2.2. Non-Government Engagement and Outsourcing

Objective

2.2.1. Non-government organisations handling classified information implement the same information security and protective measures as government agencies.

Context

Scope

2.2.2. This section covers information on outsourcing information technology services and functions to contractors and commercial entities as well as providing those partners with necessary classified information in order to undertake their contracted duties.

Cloud computing

2.2.3. Cloud computing is a form of outsourcing information technology services and functions usually over the Internet. The requirements within this section for outsourcing equally apply to providers of cloud computing services.

PSR References

2.2.4. Additional information on third party service providers is supplied in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV4, GOV5, INFOSEC1, INFOSEC2, PERSEC1, PERSEC2, PERSEC3, and PERSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements

Rationale & Controls

Outsourcing information technology services and functions

2.2.5.R.01. **Rationale**

In the context of this section, outsourcing is defined as contracting an outside entity to provide essential business functions and processes that could be undertaken by the Agency itself.

Outsourcing may present elevated levels of risk and additional risks. Outsourcing therefore, requires greater consideration, demonstrable governance, and higher levels of assurance before committing to such contracts.

2.2.5.R.02. **Rationale**

A distinction is drawn between important business functions and the purchase of services such as power, water, building maintenance, stationery and telecommunications. These services are not usually provided by the agency itself.

Purchased services, as identified above, do NOT require accreditation or a third party review as defined in the NZISM. However, normal contract due diligence should be exercised before committing to these supply contracts.

2.2.5.R.03. **Rationale**

Contractors can be provided with classified information as long as their systems are accredited to an appropriate classification in order to process, store and communicate that information. Contractors and all staff with access to the classified systems must also be cleared to the level of the information being processed. This ensures that when they are provided with classified information that it receives an appropriate level of protection.

2.2.5.R.04. **Rationale**

New Zealand, in common with most developed countries, has agreements with other nations on information exchange on a variety of topics,

including arms control, border control, biosecurity, policing and national security. The lead agency in each sector will usually be the controlling agency for each agreement. While the detail and nature of these agreements is sometimes classified, the agreements invariably require the protection of any information provided, to the level determined by the originator. Agencies that receive such information will be fully briefed by the relevant controlling agency or authority, before information is provided. It is important to note that there is no single list or source of such agreements.

2.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:216]

Agencies engaging industry for the provision of off-site information technology services and functions MUST accredit the systems used by the contractor to at least the same minimum standard as the agency's systems. This may be achieved through a third party review report utilising the ISAE 3402 Assurance Reports on Controls at a Third Party Service Organisation.

2.2.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:217]

Agencies SHOULD NOT engage industry for the provision of off-site information technology services and functions in countries that New Zealand does not have a multilateral or bilateral security agreement with for the protection of classified information of the government of New Zealand. If there is any doubt, the agency's CISO should be consulted.

Independence of ITSMs from outsourced companies

2.2.6.R.01. **Rationale**

If an agency engages an organisation for the provision of information technology services and functions, and where that organisation also provides the services of an Information Technology Security Manager, they need to ensure that there is no actual or perceived conflict of interest (See also Section 3.3 - Information Technology Security Manager).

2.2.6.R.02. **Rationale**

When an agency engages a company for the provision of information technology services and functions having a central point of contact for information security matters within the company will greatly assist with incident response and reporting procedures.

2.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:221]

Where an agency has outsourced information technology services and functions, any ITSMs within the agency SHOULD be independent of the company providing the information technology services and functions.

2.2.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:222]

Where an agency has outsourced information technology services and functions, they SHOULD ensure that the outsourced organisation provides a single point of contact within the organisation for all information assurance and security matters.

Developing a contractor management program

2.2.7.R.01. **Rationale**

The development of a contractor management program will assist the agency in undertaking a coordinated approach to the engagement and use of contractors for outsourcing and provision of information technology services and functions.

2.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:225]

Agencies SHOULD develop a program to manage contractors that have been accredited for the provision of off-site information technology services and functions.