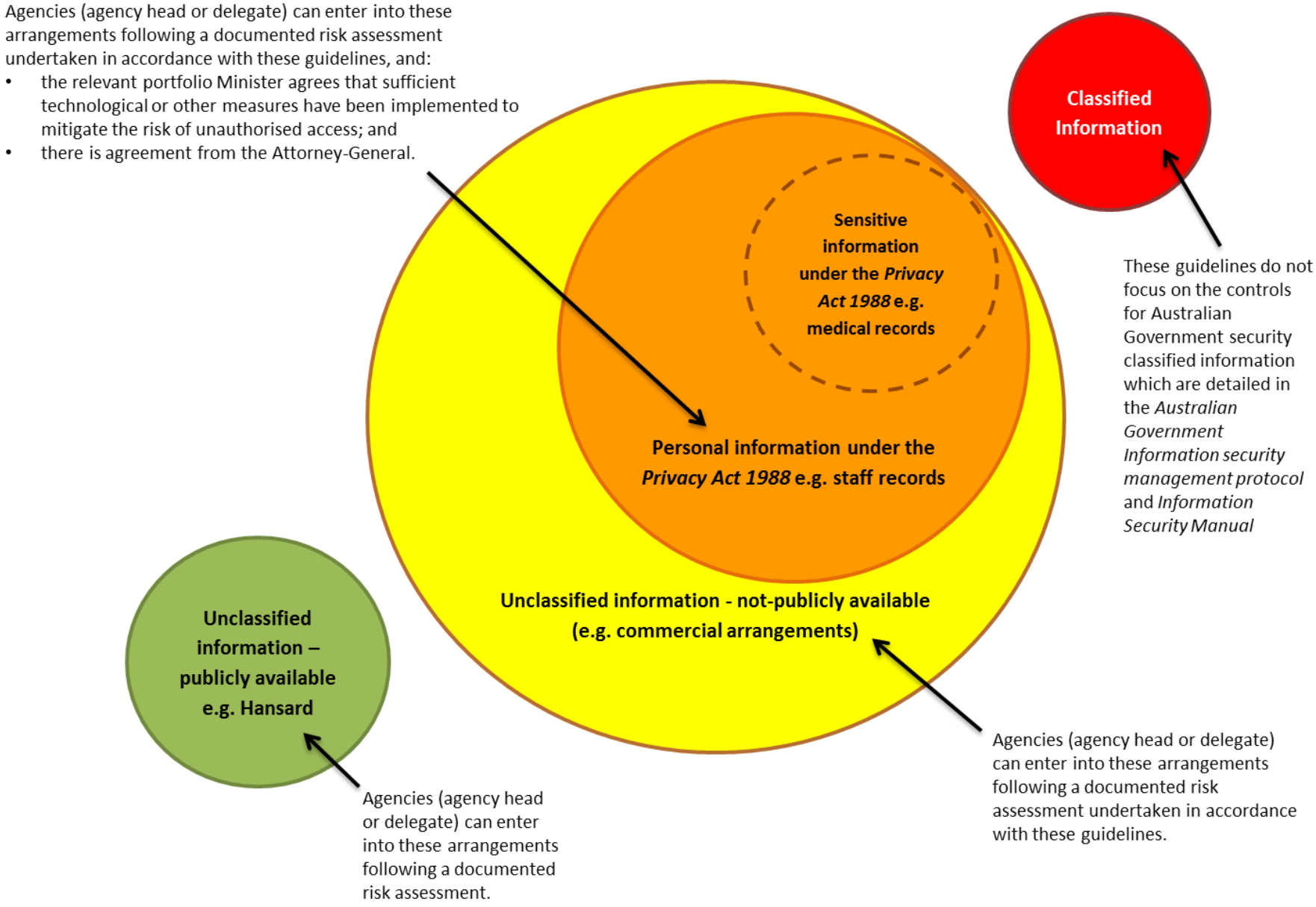

Figure 1: *Policy overview for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements*

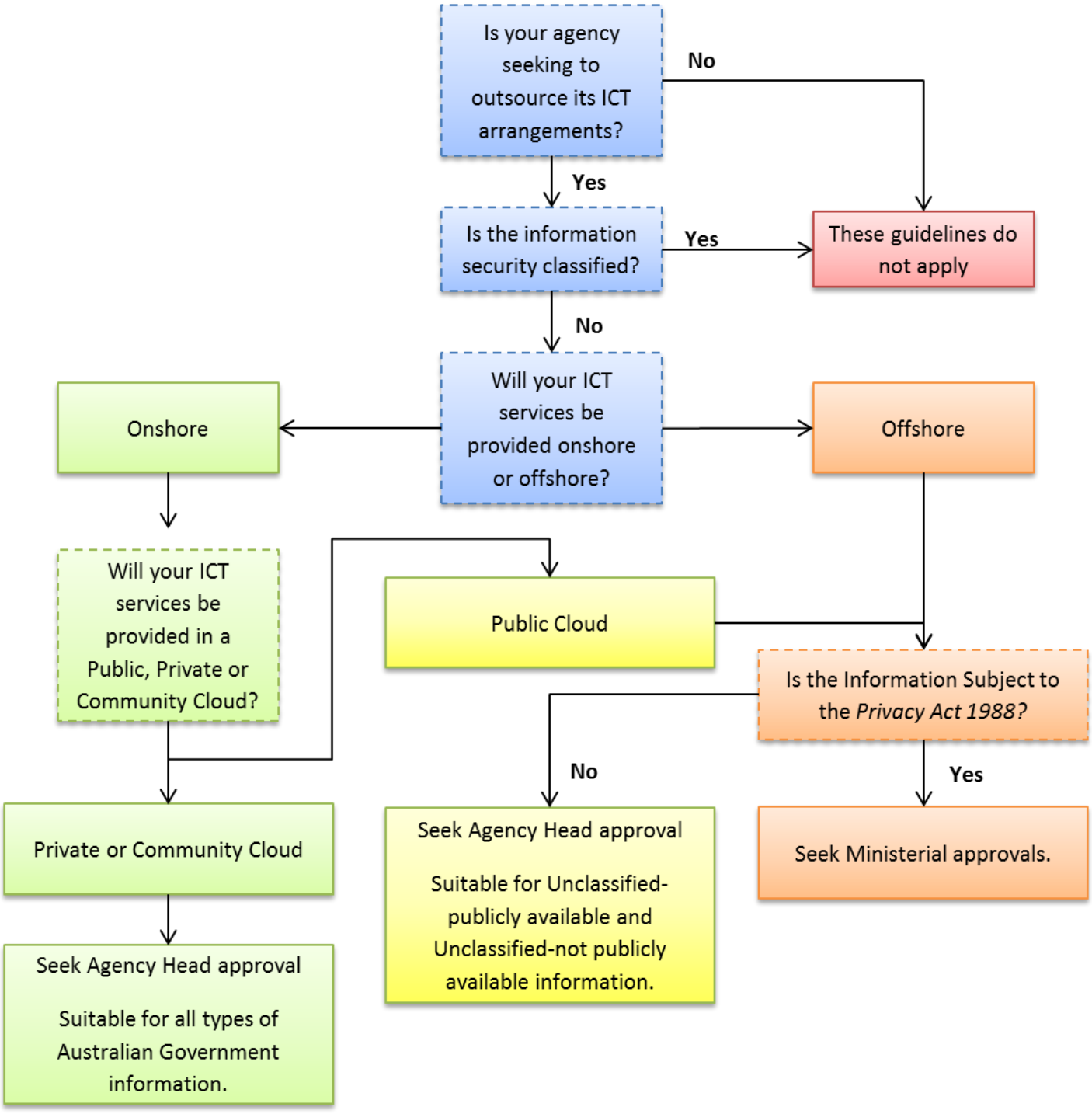

Figure 2: *Policy decision tree*.

2. Guidelines - Introduction

2.1 Purpose

The purpose of this document is to provide guidance to agencies when considering the storage and processing of Australian Government information in outsourced or offshore ICT arrangements.

2.2 Audience

This document is primarily intended for Australian Government employees or contractors performing the role of the Information Technology Security Advisor (ITSA) and/or Chief information Officer (CIO) in support of their agency head and Minister.

2.3 Scope

These guidelines cover Australian Government information proposed to be held in outsourced or offshore arrangements.

These guidelines focus on the risk management of unclassified Australian Government information in outsourced or offshore arrangements (see Figure 1 and Table 1 for policy overview).

These guidelines do not focus on the controls for Australian Government security classified information which are detailed in the *Australian Government Information security management protocol* and the *Information Security Manual* (ISM).

2.4 Why the guidelines were developed

Agencies have procured outsourced arrangements for the storage and processing of Australian Government information for several years, and are actively examining cloud computing services for their possible efficiency, flexibility and lower costs. These guidelines provide a consistent and structured approach to undertaking a risk assessment when considering outsourced or offshore ICT arrangements for Australian Government information. They are intended to assist government decision makers to evaluate the benefits of the adoption of cloud computing services and assist agencies to consider the contextual risks specific to their agency and operating environment. These guidelines do not preclude the offshoring of Australian Government information or prevent the adoption of cloud computing services by agencies.

These guidelines provide generic information and advice to inform the risk assessment process.

2.5 Relationship to other documents

These guidelines support the implementation of the PSPF. In particular, these guidelines support the Australian Government *Information security management core policy* and the *Information security management protocol*, and the Australian Government *Information Security Manual* (ISM). The guidelines are part of a suite of documents including the Australian Government Information Management Office's *Australian Government Cloud Computing Policy,* the Department of Broadband, Communications and the Digital Economy's *National Cloud Computing Strategy*, and the Defence Signals Directorate's *Cloud Computing Security Considerations* which assist agencies in meeting their information security mandatory requirements. Annex A provides a list of relevant documents.

2.6 Use of specific terms in these guidelines

In these guidelines the terms:

- ‘need to’—refers to a legislative requirement that agencies must meet
- ‘are required to’ or ‘is required to’—refer to a control:
    - to which agencies cannot give a policy exception, or
    - is used in other protective security documents that set controls
- ‘are to’ or ‘is to’—are directions required to support compliance with the mandatory requirements of the core policy, and
- ‘should’—refers to better practice; agencies are expected to apply better practice unless there is a reason based on their risk assessment to apply alternative controls.

3. Overview of the risk assessment process

3.1 Risk assessment process

Agencies are required to adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standards AS/NZS ISO 31000:2009 *Risk management – Principles and guidelines* and HB 167:2006 *Security risk management*.

Agencies have different business requirements and operating environments and are usually best placed to:

- identify the agency's level of risk tolerance
- identify specific risks to their people, information and assets, and
- identify appropriate protections to reduce or remove risks.

3.2 Suggested risk assessment framework

These guidelines set out a risk assessment process based on existing frameworks defined in AS/NZS ISO 31000:2009 and HB 167:2006. Sections 4-5 provide step-by step guidance and supporting information to assist agencies undertake a risk assessment for the storage and processing of Government information in outsourced or offshore arrangements. Section 6 outlines agency head requirements for entering into such an arrangement. Risk assessment is a subjective process and agencies should ensure that the process is transparent, justifiable and documented. Figure 3 provides a visual overview of the process and the relevant corresponding guidance.

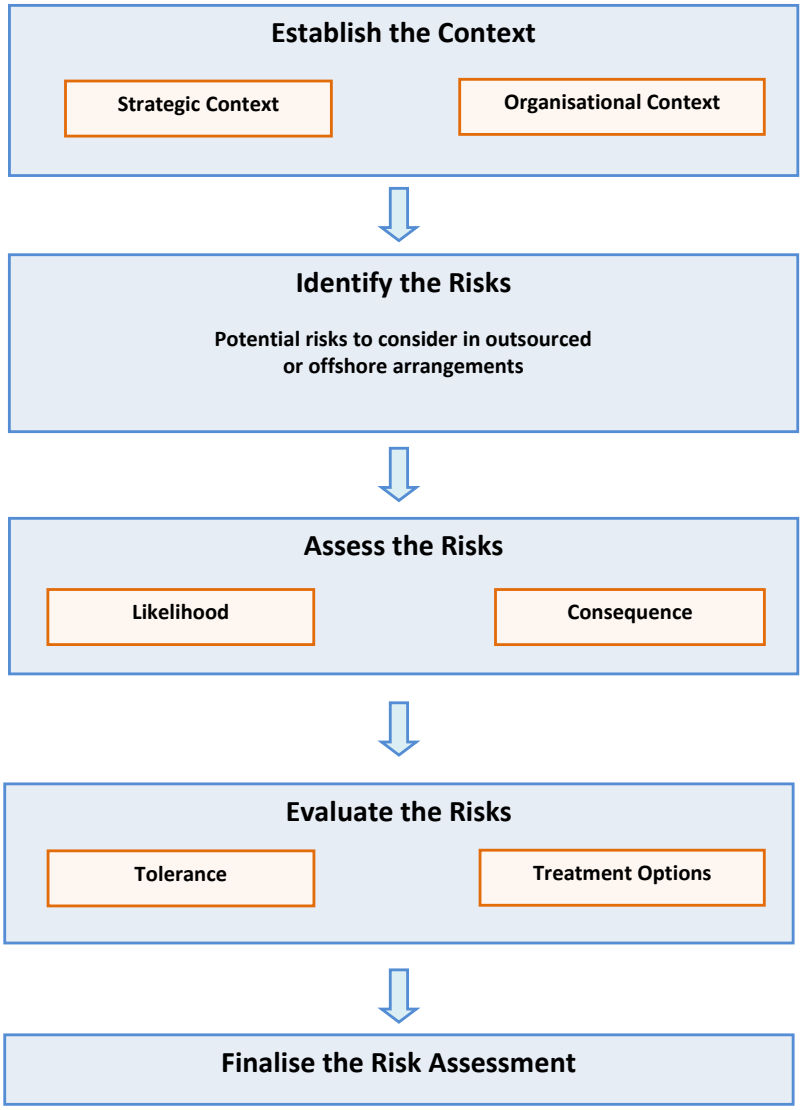

Figure 3: *Overview of the risk assessment framework.*

4. Establish the context

An agency's risk assessment process should address the strategic [4.1], organisational [4.2] and security risk management [4.3] contexts.

4.1 The strategic context of outsourcing and offshoring

The strategic context is the external environment in which the agency seeks to achieve its objectives. The external context can include, but is not limited to:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local
- key drivers and trends having impact on the objectives of the organisation, and
- relationships with, perceptions and values of external stakeholders.

Agencies should consider what aspects of strategic context are relevant to their situation, and factor these into their risk assessment process. These can include:

- relevant Australian legislation, regulation and policy, including responsibility for safeguarding Australian Government information as part of the PSPF (refer Annex A)
- foreign laws and potential jurisdictional access to information, and
- the potential benefits of outsourcing or offshoring arrangements.[3]

4.2 How to determine your organisational context

The organisational context is the internal environment in which the agency seeks to achieve its objectives. This can include, but is not limited to:

- governance, organisational structure, roles and accountabilities
- policies, objectives, and the strategies that are in place to achieve them
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies)
- the relationships with and perceptions and values of internal stakeholders
- the organisation's culture, including the security culture
- information systems, information flows and decision making processes (both formal and informal)
- standards, guidelines and models adopted by the organisation, and
- nature and extent of contractual relationships.

---

[3] Extensive advice exists on this subject. As a starting point, see the Australian Government Information Management Office's *Cloud Computing Strategic Directions* paper.

4.3 How to determine the security risk management context

The risk management context refers to the organisation and parameters of the risk management task itself. Table 2 outlines some elements of the risk management context and suggested parameters when undertaking a risk assessment.

Table 2: *Security risk management factors for consideration*.

Elements of the risk management context	Suggested parameters
Who owns the risk? Who is the decision maker?	Agencies should consider the category of information in the context of the proposed arrangements to determine what level of approval is required. For example ministerial approval is mandatory for the storage of personal information in offshore arrangements.
Defining the goals and objectives of the risk management activities	To take advantage of available technologies and business models while managing the associated risks in considering the storage and processing of Australian Government information.
Defining responsibilities for and within the risk management process	Agency heads may wish to nominate an individual or area to gather information or capture the risk assessment process, including justification for decision-making. Risk Management Officers, agency IT security managers, Chief Information Officers or other equivalent staff are a good place to start when considering who may be an appropriate stakeholder.
Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions	See Section 1.3 for the scope of information covered in this risk assessment process.
Defining risk assessment delivery timeframes	Determined on an agency basis.
Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation	Dependent on project interdependencies.
Defining the risk assessment methodology	See section 3.1 on methodology requirements.
Defining risk criteria	This includes defining the criteria for evaluating risk, and covers: • the nature and types of causes and consequences that can occur and how they will be measured • how likelihood will be defined • the timeframe(s) of the likelihood and/or consequence(s) • how the level of risk is to be determined • the views of stakeholders • the level at which risk becomes acceptable or tolerable, and • whether combinations of multiple risks should be taken

	into account and, if so, how and which combinations should be considered.

5. Identifying, assessing and evaluating the risks

In order to adequately assess and evaluate the risks to Australian Government information agencies should refer to the Australian Government's Cyber Security Operations Centre *Cloud Computing Security Considerations* document. Annex B references other important considerations in support of agencies' risk assessments.

5.1 How to identify potential risks

Agencies are to identify risks to the confidentiality, availability and integrity of Government information subject to outsourced or offshore arrangements relevant to the classification of the information. The risk identification process should be broad and comprehensive, as the risks identified will form the basis of the assessment process.

Understanding the nature of the relevant or potential threat, criticality and vulnerabilities is an essential component of this. One way to do this would be to consider the questions below:

- How could the integrity of Government information be affected? What would be the impact of loss of confidence in the integrity of your information? For example, the integrity of the Hansard record.
- How could an unintended disclosure of Government information occur in an outsourced or offshore arrangement? What are the sources of risk? What threats are there?
- What would the impact of an unintended disclosure be for the various classes of information?
- Why could an unintended disclosure occur? What is the cause (actions, incidents or factors) behind the source of risk? Are there any measures in place that limit or encourage sources of risk?
- What would an unintended disclosure look like? What would an event or incident look like?
- Where would this happen? Based on arrangements, would this happen in Australia? If offshore, what countries could the information be stored or processed through?
- When could an unintended disclosure happen? What is the length of the proposed arrangement? What is the time period that risks need to be considered over?
- Who would be involved in an unintended disclosure? Who is the threat source? Who will be involved in a response? Who would be impacted? Does this include the Australian public or is it limited to Government?

When searching for information to inform the risk identification process, agencies should take into account individual agency security plans, as this is a ready source of information on risks to agency information.

For additional information on different ways to identify risks, see Chapter 4 of HB 167:2006 *Security Risk Management*, and to assist in determining impact see the PSPF *Business Impact Levels*.

5.1.1 Potential risks to consider

Below are some suggested risks for consideration. Agencies should not limit their consideration exclusively to this list.

The Government's ability to effectively manage and control its information in an outsourced or offshore arrangement can potentially be put at risk from any of the following:

- compromise of the integrity of the information which impacts on business functioning
- unavailability of the information which impacts on business functioning
- unauthorised access by a third party
- unauthorised access by the service provider's other customers
- unauthorised access by rogue service provider employees, or
- inadequate resilience and security measures applied to the associated physical infrastructure, supply chain and ICT networks.

In addition to the risks associated with outsourcing arrangements, entering into an agreement with an offshore component can cause additional complications due to:

- the nature of the legal powers to access or restrict data
- the lack of transparency (and reduced ability to directly monitor operations),
- the prevailing culture of some countries, or
- complications arising from data being simultaneously subject to multiple legal jurisdictions.

5.1.1.1 The nature of legal powers to access or restrict data

Like Australia, most foreign jurisdictions have legislation legal powers that allow access to communications and stored information for the purposes of law enforcement and national security. In some cases these laws allow law enforcement and national security agencies to access information held overseas or in Australia.

5.1.1.2 The lack of transparency

Should agencies enter into arrangements where information is held offshore, there is the potential for that information to be stored or processed in jurisdictions where Government information access mechanisms operate without transparency or outside of established legal frameworks. Alternatively, the lack of effective rule of law may fail to deter attempts by non-state actors to misappropriate information.

5.1.1.3 The prevailing culture of some countries

The prevailing culture of some countries may give rise to additional risks. For example, the tolerance (legal and/or law enforcement effectiveness) and acceptance of corruption and white collar crime differs across countries and may impact on an agency's ability to ensure the confidentiality, availability and integrity of the Government's information. Similarly, extrajudicial behaviour of government agencies, and the ability of citizens to refuse those demands may be limited, potentially giving rise to further risks that need to be considered.

5.1.1.4 Complications arising from data being simultaneously subject to multiple legal jurisdictions

Complications may arise from information being subject to the laws of multiple jurisdictions. This may occur in circumstances where:

- foreign laws apply to a vendor because it is located offshore
- foreign laws have an extra territorial application to vendor located in Australia, or

- the services provided by the vendor pass through a foreign jurisdiction.

5.2 How to assess risk

Having identified a range of relevant risks, the risk assessment process should determine the level of risk by considering the potential consequences, and the likelihood of it occurring, and the acceptable levels of tolerance. The sources of risk events, and the effectiveness of existing controls to prevent or reduce the consequences of risk events should be considered in assessing the likelihood and consequence levels. This includes the level of oversight and control agencies have on the management of their information.

For additional information on assessing risks, see Chapter 5 of HB 167:2006 *Security Risk Management*.

5.2.1 Guidance on determining potential consequences

The consequence of unintended disclosure of government information will depend on the profile of that information. The majority of government information is neither publicly available nor security classified. This includes information that is unclassified, but potentially sensitive, such as Medicare client and taxpayer records; details of business dealings with Government; correspondence between citizens and Ministers; and public service employee records.

Unintended disclosure or compromise of Government information could, for example, affect the:

- Government's capacity to make decisions or operate
- privacy and integrity of personal information about Australian citizens
- the safety of persons
- public's confidence in Government
- market stability and commercial interests
- the competitive process, and
- compliance with legislation.

Agencies may wish to apply the *Australian Government Protective security governance guidelines – Business impact levels* when determining the consequences of compromise of agency information in outsourced or offshore arrangements.

5.2.2 Guidance on determining likelihood

The likelihood is the chance or probability of an event or incident occurring resulting in the unintended disclosure of Government information. When considering the likelihood, agencies should consider the timeframe in which the risk could potentially occur. Agencies may wish to represent likelihood on a pre-determined scale, for example, low, medium and high. Alternatively, it can be presented as a percentage.

5.3 Evaluating the risks

Evaluating the risks of unintended disclosure of Government information in outsourced or offshore arrangements involves considering the risks within the context of the agency risk tolerance and potential treatment options.

In some circumstances, the risk of unauthorised access or disclosure of Australian Government information can be quantified almost entirely in financial terms based on a loss of revenue. In these circumstances, determining the risk is a matter of financial calculation. However, in most circumstances, agencies will need to consider a wider range of factors, including the potential reputational cost of a disclosure due to a loss of citizens' or businesses' data. In these circumstances, calculating the risk is a more complex process and the acceptance of that risk is a responsibility of ministers.

There may be circumstances where the factors for consideration and judgments required are so complex that the risk of outsourcing or offshoring data is incalculable. If the risk is determined to be incalculable, it will not be possible to manage it and agency heads are not to enter into these arrangements.

For further information on evaluating risks, see Chapter 6 of HB 167:2006 *Security Risk Management*.

5.3.1 How to determine risk tolerance

Determining risk tolerance will be highly dependent on the organisational context of the agency and agency head. However, in most cases the concept can be understood as a gradient, where the risk may become increasingly less tolerable as the risk level is elevated (see Figure 4).

Agencies may also use their agency security plans as a source of information as the risk tolerance determined as part of that plan should be broadly consistent with risk assessments undertaken for outsourced or offshore arrangements.

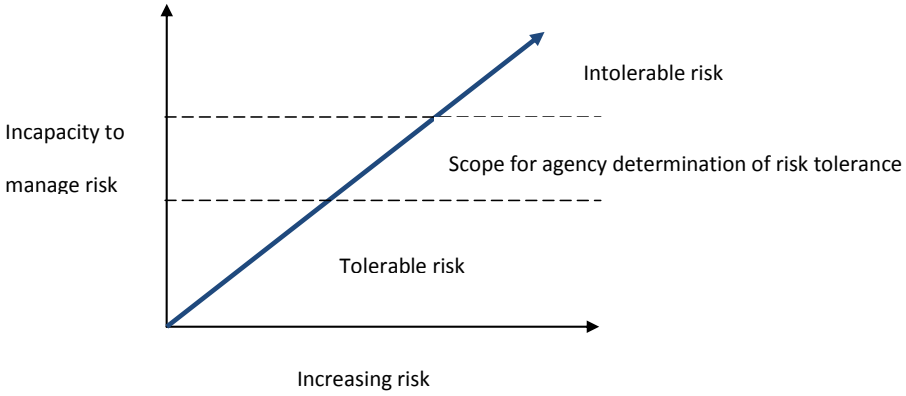

Figure 4: *Risk tolerance.*

5.3.2 How to consider potential risk treatment options

There is no such thing as absolute security. This means that efforts to treat risks will not remove them completely, but should aim to make the risk levels more tolerable.

Chapter 7 of HB 167:2006 *Security Risk Management* outlines strategies for risk treatment. This includes a six step process where agencies:

1. Prioritise intolerable risks.
2. Establish treatment options.
3. Identify and develop treatment options.
4. Evaluate treatment options.
5. Detailed design and review of chosen options, including the management of residual risks.
6. Communication and implementation.

5.3.3 Suggested treatment options

Contractual arrangements present a potential tool that agencies can use to mitigate risks associated with the outsourcing or offshoring of government information through:

- specifying the necessary protective security requirements in the terms and conditions of any contractual documentation (including sub-contractual arrangements), and
- verifying that the contracted service provider complies with the terms and conditions of any contractual documentation.

However, in some cases it may be impractical or impossible for the agency to verify if the service provider is adhering to the contract. This can be addressed through the use of third party audits, including certifications, but at an additional cost.

Other resources include the PSPF *Protective security governance guidelines – Security of outsourced services and functions* and ANAO *Better Practice Guide: Developing and Managing Contracts*.

6. Finalise the risk assessment

6.1 Requirements for entering into outsourced and offshore arrangements

6.1.1 Documenting the risk assessment and risk treatment

Agencies are to document that they have considered, calculated and accepted the associated security risks in outsourced or offshore arrangements.

6.1.2 Agency head approval

With the exception of unclassified information subject to the *Privacy Act 1988*, agency heads can enter into these arrangements following a documented risk assessment.

Agency heads should advise the Secretaries ICT Governance Board when they are considering or where they have entered into outsourced or offshore arrangements for the storage and processing of Australian Government information. The purpose of this measure is to support information sharing and inform potential whole-of-government ICT procurement arrangements.

6.1.3 Ministerial approval

Where there are risks to personal information, the potential impacts are broader than just financial considerations and include loss of public confidence and trust in Government. Where these risks are calculable and manageable, relevant Ministers are to accept those risks before an agency head can enter into such an arrangement.

Agency heads wanting personal information (as defined in the Privacy Act 1988) to be stored and processed in outsourced onshore public cloud or offshore arrangements, are to seek Ministerial approval (both the relevant agency's Minister and the Attorney-General as the Minister responsible for privacy and protective security).

7. Review of Policy and Guidelines

The Protective Security Policy Committee (PSPC) is responsible for the maintenance and regular review of these guidelines under the Protective Security Policy Framework. It is recommended that the guidelines be reviewed 12-24 months after their initial implementation.

The sponsoring agencies for the policy, the Attorney-General's Department, the Australian Government Information Management Office and the Department of Broadband, Communications and the Digital Economy, will review the policy jointly and make recommendations to PSPC. It is recommended that the policy be reviewed 12-24 months after initial implementation.

List of relevant documents

Attorney-General's Department [AGD website: www.protectivesecurity.gov.au]

1. Protective Security Policy Framework (PSPF) Information security management document suite

Defence Signals Directorate [DSD website] Note new name: Australian Signals Directorate

1. Information Security Manual (ISM)
2. Cloud Computing Security Considerations

Australian Government Information Management Office [AGIMO website]

1. Australian Government Cloud Computing Policy
2. A Guide to Implementing Cloud Services
3. Privacy and Cloud Computing for Australian Government Agencies
4. Negotiating the Cloud – Legal Issues in Cloud Computing Agreements
5. Financial Considerations for Government use of Cloud Computing
6. Community Cloud Governance – Better Practice Guide

Department of Broadband, Communications and the Digital Economy [DBCDE website]

1. National Cloud Computing Strategy

National Archives of Australia [NAA website]

1. Records Management in the Cloud