3.1. The Agency Head

Objective

3.1.1. The agency head is accountable for information security within their agency.

Context

Scope

3.1.2. This section covers the role of an agency head with respect to information security.

Chief executive officer /or other title

3.1.3. In some agencies and bodies, the person responsible for the agency or body may also be referred to as the CEO, Director General, Director or similar title specific to that agency. In such cases the policy for the agency head is equally applicable.

Devolving authority

3.1.4. When the agency head's authority in this area has been devolved to a board, committee or panel, the requirements of this section relate to the chair or head of that body.

3.1.5. The Agency Head is also the Accreditation Authority for that agency. See Section 4.4 – Accreditation Framework.

3.1.6. Smaller agencies may not be able to satisfy all segregation of duty requirements because of scalability and small personnel numbers. In such cases, potential conflicts of interest should be clearly identified, declared and actively managed for the protection of both the individual and of the agency.

3.1.7. Refer also to *Compliance By Smaller Agencies* in 1.2.8 for information on joint approaches and resource pooling.

Rationale & Controls

Delegation of authority

3.1.8.R.01. **Rationale**

Where an agency head chooses to delegate their authority as the Agency's Accreditation Authority they should do so with careful consideration of all the associated risks, as they remain responsible for the decisions made by their delegate.

3.1.8.R.02. **Rationale**

The most suitable choice for delegated authority is a senior executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

3.1.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:282]

Where the agency head devolves their authority the delegate MUST be at least a member of the Senior Executive Team or an equivalent management position.

3.1.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:283]

When the agency head delegates their authority, the delegate SHOULD be a senior executive who understands the consequences and potential impact to the business of the acceptance of residual risk.

3.1.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:284]

Where the head of a smaller agency is not able to satisfy all segregation of duty requirements because of scalability and small personnel numbers, all potential conflicts of interest SHOULD be clearly identified, declared and actively managed.

Support for information security

3.1.9.R.01. **Rationale**

Without the full support of the agency head, security personnel are less likely to have access to sufficient resources and authority to successfully implement information security within their agency.

3.1.9.R.02. **Rationale**

If an incident, breach or disclosure of classified information occurs in preventable circumstances, the relevant agency head will ultimately be held accountable.

3.1.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:288]

The agency head MUST provide support for the development, implementation and ongoing maintenance of information security processes within their agency.