Australian Government

Information Security Management Guidelines

Risk management of outsourced ICT arrangements (including Cloud)

Approved August 2014
Amended April 2015

Version 1.1

Contact us

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

Commercial and Administrative 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 August 2014 Amended April 2015

Contents

Amendments

No.	Date	Location	Amendment
1.	April 2015	Throughout	Update links

1. Introduction

1.1 Purpose

1. The purpose of this document is to provide guidance to agencies when considering the storage and processing of Australian Government information in outsourced[1] ICT arrangements with particular focus on Cloud services.

1.2 Audience

2. This guideline is primarily intended for use by:
    - Agency Heads (or their delegate)
    - Australian Government employees or contractors
    - Agency Security Advisers, and
    - Information Technology Security Advisers (ITSA) and/or Chief information Officer (CIO) in support of their agency head and Minister.

1.3 Scope

3. These guidelines provide a security risk management approach to the confidentiality, integrity and availability of unclassified Australian Government information (including unclassified information subject to a DLM)[2] in outsourced arrangements, including Cloud services.
4. These guidelines do not address the controls for Australian Government security classified information. Guidance for the protection of security classified information can be found in the Australian Government Information security management protocol and the Information Security Manual (ISM).

1.4 Why these guidelines were developed

5. Australian Government agencies continue to consider new ICT arrangements for Australian Government information that maximises their agencies efficiency and effectiveness.
6. Managing the responsibility and accountability for key functions such as governance and control over data and IT operations and ensuring compliance with laws and regulations can represent a challenge for many agencies.
7. The indirect governance and control over data and IT infrastructure in outsourced ICT arrangements presents additional risks.
8. These guidelines provide a consistent and structured approach to assist agencies undertaking a risk assessment when considering outsourced ICT arrangements for Australian Government information.

1.5 Relationship to other documents

9. These guidelines support the Australian Government's *Protective Security Policy Framework* (PSPF), in particular the *Information security management core policy* and *Information*

[1] Outsourced - to procure services from a source outside the agency.
[2] For more information on the classification system refer to the *Australian Government information security management guidelines—Australian Government security classification system*

security management protocol, and the Australian Government *Australian Government information Security Manual* (ISM).

10. These guidelines are part of a suite of documents including:
    - the *Australian Government Cloud Computing Policy*
    - the Australian Signals Directorate's *Cloud Computing Security* guidance which assist agencies in meeting their information security mandatory requirements.
11. The management of outsourced ICT systems and facilities is also covered in the *Australian Government protective security governance guidelines—Security requirements of outsourced services and functions*, and *Australian Government physical security management guidelines—Physical security of ICT equipment, systems and facilities*. Annex A provides a list of some of the key relevant documents.

1.6 Use of specific terms in these guidelines

12. In these guidelines the terms:
    - 'are to' or 'is to'—are directions required to support compliance with the mandatory requirements of the physical security 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.

2. Applicable policy and legislation

2.1 Applicable policy

13. The Australian Government policy for security of information is promulgated through the PSPF and the ISM.

14. The PSPF and ISM policies, protocols and guidance when applied by agencies demonstrate to Government that they are effectively managing the risks associated with the confidentiality, integrity, availability and aggregation of their information. The application of the principles of the PSPF, and its associated protocols, supports business and operational continuity.

15. There are several mandatory requirements within the PSPF that directly relate to the handling of Australian Government information.

16. Specifically, the PSPF mandatory requirement GOV 6 requires agencies to adopt a risk management approach to cover all areas of protective security, including procurement and management of ICT. In addition, GOV 12 requires agencies to ensure that where contracted service providers are engaged they comply with the policies and protocols of the PSPF. Further policy direction is articulated in the personnel, information and physical security mandatory requirements[3].

17. Agencies can only achieve effective protective security if it is part of the agency's culture, practices and operational plans. Therefore agencies **should** build protective security into governance processes rather than implementing it as an afterthought.

18. Agencies **should** proactively identify, assess and manage the protective security risks associated with outsourced ICT arrangements throughout all stages of the procurement cycle.

19. Each Agency **is to** document that they have calculated and accepted the associated security risks to Australian government information in accordance with the PSPF, ISM before entering into outsourcing ICT arrangements.

20. Agency heads **should** not enter into outsourced ICT arrangements if the risks to Australian Government information cannot be quantified or are too complex to be calculated.

21. Agencies can outsource their ICT arrangements; however, responsibility for the risk remains with the Agency head.

2.2 Australian Privacy Law

22. The *Privacy Act 1988* (Cth) includes a set of 13 Australian Privacy Principles (APPs) that regulate the handling of personal information by Australian Government agencies and some private sector organisations[4].

23. Australian Government agencies and organisations handling information determined to be "personal" must do so in accordance with the principles of the APPs. For more information on the APPs and the applicable legislative requirements see http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform.

2.3 Privacy legislation

[3] For more information on the PSPF and its mandatory requirements visit – www.protectivesecurity.gov.au

[4] The APPs replace both the Information Privacy Principles (IPPs) that applied to Australian Government agencies and the National Privacy Principles (NPPs) that applied to some private sector organisations.

24. The following pieces of legislation are applicable to this policy:

- *Freedom of Information Act 1982* - http://www.comlaw.gov.au/Series/C2004A02562
- *Archives Act 1983* - http://www.comlaw.gov.au/Series/C2004A02796
- *Privacy Act 1988* - http://www.comlaw.gov.au/Series/C2004A03712

3. Outsourcing

25. Outsourcing ICT arrangements can offer a host of benefits, including scalability, elasticity, high performance, resilience and security together with cost efficiency. The range of technology options available through outsourcing of ICT is extensive.

26. It is important to recognise that any ICT arrangements delivered by the agency have a range of risks that an agency is responsible for identifying, assessing and managing. Outsourcing of agencies ICT arrangements can in some circumstances reduce the overall risk associated with delivering these services in house.

27. However, contracting an outsourced provider for the storage and handling of Australian Government information introduces new risks that must be considered and assessed before a decision is made to engage a provider. The physical location of stored information also represents a series of new risks and vulnerabilities.

3.1 Offshore ICT arrangements

28. Entering into an ICT arrangement in which information is held offshore[5], either by the contractor or subcontractor, can have additional risks. For example, while the term 'Cloud' implies that the information is 'not fixed'; all information stored in a Cloud service is physically located somewhere in a data centre or multiple data centres. Below is a list of factors that **should** be considered prior to entering into an offshore ICT arrangement.

    - the nature of the legal powers to access or restrict access to data
    - complications arising from data being simultaneously subject to multiple legal jurisdictions
    - the lack of transparency (and reduced ability to directly monitor operations), and
    - the difference in the business and legal cultures in other nations.

3.2 The nature of legal powers to access or restrict data

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

30. Agencies **should** seek legal advice as to the applicability of foreign legislative legal powers prior to outsourcing their information.

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

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

    - foreign laws apply to a vendor because it is located offshore, sometimes in multiple locations.
    - foreign laws have an extra-territorial application to a vendor located in Australia, or
    - the services provided by the vendor pass through a foreign jurisdiction.

[5] These are arrangements in which the information is stored or processed in equipment that is located outside of Australia.

3.4 The lack of transparency

32. In addition to managing the risks associated with other countries lawful access to Australian Government information (as discussed above), agencies also need to consider the risk posed to their information by other Governments (for example, foreign intelligence services) that may operate without transparency or outside of established legal frameworks.

3.5 The difference in the business and legal cultures in other nations

33. The difference in the business and legal cultures in other economies 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 affect an agency's ability to ensure the confidentiality, availability and integrity of Australian Government information. Similarly, extrajudicial behaviour of foreign government agencies, and the ability of citizens to refuse those demands may be limited, potentially giving rise to further risks that **should** be considered.

34. The lack of effective rule of law may encourage attempts by non-state actors (including organised crime) to misappropriate information.

3.6 Cloud

35. Cloud computing is a new way of delivering computing services that can be efficient and effective. Such services can be available on-demand. These services range from storage and processing, to software such as email handling. With a resources constrained environment influencing senior decision-making processes, this new economic model for information handling and computing can be highly attractive.

36. Although shifting to Cloud technologies can be a more affordable and faster alternative to existing ICT solutions, doing so without the proper consideration could undermine an agency's security policies, processes and practices.

37. In the absence of international, Australian or industry standards, there is a greater responsibility on agencies to undertake due diligence[6].

38. Consequently, understanding cloud computing delivery models is crucial before migration to such a service is considered. To help consumers understand cloud services the US National Institute of Standards and Technology (NIST) has defined the range of Service Models (Software as a Service, Platform as a Service, Infrastructure as a Service) and Deployment Models (Private cloud, Community cloud, Public cloud and Hybrid cloud) in cloud computing.

39. In recognition of the Service and Deployment Models, agencies entering into cloud service arrangements typically do so with multiple service providers to deliver the desired ICT arrangement. Consequently, the risk associated with each of these vendors needs to be considered independently and holistically.

[6] AGD notes that Standards relating to Cloud services are currently being developed.

4. Overview of risk management for outsourced ICT arrangements (including Cloud).

4.1 Risk assessment framework

40. These guidelines set out a risk assessment process based on existing frameworks defined in Australian Standards AS/NZS ISO 31000:2009 *Risk Management – Principles and guidelines* and HB 167:2006 *Security Risk Management*. Risk assessment is a subjective process and agencies **should** ensure that the process is transparent, justifiable and documented. *Figure 1* provides an overview of the process and the corresponding guidance.

41. Each agency will have different business requirements and operating environments and is best placed to:

    - identify its level of risk tolerance
    - identify specific risks to its people, information and assets, and
    - identify appropriate protections to mitigate identified risks.

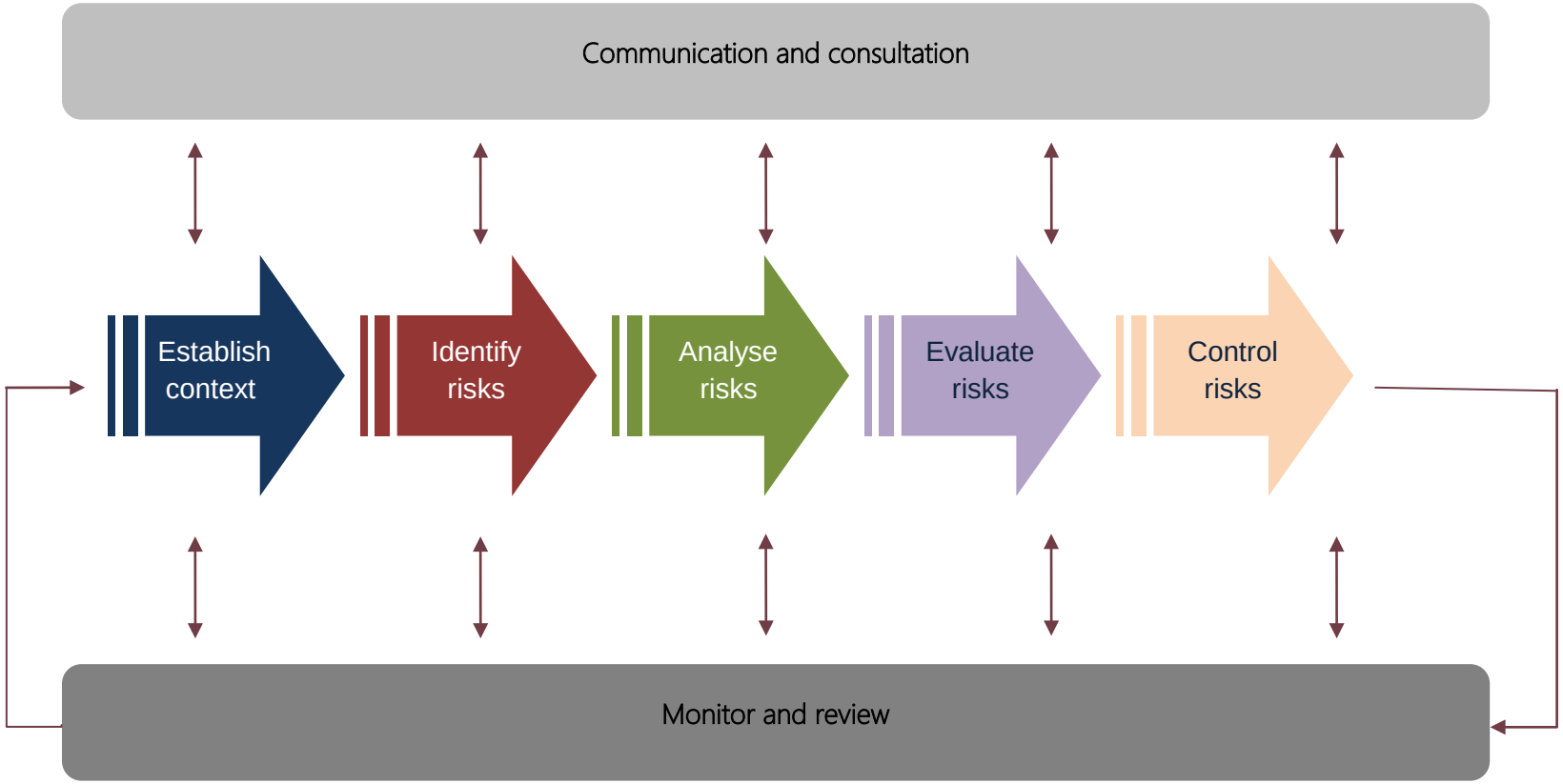
4.2 Applying AS/NZS ISO 31000

42. The risk assessment process **should** be consistent with existing standards. There are five keys steps that agencies **should** undertake as part of a risk assessment.

    - *Establish the Context* – defining the internal and external influences that have direct or indirect impact on the implementation of the arrangement.
    - *Identify Risks* – develop a robust list of risks that could affect the successful implementation of this arrangement.
    - *Assess the Risks* – analyse the list of risks against the organisations tolerances, the likelihood and impact.
    - *Select treatments* – choose appropriate risk mitigation strategies and controls for the identified risks.
    - *Develop overall risk assessment* – summarise the result of each risk with its associated mitigation or control into an overall category of risk.

For further information on using a Risk Assessment framework, see AS/NZS ISO 31000:2009 and HB 167:2006

Figure 1 Risk Assessment Process



4.3 Establish the context

43. An agency's risk assessment process **should** address the strategic, organisational and security risk management contexts. Security risk management is applicable across all facets of an organisation's functions, or activities. In particular the risk assessment needs to be appropriate to the prevailing and emerging risk environment. Establishing the context is critical as it sets the basis on which all subsequent risk assessment activities are conducted.

4.4 How to determine your organisational context

44. 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.

4.5 The strategic context of outsourcing

45. Agencies **should** consider what aspects of strategic context are relevant to their situation, and factor these into their risk assessment process. These can include, but are not limited to:

    - relevant Australian legislation, regulation and policy, including responsibility for safeguarding Australian Government information as part of the PSPF
    - foreign laws and potential jurisdictional access to information, and
    - the potential benefits of outsourcing or offshoring arrangements.[7]

4.6 Identifying risk

46. This step is used to comprehensively determine all applicable sources of risk and potential events that could impact government or agency business.

47. Each risk **should** be described in as full a manner as possible, so that decision makers can fully understand the situation. Agencies **should** identify risks to the confidentiality, availability and integrity of Government information subject to their ICT arrangements.

48. AS/NZS 4360:2004 defines risk as:

    "The chance of something happening that will have an impact on the objectives".

[7] The Australian Government Information Management Office's *Cloud Computing Strategic Directions* paper provides advice on the potential benefits of cloud computing.

4.7 How to determine agency risk tolerance

49. The criteria for determining an agency's risk tolerance **should** be done during the 'Establishing the context' phase of the risk assessment process.

50. Determining risk tolerance will be highly dependent on the organisational context of the agency and agency head. The level of tolerance for risk is the sum of the agency's risk appetite. The agency's risk tolerance is based on the principle of managing risk to a level that is as low as reasonably practicable, while still allowing scope for flexible and innovative business practices.

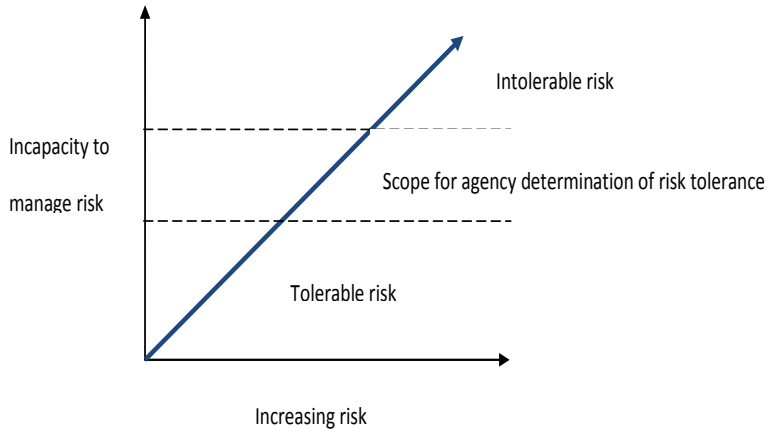
51. An agency's tolerance can be affected by certain changing evaluation criteria. Therefore, an agency head's appetite for risk can vary depending upon:

    - prevailing political and community sensitivities and expectations
    - the nature of the security incident (e.g. terrorist act, hacking)
    - existing or emerging security incidents trends (trusted insider, cyber-attacks)
    - strategic or business priorities
    - resource availability for treatment, and
    - the ability of the Government, agency or individual to absorb losses.

52. In most cases determining an agency risk tolerance can be understood as a gradient, where the risk may become progressively less tolerable as the risk level is increased (see Figure 4).

53. 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*



4.8 Questions to consider when determining risks within a Cloud context

54. Understanding the nature of the relevant or potential threat, criticality and vulnerabilities is an essential component of establishing context in a risk management process. Below are a series of considerations and questions that can facilitate this process[8]:

    - How could the confidentiality, integrity and availability of Australian Government information be affected?
    - What is the aggregated value[9] of the information holdings to the agency?
    - What would an unintended disclosure look like? What would an event or incident look like?
    - 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 Australian Government information occur in an outsourced or offshore arrangement? What are the sources of risk? What threats are there?

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

56. For additional information on different ways to identify risks, see Australian Standard HB 167:2006 *Security Risk Management* Chapter 4, and to assist in determining impact see the PSPF – *Australian Government protective security governance guidelines—Business Impact Levels* (BILs).

4.9 Potential threats when outsourcing information

57. Below are the top nine threats to Cloud service as identified by the Cloud Security Alliance's *The Notorious Nine: Cloud Computing Top Threats in 2013.* Agencies **should** not limit their consideration exclusively to this list, but use this list to inform their assessment of the use of outsourcing or offshoring information.

    - **Data Breaches** – sensitive internal data is stolen, leaked or accessed by external unauthorised entities.
    - **Data Loss** – the permanent loss or deletion of data by accident or malicious activity.
    - **Account or Service Traffic Hijacking** – external entities eavesdropping on your activities, transactions, manipulating data, return falsified information, through phishing, fraud and exploitation of software vulnerabilities still achieve results.
    - **Insecure Interfaces and Application Programming Interface (API)** – vulnerable interfaces can be exploited both accidentally and maliciously in an attempt to circumvent security process.
    - **Denial of service (DoS)** - DoS attacks can prevent users from accessing their data or applications, while forcing the victim to consume inordinate amounts of finite system resources.

[8] The Australian Signals Directorate's *Cloud Computing Security* guidance provides additional considerations that should be assessed prior to engaging cloud services.

[9] Agencies should use the BILs to determine the aggregated value of their information.

- **Malicious Insider** – a current or former employee, contractor or other business partner who has or had authorised access to an organisation's network, system, or data and intentionally exceeded or misused that access in a manner that negatively impacts the organisation's information systems.
- **Abuse of Cloud Services** – this threat is more an issue for Cloud service providers, but Cloud services can facilitate malicious agendas through the exploitation of Cloud infrastructure.
- **Insufficient Due Diligence** –entering into ICT arrangements with Cloud services providers without effectively understanding the full scope of the undertaking, its weakness and vulnerabilities.
- **Shared Technology Vulnerabilities** - Cloud infrastructure (CPU caches, GPU, etc) that is not designed to offer a multi-tenant architecture is vulnerable to scalable sharing practices. This vulnerability is dangerous because it can affect an entire Cloud at once.

58. The Australian Government's ability to effectively manage and control its information in an outsourced or offshore arrangement is limited. Qualified assurances and controls provided by the vendor **are to** align with agency risk profiles to ensure that Australian Government information is managed securely.
59. Due to the evolving nature of technology the threat environment is constantly changing. As a result, there is a need for ongoing oversight and management of the threat environment and its potential impact and consequences[10].

4.10 Mapping risks

60. To fully understand the potential of the risks identified, agencies **should** develop a clear understanding of the vulnerabilities that are apparent from each risk event. This is essential to gauge the consequence and likelihood of these risk events to inform the risk assessment. This process will also help in the prioritisation of the identified risks, and guide the allocation of resources in mitigating their impacts.
61. Agencies **should** consider the following for each identified risk:
    - What is the likely outcome of the risk eventuating?
    - When and how frequently can the risk happen?
    - Where is risk the likely to impact?
    - Who could be impacted by the occurrence of the risk event?
    - Who are the stakeholders of the risk event? What is the impact to them?
    - What catalysts could lead to the risk event?
    - How can eventuality of the risk be mitigated?
    - How can the consequences of the risk event be mitigated?
    - How reliable is the information that this risk assessment is being based upon?

4.11 Assessing risk

62. Once the range of relevant risks has been identified, the risk assessment process **should** determine the level of risk. To achieve this, the potential consequences of the risk event, the

[10] For further information see - http://www.asd.gov.au/infosec/cloudsecurity.htm

likelihood of it occurring, and the acceptable levels of tolerance **should** be evaluated holistically.

63. 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.

    - As an example, all Australian Government information **should** be assessed in relation to Confidentiality, Integrity and Availability, including aggregation. For each of these areas, risks events must be assessed against the potential of their impact for-Whole of Government, their Department/Agency, and their customer. The chance of the risk event occurring and whether there are extant controls or measures in place to reduce the effects of the event needs to also be considered.

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

4.12 Guidance on determining potential consequences

65. The consequence of unintended disclosure of Australian 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. For example – unintended disclosure or compromise of Australian Government information could 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.

4.13 Guidance on determining likelihood

66. The likelihood is the chance or probability of an event or incident occurring resulting in the unintended disclosure or compromise of Australian 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.

4.14 Guidance on rating risk

67. Determining the risk rating is the sum of combining the defined likelihood and consequence estimations. The risk rating **should** be between the level of "Extreme" and "Low". While initial estimations of likelihood and consequence can present risks identified as "extreme" or "low", the overall risk rating **should** be the sum of all identified risks calculated together. It is appropriate, when rating risk to use the 'most credible' scenario to determine the overall

level. Agencies may wish to apply the *Australian Government Protective security governance guidelines – Business impact levels* when determining its risk rating.

LIKELIHOOD	CONSEQUENCES				
	Insignificant	Negligible	Moderate	Major	Extreme
Remote	VERY LOW	VERY LOW	LOW	MEDIUM	HIGH
Unlikely	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
Possible	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
Likely	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
Almost certain	LOW	LOW	MEDIUM	HIGH	VERY HIGH

4.15 Evaluating the risks

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

69. 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 **should** 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 resides with the agency head.

70. 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 **should not** enter into these arrangements.

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

4.16 How to consider potential risk treatment options

71. Security is not absolute. Efforts to treat risks will not remove them completely, but **should** aim to make the risk levels more tolerable.

72. When selecting risk treatments the allocation of resources **should** be conducted proportionally to the determined risks rating level.

73. Australian Standard HB 167:2006 *Security Risk Management* Chapter 7 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.

4.17 Outsourced treatment options

74. Contractual arrangements present a potential tool that agencies can use to mitigate risks associated with the outsourcing Australian 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.
75. 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[11].

Other resources include the PSPF *Protective security governance guidelines – Security of outsourced services and functions* and ANAO *Better Practice Guide: Developing and Managing Contracts: Getting the right outcome, achieving value for money*.

[11] For further information on certification see - http://www.asd.gov.au/infosec/irap.htm

4.18 Communication and consultation

76. A communication and consultation plan **should** be established at an early stage of the risk assessment to determine how the process will be communicated to key internal and external stakeholders.

77. Effective communication and consultation throughout the risk assessment process will ensure that those responsible for implementing risk management and those with a stake in the process understand the basis on which risk management decisions are made.

78. The provision of ongoing security implications and better practice can be integrated into agency's security awareness training, in accordance with GOV-1. Regular training and communication of the risks associated with the use of outsourced ICT arrangements will contribute to an effective security culture.

79. It is the responsibility of the agency conducting the risk assessment to communicate any identified risks that could potentially impact upon the business of other government agencies, particularly, if the risks have any national security implications.

80. Where the information has multiple government stakeholders, the relevant risks and associated treatments **should** be communicated to inform those agencies of the likely impacts. Stakeholders' perceptions of risk will vary in accordance with their different assumptions and needs. It is important that these different perceptions are appropriately factored into the risk assessment process.

4.19 Risk monitoring and review

81. For risk management processes and practices to remain relevant and effective they must be adaptable to, and evolve with, changes in the agency's internal and external environment, methods of operation and stakeholders' perceptions and actions.

82. Key questions to ask when monitoring and reviewing risk may include:

    - Are the controls (and their respective implementation strategies) effective in minimising the risks? (e.g. Is tokenisation [12]reducing the risk of disclosure?)
    - How might improvements be made and measured? (e.g. does the Cloud vendor have a continuous improvement program?)
    - Are the controls comparatively efficient/cost effective? (e.g. can the risk be reduced through other means?)
    - Are the assumptions you made about the internal and external environment, technology and resources still valid? (e.g. is there, or is there likely to be a better solution available in the near future?)
    - Do your controls comply with legal requirements, Government and agency policies, including access, equity, ethics and accountability? (e.g. does the Cloud solution meet the legislative requirements of Australia?)

[12] Tokenization is the replacement of sensitive data with a unique identifier that cannot be mathematically reversed.

5. Finalise the risk assessment

5.1 Documenting the risk assessment and risk treatment

83. Agencies **are to** document that they have considered, calculated and accepted (or not) the associated security risks in potential outsourced or offshore arrangements.

5.2 Approval process

84. Agency head or delegates **are to** consider the risk assessment before entering into an outsourced ICT arrangement. Agency heads are ultimately responsible for managing risk within their agency, and their understanding and acceptance of any risk manifested through outsourced ICT arrangements, including Cloud.

6. List of relevant documents

6.1 Australian Government resources

Attorney-General's Department – www.protectivesecurity.gov.au

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

Australian Signals Directorate (formerly Defence Signals Directorate) - http://www.asd.gov.au/

1. Information Security Manual (ISM)
2. Cloud Computing Security Considerations
3. Top 35 Mitigation Strategies

Australian Government Information Management Office - http://www.finance.gov.au/policy-guides-procurement/Cloud/

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 Communications - http://www.communications.gov.au/digital_economy/Cloud_computing

National Archives of Australia - http://www.naa.gov.au/records-management/publications/Cloud-checklist.aspx

6.2 Other resources

The Australian Government accepts no liability for the content on external third party web sites that contain additional information:

1. US National Institute of Standards and Technology - Cloud Computing
2. European Network and Information Security Agency - Cloud Computing Risk Assessment and Security and Resilience in Governmental Clouds
3. Cloud Security Alliance - Security Guidance, Top Threats to Cloud Computing and Governance, Risk Management and Compliance Stack

4. Appendices

8.1 Risk assessment process

Task	Outputs
1. Establishing the context	▪ Identification of objectives and key stakeholders ▪ Assessment of the ability of the work area to achieve its objectives ▪ Identification of key factors influencing risks in the department.
2. Identifying the risks	▪ A list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.
3. Analysing the risks	▪ Analysis of the likelihood of a risk occurring and its potential impact.
4. Evaluating the risks	▪ Assessment of existing controls or management strategies for each risk. This will provide clarity about: o the timeframe for when the risk is likely to occur o what are the possible courses of action available to manage the risk o what pre-planning can be undertaken ahead of the risk occurring o whether it is worthwhile developing a contingency plan to manage the risk.
5. Controlling the risks	▪ Where necessary, identification of potential new controls for each risk ▪ Decision about how to control the risk (avoid, reduce or eliminate, transfer, or accept).
▪ **Communication and consultation** *takes place at all stages of the process*	▪ Communication with key internal and external stakeholders ▪ Factoring of stakeholder perceptions of risks and benefits into the risk management process.
▪ **Monitoring and review** *takes place at all stages of the process*	▪ Monitoring of factors that might warrant a change to the risk management strategy.
▪ **Documentation** *takes place at all stages of the process*	▪ Clear and comprehensive risk assessments in the risk register and action plan templates.

8.2 Risk Assessment Tool

Agency:

Criteria	Y/N	Comments
Risk – based approach (AS/NZ ISO 31000:2009 and HB 167:2006)		
1. Establish Context		
a. Defines the proposal		
b. Description of information stored/processed		
c. Subject to *Privacy Act 1988*		
d. Protective markings		
e. Information held in Onshore/Offshore arrangement		
f. Public/Private/ Community Cloud		
g. Identifies all stakeholders (Contractors, Sub-contractors)		
2. Identifies Risk to Confidentiality, Availability and Integrity		
a. Risk to Government		
b. Risk to Agencies/Department		
c. Risk to the User (What consent to store/use information)		
d. Risk to the Provider		
3. Risk Analysis		
a. Defined Consequences		

b. Defined Likelihood		
c. Defined Tolerance		
d. Identify risks with insufficient Information		
e. Risks associated with Privacy Act		
4. Risk Evaluation		
a. Determined level of risk		
b. Risk assessed with risk tolerances		
c. Integrated into Agencies security plan		
5. Risk Treatments		
a. Risk treatments selected		
b. Risk treatments assessed		
c. Risks level stated and accepted		
6. Monitoring and Review		
a. Mechanisms to review changes in risk		
b. Regular risk review process		
c. Monitoring process in place (Annual, Quarterly, Monthly reports from Service Provider)		