TISN

FOR CRITICAL INFRASTRUCTURE
RESILIENCE

Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers)

June 2011

DISCLAIMER: This document is intended as a general guide only. To the extent permitted by law, the Australian Government makes no representations or warranties of any kind, express or implied, about the accuracy or completeness of the material contained in the document. The reliability of any assessment or evaluation based on its content are matters for the independent judgement of users. Users should seek professional advice as to their specific risks and needs. The Australian Government accepts no responsibility for the consequences of any use of this document.

This Page is Intentionally Blank

Foreword

Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers) (The Guide) provides Australian critical infrastructure providers with a resource to assist with the potential information security issues when considering the outsourcing of services or assessing the IT arrangements contained in existing outsourcing contracts.

The Department of Broadband, Communications and the Digital Economy (DBCDE) on behalf of the IT Security Expert Advisory Group (ITSEAG) of the Trusted Information Sharing Network (TISN) has prepared this guide.

This guide builds upon the previous guide, published by DBCDE in 2007, relevant standards and guidance as well as referencing information contained within the Centre for the Protection of National Infrastructure's (UK) document entitled, *'Outsourcing: Security Governance Framework for IT Managed Service Provision (Version 2, 2009)'*[1].

In preparing this updated version of the Guide in 2011, a range of drafting principles were used to inform its structure and content. These principles included:

- Broadening the intended audience of the guide to a wider CXO community rather than focussing solely on the CIO;
- Including a consideration of specific information security issues that may be faced with the use of cloud computing;
- Ensuring the language in the Guide is non-technical in its nature;
- Complementing established information security standards and frameworks; and
- Avoiding the provision of legal advice specific to a particular organisation's IT outsourcing arrangements.

DBCDE would like to thank the UK Government for allowing the Australian Government to reference their published guidance on this resource. DBCDE would also like to acknowledge the active involvement of the ITSEAG members throughout the preparation of the Guide.

A supplementary Executive Overview of this document is also available on the TISN website for download.[2].

ITSEAG Secretariat
Communications Critical Infrastructure Resilience
Department of Broadband, Communications and the Digital Economy
Email: itseag@dbcde.gov.au
Web: www.dbcde.gov.au and www.tisn.gov.au

[1] Available at *www.cpni.gov.uk/Products/guidelines.aspx*

[2] Available at *www.tisn.gov.au*

1. Executive Summary

Risk comes from not knowing what you are doing.

......Warren Buffet

Outsourcing of IT services can provide an organisation the opportunity to realise valuable strategic and economic benefits. However, for critical infrastructure providers, prior to the commencement of any outsourcing arrangement, the careful consideration of risks and threats, the structure of contractual arrangements, and compliance obligations must take place.

For a critical infrastructure provider, the design and implementation of sound information security principles and practices should be of paramount importance and integrated throughout each and every business process.

The failure to adequately consider the range of information security risks and threats that could compromise the integrity, availability and performance of the services provided through an outsourcing arrangement may result in:

- The lack of compliance to legislative obligations, carried at both the corporate and executive levels of the organisation, resulting in exposures to potential litigation;
- The inability to provide critical services to the community leading to potential national security exposures; and
- Costly remediation activities to rectify the service provision in the event of an information security incident.

Services may be outsourced but risks and regulatory compliance remain the responsibility of the Critical Service Provider

Further to these potential exposures, it is important for critical infrastructure providers to understand that whilst the establishment of an outsourcing arrangement may transfer the delivery of a business function to a third party - the ultimate responsibility for the design and implementation of information security policies, regulatory compliance, and control execution remains with the critical infrastructure provider.

This guide covers a wide range of potential information security issues that a critical infrastructure provider should consider in an outsourcing environment. The Guide is intended to provoke dialogue within an organisation’s executive to firstly assess whether a service could be suitable for outsourcing, and if so, what are the first principles relating to information security that should be considered.

The structure of the Guide covers eight (8) information security management elements that occur throughout the outsourcing lifecycle, namely:

- Information security governance;
- Roles and Responsibilities;
- Risk Management and Assessment;
- Change Management;
- Assurance and Conformance;
- Managing information security throughout the outsourcing arrangement;
- Incident Management; and
- Termination and Transition.

The Guide also briefly discusses cloud computing (the cloud) as a particular outsourcing variant, providing some insights into the differences from traditional outsourcing arrangements and some of the specific information security exposures that should be considered by a critical infrastructure provider, including:

- Compliance with jurisdictional legislation beyond that of Australian Federal, State and Territory Governments;
- Managing the confidentiality of information in an environment that may provide services to a large number of different customers;
- Gaining assurance over the effectiveness of information security controls in the cloud; and

  Ensuring the security posture of the cloud provider is aligned to the Critical Service Provider.

Outsourcing services to a cloud-based provider doesn’t change the security principles; it just changes the complexity of maintaining effective information security.

Whilst this guide is not intended to be a comprehensive “how-to” manual, for the design and implementation of information security within an outsourcing environment, a number of useful tools and references have been included in the appendices that may provide further insights for an executive team, wishing to gain a deeper understanding of this important topic.

2. Definitions

Outsourcing

An organisation's chosen ICT sourcing mechanism determines how an organisation's ICT components are obtained, managed and operated. The basic objective of ICT sourcing functions is to deliver the best level of support for the organisation's business requirements in the most cost-effective way.[3]

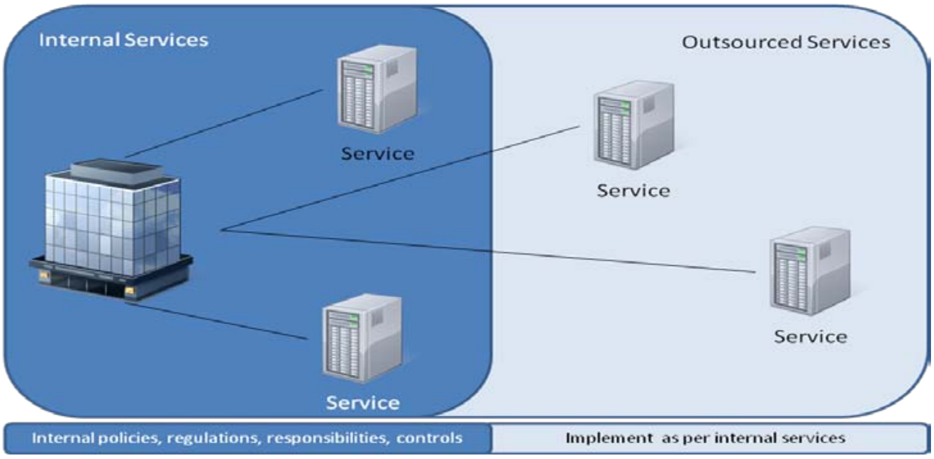
Drivers for ICT sourcing may include cost savings, increased business flexibility, exploitation of new technologies and accessing specialist expertise as well as government directives.

Outsourcing as a sourcing option, refers to an arrangement by which a task (s) that would otherwise be performed by staff internal to the organisation is transferred to an external entity specialising in the management and delivery of the task (s).

As a result, outsourcing involves transferring or sharing management control of a business function, enabled by two-way information exchange, coordination, and trust between the outsourcer and the client.[4]

It is important to understand that responsibilities and controls must remain in place for services, whether internally managed or outsourced, particularly with regards to IT security.

Figure 1: Internal versus outsourced service responsibilities


Internal Services
Outsourced Services
Service
Service
Service
Service
Internal policies, regulations, responsibilities, controls
Implement as per internal services

As **Figure 1** shows, under an outsourcing arrangement, whilst the delivery of the service has been moved to a service provider from outside the organisation, the design, implementation and deployment of internal policies, regulatory elements, responsibilities and controls need to be mirrored across both organisations. If this consistency is not maintained across both organisations, the likelihood of the arrangements succeeding will be diminished as well as creating additional

[3] *A Guide to ICT Sourcing for Australian Government Agencies*, Department of Finance and Deregulation, Sept 2007, p 2

[4] *Secure Your Information – Information Security Principles for Enterprise Architecture: Report,* TISN, Sept 2007, p 52 http://www.tisn.gov.au/Pages/Publications.aspx

management overheads when trying to maintain effective information security controls.

As with all outsourcing arrangements, the nature of the information being managed by the third party provider should be carefully considered prior to embarking on an outsourcing arrangement. If the information under management is deemed to be of a sensitive nature, an organisation should strongly assess the suitability of outsourcing as a provision mechanism.

Information Security

Information security is the protection of information and information systems and encompasses all infrastructure that includes processes, systems, services, and technology. It relates to the security of any information that is stored, processed or transmitted in electronic or similar form.

IT security is a subset of information security and is concerned with the security of electronic systems, including computer, voice, and data networks[5].

Information security has the following objectives:

Confidentiality – Ensuring that information is accessible only to those with a legitimate requirement and authorised for such access;

Integrity - Safeguarding the accuracy and completeness of information and processing methods; and

Availability - Ensuring that authorised users have access to information and associated assets when required.[6]

Underpinning these objectives is a set of information security principles, outlined in the ITSEAG paper *Secure your Information: Information Security Principles for Enterprise Architecture*[7], as follows:

1. Information Security is Integral to Enterprise Security;
2. Information Security Impacts on the Entire Organisation;
3. Enterprise Risk Management defines Information Security Requirements;
4. Information Security Accountabilities should be Defined ad Acknowledged;
5. Information Security must consider Internal and External Stakeholders;
6. Information Security requires Understanding and Commitment; and
7. Information Security requires Continual Improvement.

[5] *IT Security Management Audit Report No. 23, Australian* National Audit Office, Dec 2005, p 21

[6] *Protective Security Policy Framework*, Australian Government Attorney-General’s Department, Jan 2011, p 24

[7] *Secure your Information: Information Security Principles for Enterprise Architecture*, Department of Broadband, Communications and the Digital Economy, Information Technology Security Expert Advisory Group, June 2007, Executive Summary

Cloud Computing

> The Australian Government definition of Cloud Computing is based on the US Government's National Institute of Standards and Technology (NIST) definition as 'an ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction'.

Cloud Computing as a business model for service provision is becoming more prevalent, driven by the potential for cost and time efficiencies. Cloud computing delivery models can be summarised as:

- Infrastructure as a Service (IaaS), which involves the vendor providing physical computer hardware including processing, memory, data storage and network connectivity;
- Platform as a Service (PaaS), which includes the vendor provisioning IaaS as well as operating systems and server applications; and
- Software as a Service (SaaS) which includes the vendor providing cloud hosted software applications.

Cloud computing is also categorised by a range of different deployment models that include:

- The **public cloud**, which is shared by multiple organisations and accessed through the public internet;
- The **private cloud**, where an organisation utilises a cloud that is provisioned by the vendor for its sole use and accessed through a private connectivity mechanism;
- A **community cloud**, which is generally used by like type organisations with a similar security and risk profile; and
- The **hybrid cloud**, which involves a combination of the other three deployment models.

Table 1: Key cloud computing characteristics and enablers

Cloud computing characteristics	Cloud computing enablers
• On-demand self-service	• Reliable, high-speed networks
• Broad network access	• Large, global-class infrastructures
• Resource pooling	• Virtualisation capabilities
• Rapid elasticity	• Commodity server hardware
• Measured service	• Open-source software
	• Adoption of Web 2.0 standards

Integral to cloud computing is the concept of leveraged infrastructure and the sharing of resources, allowing the delivery of services at a lower cost. However, pushing the business applications and corporate data beyond the perimeter of the corporate environment (and in many cases beyond geographic boundaries) can result in higher levels of complexity and risk when attempting to effectively manage security.

Whilst the trend for organisations to embrace and leverage new technologies and delivery platforms (including cloud computing) for their services is unlikely to slow down in the future, the importance ascribed by an organisation to effectively manage security needs to keep pace with this adoption. The use of emerging technologies by organisations may have an adverse effect on an organisation's security profile, increasing the risk complexity and threat landscape for an organisation.[8] When this changing landscape is coupled with the outsourcing of services to third-party providers, the complexity of managing security can be magnified, resulting in offsets to the savings driven by outsourcing through a requirement for higher security management costs.

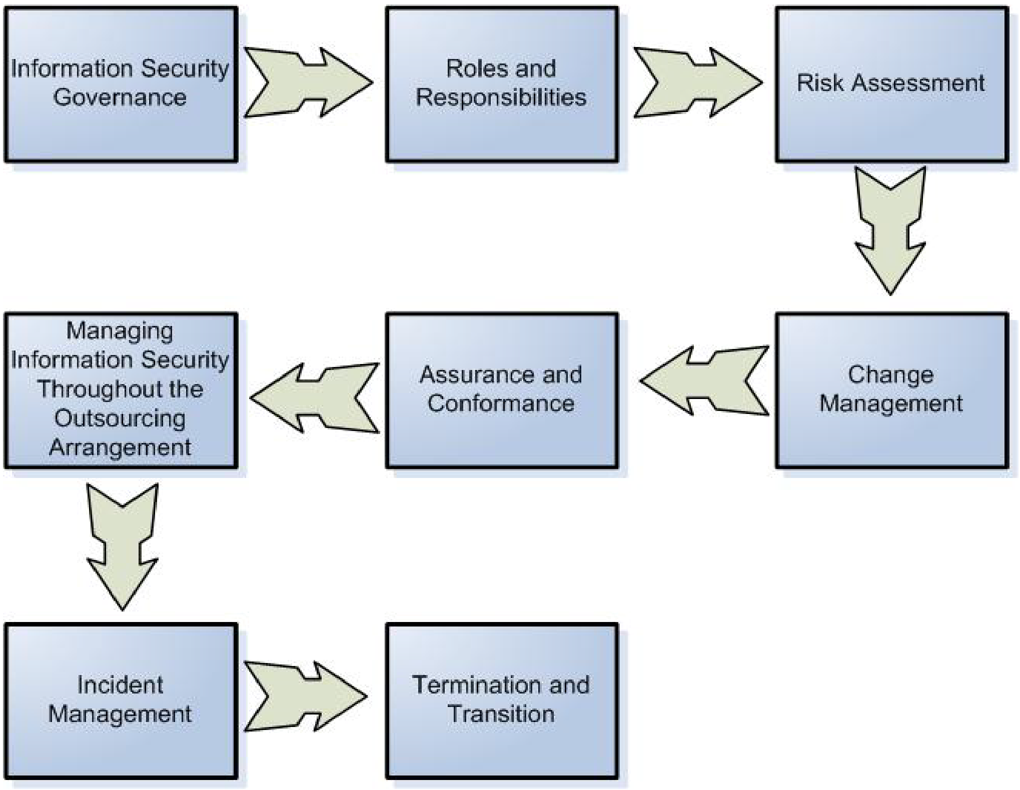
Throughout this guide's discussion of the information security management elements related to outsourcing, specific reference will be made to cloud computing in order to highlight any differences to a traditional outsourcing arrangement that a Critical Infrastructure Provider may need to consider.

[8] *Achieving IT Resilience – Advice for CIOs and CSOs*, Trusted Information Sharing Network, May 2010, p 3

3. Information Security Management Elements and Potential Issues for an Outsourcing Arrangement

This section provides an overview of each of eight information security management elements within the context of an organisation considering the initiation and management of an outsourcing arrangement. In order to promote a truly effective information security management approach, each of these elements requires the same priority and focus from an organisation.

Figure 2 Information security elements


Information Security Governance
Roles and Responsibilities
Risk Assessment
Change Management
Assurance and Conformance
Managing Information Security Throughout the Outsourcing Arrangement
Incident Management
Termination and Transition

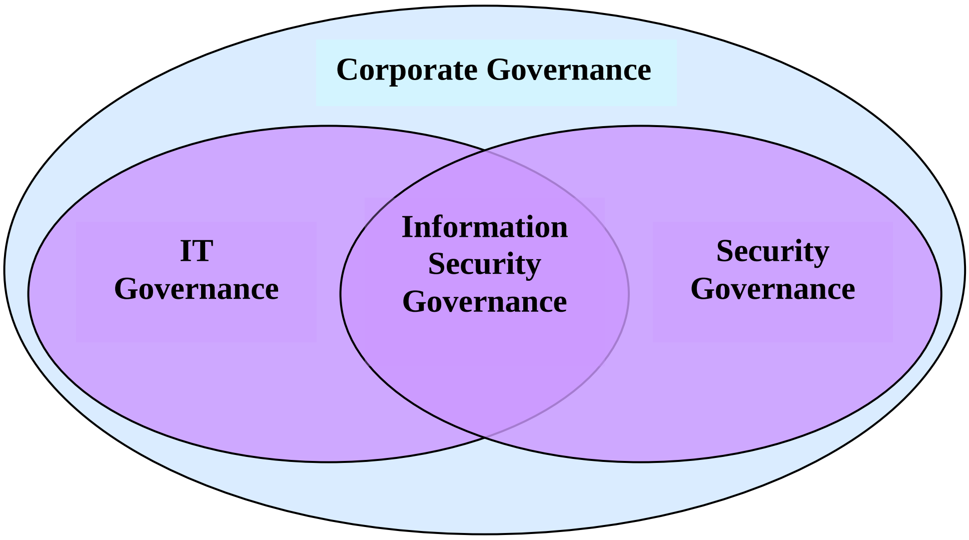
Information Security Governance

It is important for management to understand their role in planning, implementing and maintaining effective information security governance in organisations. Information security governance defines the security principles, accountabilities, and actions required by an organisation to achieve their identified security objectives. Underpinning effective information security governance is the governance of an organisation's Information Technology (IT) systems. IT systems are a core component of an organisation's operations and therefore the implementation of sound governance practices across these systems forms a key component of an organisation's corporate governance.[9]

[9] CIO, CISO and Practitioner Guidance, IT Security Governance, Department of Broadband, Communications and the Digital Economy, Revision 2 December 2009, provides further information and guidance relating to IT Security Governance

Information security governance should align to all other governing areas within an organisation, forming part of the overall corporate governance of an organisation.

Figure 3: Corporate, IT, Information and security governance relationships



In an outsourcing arrangement, information security must be comprehensively addressed at all stages, including prior to the arrangement being established, throughout the operation of the arrangement and during termination or transition. An incident caused by human error, systems failure, or malicious code/activity that compromises the integrity, availability or confidentiality of a critical infrastructure provider's information may result in negating any net benefits derived from an outsourcing arrangement. The consequences of such an incident may also result in widespread flow-on effects that may impact national security, the economy and, potentially, loss of life.

In conjunction with the establishment of sound information security governance principles in an outsourcing arrangement, it is also important for organisations to consider issues relating to Identity, Entitlement and Access (IdEA) management for both the end consumer and the service providers involved in the delivery of the outsourced service.[10]

Although an organisation may have sound internal information security governance systems in place, it is possible that these systems may not have been designed for an outsourcing arrangement where the roles and responsibilities are shared between the organisation and an external service provider.

[10] Further information on IdEA can be found within the Jericho Forum Commandments, www.opengroup.org/jericho/commandments_v1.1.pdf

Both the organisation and outsourcing provider’s information security governance policies should be consistent and complimentary, ensuring the effective mitigation of both the risks and threats that may impact the delivery of the service covered by the outsourcing arrangement.

The principles that determine information security governance under a cloud computing outsourcing arrangement are no different to a traditional outsourcing arrangement; however, the complexity of achieving effective information security governance may be magnified due to:

- The potential for data or business functionality to be replicated with additional vendors, other than the prime outsourcing provider;
- Compliance with jurisdictional legislation, if the cloud service operates beyond domestic boundaries;
- The hosting of data or business functionality on infrastructure shared by other organisations (potentially with different confidentiality, availability and integrity requirements);
- Lack of transparency across the platform hosting the data and business functionality; and
- The provider’s security posture differing from the critical infrastructure provider.

Roles and Responsibilities

In any outsourcing arrangement, the establishment of clear roles and responsibilities between an organisation's management and the outsourcing provider is essential. Underpinning the establishment of clear roles and responsibilities is the drafting and execution of clearly articulated contractual arrangements for the provision of the service.

Critical Infrastructure Providers should also be cognisant of the fact that many outsourced arrangements may rely on the use of sub-contractors for the delivery of components within the service-in-view. Where this is the case, contractual arrangements should ensure the prime outsourcing provider remains accountable and responsible for all actions undertaken by sub-contractors, and are responsible for managing information security governance across all sub-contractors, providing assurance to the organisation.

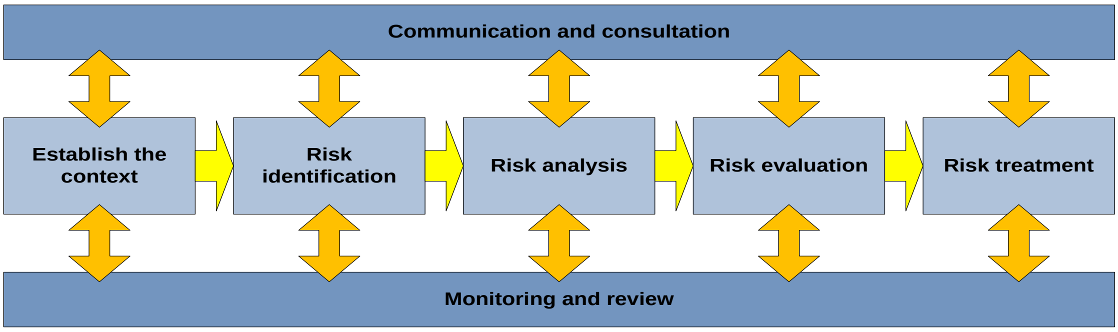
Further information relating to the definition of roles and responsibilities between an organisation and an outsourcing provider can be found in Appendix A.

Under a cloud based outsourcing arrangement, the establishment of clear roles and responsibilities may become more difficult for an organisation due to the potential for a greater number of cascading service providers to be involved in the provision of the service. However, regardless of the potential for greater complexity, the requirement to define clearly articulated roles and responsibilities is the same as within traditional outsourcing arrangements.

Risk Management and Assessment

Effective risk management processes and detailed risk assessments are pivotal to the success of an outsourcing arrangement. Information security risk can be closely tied to other business risks, such as reputational or financial and as such, the importance of gaining a clear understanding of the relationship between information security risk and an organisation's overall corporate risk assessment cannot be understated.

Figure 4: Risk management process



a) **Communication and consultation:** Underpins the entire information security risk management process, addressing issues related to the risk, ensuring that stakeholders are informed on the basis of decisions made relating to the risks.
b) **establish the context:** Articulation of the objectives to be taken into account when managing the risks, including setting the scope and risk criteria for the process.
c) **Risk identification:** Identification of the sources of IT security risks, areas of impact, events, and causes, and their potential consequences. Identification of risks should include those risks which are not under the control of the organisation.
d) **Risk analysis:** Includes an evaluation and decision of whether an identified risk must be addressed. Includes determination of likelihood, consequences, and the mitigation strategies required to effectively treat the risks.
e) **Risk evaluation:** Determine whether to address risks based on the outcome of the risk analysis process, the risk criteria established, and the wider context of risk within the organisation.
f) **Risk treatment:** Selection of options for treating risks, and the implementation of the options chosen to address the risks.
g) **Monitoring and Review**: Regular determination of the effectiveness of controls implemented against risks, detection of changes in the context, risk criteria, scope and the identification of improvements to better address risks.

Once an organisation has selected an appropriate risk management methodology, such as *AS/NZS ISO/IEC 31000*, a thorough assessment of information security risks should be undertaken prior to a decision to enter into an outsourcing arrangement. Forming part of this assessment should include a consideration by the organisation of the suitability of the data that will be managed throughout the arrangement. As an example, if the data has a security classification other than unclassified or, if the data is commercially important or critical in its nature, the outsourced provision of services maybe unacceptable based on the potential risks of data loss or access by unauthorised individuals.

A risk assessment is vital to ensure that the organisation understands its information security requirements, as well as ensuring outsourcing suppliers understand the risks they are expected and contracted to manage. Where a supplier utilises sub-contractors to perform some of the outsourced IT functions, the sub-contractors must be bound by the same risk management analysis as performed with the prime-provider.

It is also important to note that an organisation's risk landscape is rarely static and is highly likely to change over time. As a result of the fluidity that may underpin risk management, an organisation should re-assess their risk and associated mitigation strategy on a regular basis in order to ensure the risk landscape is accurate and up to date.

Once a risk assessment has been performed by an organisation and an appropriate outsourcing provider has been engaged, ensuring information security risks are effectively managed during the transition period requires the organisation and the outsourcing provider to jointly develop a security management transition plan, which should in turn, form part of the contract. The plan should have three phases:

- the transition of any applicable information security elements to the service provider – a joint responsibility;
- the implementation of an Information Security Management System (ISMS) which aligns to the risk assessment, compliance requirements, control specification and other contractual requirements – this is the service provider's responsibility; and
- a post-implementation assurance review in a form specified by the organisation, compatible with the security management approach – this is the organisation's responsibility.

Further detail relating to the design components within an ISMS can be found in the "*Managing Information Security during the Outsourcing Process*" section.

Risk management and assessment processes for a cloud based outsourcing arrangement does not differ from traditional outsourcing arrangements but some of the additional threats posed by such an arrangement that may need to be assessed, include:

- The geographical location of information and business functions and the resultant legislative requirements that may be applicable;
- The privacy and integrity of the data within the cloud;
- The transparency over security controls, knowing the location of the servers, and the ability to audit them for compliance to policies;
- The availability of the cloud service and business continuity provisions;
- The enforceability of service level agreements in the case of a service degradation or outage;
- The ability for a critical infrastructure provider to relocate or transfer services from one service provider to another;

- The outsourcing provider's security processes and policy alignment to the organisation's security posture; and the outsourcing provider's ability to segregate data and business functionality between customers.

Change Management

As was touched upon in the "*Risk Management and Assessment*" section, large and complex contracts may require changes over their course. These changes may relate to information security, either through changes in the scope, functionality or performance of the outsourced services, or because the security requirement itself has changed. A change management procedure should be contractually agreed between the organisation and the outsourcing provider for any changes to the service which may have a material effect on information security.

One procedure that may be considered to effectively manage change is the establishment of a formal Change Management Board with representation by qualified and experienced information security professionals from both the organisation and the service provider.

Processes should be contractually established for the ongoing management of the security relationship with the service provider, covering changes in:

- risk;
- security requirements (including control specifications);
- commissioning of, results of, and corrective actions from security performance and assurance reporting; and
- access control changes relating to security.

Change management processes are no different from in a cloud based outsourcing arrangement from a traditional based outsourcing arrangement. However it should be noted that whilst one of the major benefits from cloud computing is the use of a homogenous environment that drives down the provision cost, achieving flexibility and customisation of an environment can be extremely difficult and sometimes costly.

Importantly, under a traditional outsourcing arrangement, the outsourcing provider will generally take an organisation's existing business processes and deliver them as per the organisation's design. However, under a cloud based outsourcing arrangement the organisation generally has to re-engineer their business processes to suit the standard service provided by the cloud vendor. This may mean that if the cloud provider changes its business process, a significant impact on the organisation's business processes may occur.

Assurance and Conformance

A key component of effective information security management in an outsourcing environment is the ability of an organisation to gain assurance that risks have been managed, are being managed, and will continue to be managed.

As previously discussed in the "*Risk Management and Assessment*" section, outsourced arrangements often involve corporate risk in terms of overall business continuity, loss of reputation and/or regulatory non-compliance to the extent that organisations cannot wait for an incident to happen and then seek to claim damages for remediation.

Appendix B depicts a table that describes a range of tools and mechanisms available to Critical Infrastructure Providers for the management of assurance and conformance. These tools and mechanisms include:

- Regular information security management scorecards and reporting;
- Outsourcing provider commissioned information security audits;
- Critical infrastructure provider commissioned information security reviews;
- Standards certification (e.g. SAS70 and AS/ ISO 27001); and
- Letters of assurance.

Under a cloud based outsourcing arrangement, the ability to achieve adequate assurance over information security controls and processes can be difficult due to the nature of how the data and business functionality is provisioned by the service provider. Again, the principles relating to assurance and conformance do not change from traditional outsourcing arrangements and a Critical Infrastructure Provider should be satisfied that there are adequate tools and mechanisms available to achieve assurance prior to entering into a cloud based outsourcing arrangement.

Managing Information Security during the Outsourcing Process

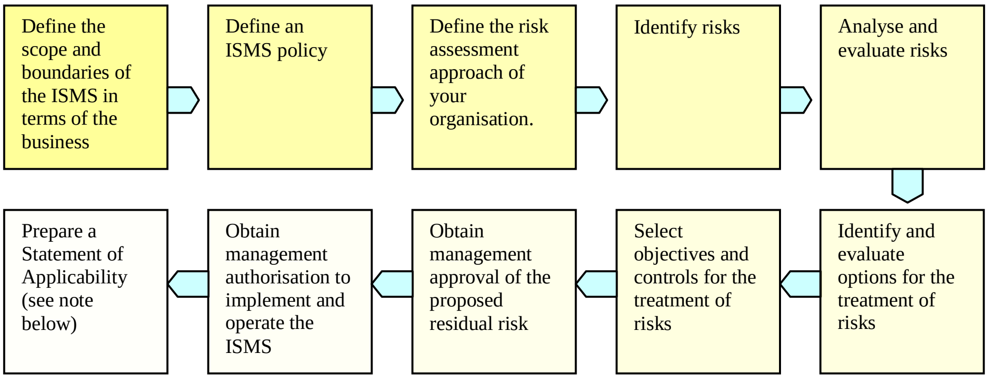
A Critical Infrastructure Provider will need to consider its in-house capability to effectively manage IT security throughout the duration of an outsourcing arrangement. If an organisation is not confident of its capability in this area, it may consider contracting this function to a qualified third party. This is important as an organisation's management has a responsibility to ensure that it has sufficient visibility over the security controls and that they are working effectively. This visibility relates not only to the outsourced service provider, but also with any subcontractors used by the service provider.

Accordingly, prior to entering into an outsourcing arrangement, an appropriate organisational IT security strategy should be put in place and uniformly incorporated into each outsourcing contract ensuring consistency. This will assist the organisation to:

- enhance alignment between outsourcing contracts and the organisation-wide strategy;
- make administration more effective and efficient;
- increase the likelihood of overall compliance; and
- allow for the easier detection of systemic and organisational issues.

S/NZS ISO/IEC 2700 x[11] provides a useful reference that specifies the requirements of an effective ISMS model. Accordingly, a critical infrastructure provider may consider using an ISMS model similar to Figure 5.

Figure 5: ISMS model



Define the scope and boundaries of the ISMS in terms of the business
Define an ISMS policy
Define the risk assessment approach of your organisation.
Identify risks
Analyse and evaluate risks
Identify and evaluate options for the treatment of risks
Select objectives and controls for the treatment of risks
Obtain management approval of the proposed residual risk
Obtain management authorisation to implement and operate the ISMS
Prepare a Statement of Applicability (see note below)

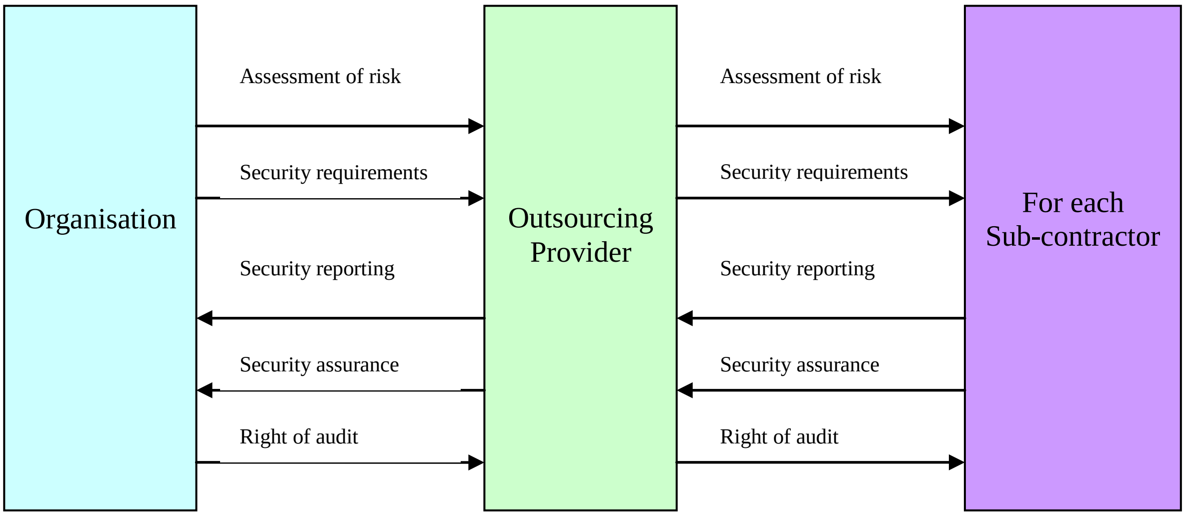
Note: A Statement of Applicability shows the controls that have been selected, or not selected from ISO 27001 and the reason for their selection, or non-selection. It must also show the controls as currently implemented.

The information security management process illustrated in Figure 6 shows the development of the relationship between the organisation and the outsourcing

[11] http://infostore.saiglobal.com/store/Details.aspx?ProductID=394879

provider, describing the flow of information related to risk assessment, security requirements, reporting, security assurance, and right of audit.

Figure 6—Flow of risk management information in an outsourcing arrangement



In the case of an outsourcing arrangement, if the service provider subcontracts work related to the organisation's IT functions, they should repeat the outsourcing information security management process with each subcontractor, such that the ISMS covers all of the information and systems outsourced by the organisation. This should be specified within the initial outsourcing contract.

> Managing information security during a cloud based outsourcing arrangement remains the same as for traditional outsourcing arrangements, however an organisation may need to accept the policies and processes on offer from the cloud vendor. Should this be the case, the organisation should satisfy themselves that the acceptance of the vendor's processes will provide suitable oversight across the service throughout the arrangement.

Incident Management

The actions taken in response to an information security breach or incident may have significant impacts on an organisation. An outsourcing arrangement should contractually oblige the outsourcing provider to report to a nominated contact within the organisation on an agreed basis (and format) all security related:

- suspected or confirmed incidents (such as a detected abnormality in an operating environment);
- anomalies;
- contact by law enforcement, regulatory or security authorities; and
- civil injunctions or search orders.

Approaches to incident management are covered in detail within the Information Technology Infrastructure Library (ITIL) framework[12], as well as *AS/ISO 27002*, which covers information security incident management.

An organisation should contractually agree with the outsourcing provider on how security incidents should be investigated and corrective actions taken, particularly those to be taken in an emergency.

In addition to conventional contingency planning and disaster recovery, the organisation should contract with the service provider about managing incidents involving sustained electronic attacks which may threaten the ability of the service provider to continue to operate the service in accordance with the security control requirements.

Incident management principles do not change under a cloud based outsourcing arrangement from those within a traditional arrangement.

[12] http://www.itil-officialsite.com/

Termination and Transition

A contract can be terminated (discharged) for a number of reasons, including:

- the outsourcing provider fulfilling all obligations;
- mutual agreement;
- due to underperformance;
- a breach of contract; or
- as a matter of convenience[13].

Security risks at this stage of the contract lifecycle may include:

- the service provider's failure to return all required materials; and
- disagreement with regard to a final payment, or the submission of unforseen additional costs by the service provider.

There are additional security risks to consider if an organisation is discharging an agreement with one service provider and transitioning IT functions to another service provider.

These include:

- failure to properly manage the transition process;
- disruption to the provision of products and services; and
- failure to address performance problems (particularly if the impetus for termination and transition was poor performance) within the previous outsourcing arrangements.

If an organisation has discharged a contractual arrangement, and commenced a tender process to engage another service provider, it should manage the process of re-tendering in line with probity requirements, particularly where the existing (or previous) service provider is re-tendering. The existing, or previous service provider, must be treated in the same way as any other tender applicant. The organisation should also ensure that the existing, or previous service provider is only privy to information about the process that is freely available to other tender applicants.

An organisation's contract with the IT service provider should detail how security will be managed in event of termination and/or the transition of the contract. For further information on termination and transition, please refer to Appendix C.

Once again, under a cloud based outsourcing arrangement a Critical Infrastructure Provider will need to define a clear set of transition or termination arrangements within the contract. Given the nature of using cloud for the provision of services,

[13] *Developing and Managing Contracts, Getting the Right Outcome, Paying the Right Price*, ANAO Best Practice Guide, February 2007, p 100
www.anao.gov.au/

which is largely homogenous, the compatibility between one provider and another can be highly variable. This in turn can mean that whilst a cloud-based arrangement may deliver greater cost efficiencies throughout the delivery of the service, the costs associated with changing providers or delivery mechanisms (e.g. to an in-sourced arrangement) may be costly and complex in its nature.

Conclusion

The outsourcing of services has the potential to deliver both strategic and economic benefits for critical infrastructure providers. However, as this guide has shown, prior to the commencement of any outsourcing arrangement, a careful consideration of risks and threats, the structure of contractual arrangements and compliance obligations must take place.

For a critical infrastructure provider, the design and implementation of sound information security principles and practices should be of paramount importance and integrated throughout each and every business process prior to entering into any agreement for the outsourcing of services.

As has been discussed throughout the guide, the outsourcing of services may transfer the responsibility for the delivery of services to a third-party provider, however the responsibility to for sound information security governance and risk management always remains the responsibility of the organisation throughout the life of the arrangements.

This guide has sought to raise awareness regarding the need for organisations to consider their responsibilities to maintain sound information security principles and practices from both a legislative and operational perspective when considering the outsourcing of services. Further information on information security principles can be found on the TISN website (www.tisn.gov.au) and within the accompanying Executive Overview of this guide.

4. Appendices

Appendix A – Example Organisational and Service Provider Roles and Responsibilities

The table below provides an overview of the typical organisational roles and security responsibilities required for the effective execution of an outsourcing arrangement. In all cases, the resources should have the commensurate experience required to fulfil the responsibilities required of the role.

Example organisational roles and security responsibilities

Outsourcing Project Sponsor	**Responsible at the organisational level for ensuring that**: • security risks and compliance requirements are defined; • the level of residual risk is understood and agreed to by the organisation; • security requirements are framed in the context of the organisational enterprise strategy; • an appropriate security framework is defined; • newly identified security risks during the outsourcing lifecycle have been appropriately assessed; and • assurance that security risks are managed and processes are in place and operating effectively.
Outsourcing Project Security Manager	**Responsible at the project level for ensuring that**: • security risks and compliance requirements have been understood by the organisation's outsourcing team; • the acceptable level of residual risk is achieved throughout the project on behalf of the organisation; • security requirements are clearly articulated; • processes are in place to sustain effective security risk management; and • incidents are reported, investigated, and corrective actions taken, where appropriate.

Outsourcing Procurement Manager	**Responsible for ensuring that contracts and schedules:** ● clearly articulate the security risks and compliance requirements; ● contain reference to all legislative and compliance obligations; ● incorporate IT security requirements within the procurement documentation and associated schedules; and ● contain well-structured and enforceable SLA's that can be, both delivered and audited for compliance.
Outsourcing Transition and Service Manager	**Accountable for ensuring that outsourced services are managed such that:** ● security risks and compliance requirements are met; ● security requirements are clearly understood; ● the organisational level of residual risk is supported by the delivered service; ● security risks are effectively managed during the outsourcing lifecycle; ● assurance is gained that security risks are managed and that processes are in place to sustain security risk management, and ensure that incidents are reported and investigated.
Appointed in-house assessor, qualified third party assessor, or auditor	**Responsible for ensuring that:** ● the security controls, implemented by the service provider correspond to those required in the contract; ● assurance is gained against the management of security risks and that processes are in place to sustain security risk management; and ● incidents are reported, investigated and corrective actions are taken.

Example service provider roles and security responsibilities

Commercial Director	**Responsible for preparing the bid response, and subsequently delivering, the outsourcing contract with accountability for ensuring that:** • security risks and compliance requirements meet the defined requirements of the organisation; • the acceptable level of residual risk will be maintained by the outsourcing provider; • security risks are managed throughout the outsourcing lifecycle; • assurance is gained and provided to the organisation, that security risks are managed and that processes are in place to sustain security risk management; • incidents have been reported, investigated and that corrective actions are taken; and • representations made to the organisation are complete and true.
Provider Transition and Service Manager	**Accountable for ensuring that outsourced services continue to be managed such as:** • the organisation's security risks and compliance requirements are met throughout the transition and operation of the service; • the agreed level of organisational residual risk is supported through the provision of the service; • assurance is maintained over the management of security risks and that processes are in place to sustain security risk management, and • incidents are reported, investigated and that corrective actions are taken.

Outsourcing Security Manager	**Accountable to the above managers for operationally ensuring that:** • security risks and compliance requirements are met throughout the delivery of the service; • the acceptable level of residual risk is agreed by the organisation; • security risks are managed effectively and actively throughout the delivery of the service, • incidents are reported, investigated and that corrective actions are taken; and • performance improvement suggestions regarding IT security are proposed throughout the delivery of the service.

Appendix B – Assurance Tools and Mechanisms

Information security assurance throughout an outsourcing arrangement may be achieved through a variety of mechanisms. The table below provides an organisation seeking to utilise the outsourcing of services with a range of useful assurance tools and mechanisms.

Method	Approach
Regular security management scorecards and reporting	The organisation should contractually agree with the service provider to provide regular reporting on performance of the outsourced functions, with specific reference to information security incidents, emerging threats, and changes to the regulatory environment affecting both the organisation and the service provider.
Service provider commissioned security audits	Provider commissions regular independent reviews or tests of the security of the systems being operated, and reports to the organisation the results of the reviews, corrective actions identified, and the progress of work to address the corrective actions.
Organisation commissioned security reviews	Organisation commissions own (or independent) auditors to review or test the security of provider's systems. Organisation may require that systems are formally accredited – these processes should be agreed as part of the security requirements for the system.
SAS70 review	Organisation contractually requires provider to provide a management attestation and to commission a third party audit review, for example using SAS70 principles and which may be a formal SAS70 audit, to provide assurance that control objectives have been complied with. AS/ ISO 27002:2006 may be used as a basis to identify control areas to be specified, although other security standards may also be used.

Letters of assurance	The provider to supply the organisation with a report verifying that security is operating in accordance with the organisations' security requirements, compliance requirements, assessment of risk, and that there has been no known or suspected security incidents other than those already reported in writing. The provider should procure the counter-signature of a regulated Auditor on the letter of assurance.
AS/ ISO 27001 Certification	The organisation and provider agree the risk assessment, compliance requirements specification and control objectives to be used as the basis of the *ISO27001 ISMS*. The *AS/ISO27001* Statement of Applicability is defined to include the entire scope of the outsourcing contract and all people, processes, facilities and systems supporting it if full coverage is to be achieved. Provider implements, operates, monitors, reviews, maintains and improves the ISMS in accordance with *ISO 27001*, carrying out all *ISO27001* requirements. Provider commissions *ISO27001* registered auditor to review the ISMS and grant *ISO27001* certification. At the organisation's option, the provider contracts with a regulated audit firm that is certified against *ISO27001* to provide dual assurance, comprising *ISO27001* certification and a *SAS70* opinion.

Appendix C – Outsourcing Termination and Transition Arrangement Organisational and Service Provider Contractual Obligations

The table below outlines, at a high level, the typical organisational and service provider contractual obligations during the transitional period of moving to a new service provider and/or during the termination of an existing outsourcing arrangement.

Upon transition	• How the service provider will work with the new service provider to transition outsourced IT systems in accordance with an agreed service termination process; • What arrangements are in place to ensure that the ISMS is transitioned to the new IT service provider in accordance with a contractually agreed ISMS termination plan; • Assurance that a transition will be properly managed and that there will be minimal disruption to services; and • Evaluation in relation to the performance of the contract, service provider and the organisation, and that any 'lessons learned' will be incorporated into new arrangements, and if necessary, requirements to update internal policies and procedures to reflect any lessons learned.
Upon termination	• Ensure the service provider will supply the organisation with documents, files, procedures, configurations, drawings or records relating to the organisation's services, and destroy all information on storage media such as disks and tapes; • Record and make clear any intellectual property rights; • Ensure that there are sufficient steps taken to terminate access rights or arrangements, which can include making sure that all administrative accounts are disabled or reset, and that all remote management systems are disabled or blocked; and • Ensure deliverables are supplied in accordance with agreed standards and that triggers for final payment are articulated.

Appendix D – Indicative Change Management Initiation and Cost Responsibilities[14]

The table below outlines the indicative change management initiation and cost responsibilities within an outsourcing arrangement.

Type of change	Responsibility
• Variations in contract scope. • Variations in service level. • Variations in system or process functionality. • Variation in system or process performance. • Organisation-defined variation in service location(s). • Increased need for vulnerability management in organisation-specified technologies. • Change in organisation-issued policies or standards. • Organisation-caused variations in the security business impact or threat. • Organisation-caused security incident investigation.	Organisation
• Provider-initiated changes to service provision technologies, location(s), and people. • Increased need for vulnerability management in Provider-specified technologies. • Provider-caused variations in the security business impact or threat. • Security incidents in provider 3rd party organisations (sub-contractor) which impinge upon the organisation or their systems.	Service Provider
• Changes in the assessed level of threat Legislative, regulatory, or compliance change or externally caused security incident.	Negotiated

[14] *Outsourcing: Security Governance Framework for IT Managed Service Provision, Good Practice Guide – 2nd Edition,* Centre for the Protection of National Infrastructure, June 2009, p 27

Appendix E – Contract Lifecycle and Security Activities

Each of the contract lifecycle stages and their relevant IT security activities are outlined in the table below:

Stage	Activities	IT Security activities
High level requirements (Stage 1)	• Organisation defines services required under outsourcing arrangement. • Organisation issues requirements to providers and invites response.	• Organisation defines security related requirements under outsourcing arrangement. • Organisation invites responses as to suggested methods of managing security.
Carry out risk assessment (Stage 1)	• Organisation carries out risk assessment and defines compliance requirements.	• Specify security risks to be managed. • Define statement of security compliance, regulatory, architectural, and policy requirements.
Detailed statement of requirements (Stage 1)	• Develop detailed statement of requirements for outsourcing arrangement.	• Organisation decides preferred method of managing security. • Organisation validates security approach complies with internal and external assurance requirements.
Choose appropriate service provider (Stage 2)	• Organisation identifies selection criteria. • Organisation evaluates provider responses.	• Identify selection criteria relating to security. • Evaluate provider's security responses. • Ensure bids address information and IT security aspects. • Verify provider's IT security capability.

Contract negotiation (Stage 2)	• Negotiation and finalisation of contract. • Contract and contract scope change processes incorporated into the contract.	• Agree and finalise contract security aspects. • Ensure security related contract and scope change processes are incorporated in contract.
Service build and transition (Stage 2)	• Provider builds necessary systems required for transition to outsourcing arrangement. • Provider transitions services from organisation to provider.	• Provider manages security in accordance with contract to ensure all requirements are met. • Provider ensures assurance as per contract. • Provider and organisation jointly plan and execute transition security activities. • Provider and organisation cooperate on agreed security accreditation reviews.
Operate service, monitor and report on provider performance (Stage 3)	• Provider operates system in accordance with contract and Service Level Agreements. • Performance of system monitored.	• Provider supplies security related reports, reviews, and audits as outlined in contract and Service Level Agreements.
Change management (Stage 3)	• Provider manages change in accordance with agreed change management processes.	• Provider manages security related change in accordance with security change processes.
Manage transition arrangements to a new contract with a service provider (Stage 4)	• Provider works with new provider to transition services in accordance with agreed service termination processes.	• Provider transitions existing ISMS to new provider in accordance with agreed service termination processes.

Appendix F – Useful Resources and Reference Material

Standards

- *AS/NZS ISO/IEC 27001:2006, Information technology – Security techniques – Information security management systems – Requirements,* Standards Australia, Sydney, 2006
- *AS/NZS ISO/IEC 27002:2006, Information technology – Security techniques – Code of practice for information security management*, Standards Australia, Sydney, 2006
- *Control Objectives for Information and related Technology (COBIT) V4.1,* IT Governance Institute, Rolling Meadows,2007
- *Statement on Auditing Standards No. 70: Service Organizations (SAS70),* American Institute of CPAs
- *Information Technology Infrastructure Library (ITIL), Office of Government Commerce (OGC)*

Trusted Information Sharing Network (TISN) www.tisn.gov.au

- *Achieving IT Resilience – Summary Report for CIOs and CSOs, May 2010*
- *Secure Your Information: Information Security Principles For Enterprise Architecture, June 2007*
- *Mobile Device Security Information for CIOs/CSOs, TISN May 2009;*
- *IT Security Governance: CIO, CISO, and Practitioner Guidance, Revision 2, December 2009*
- *Critical Infrastructure Resilience: Whose Responsibility is it?, 2009*
- *Defence in Depth,* June 2008

Australian Government

- *Cyber Security Strategy, Australian Government, November 2009*
- *Australian Government's Critical Infrastructure Resilience Strategy, Australian Government,* June 2010

Other Resources

- *Outsourcing: Security Governance Framework for IT Managed Service Provision, Good Practice Guide – 2nd Edition, Centre for the Protection of National Infrastructure, June 2009*
- *IT Security Management Audit Report No. 23, Australian National Audit Office, Dec 2*
- *Jericho Forum Commandment,* www.opengroup.org/jericho/commandments_v1.1.pdf