GOVERNMENT GUIDELINE ON CYBER SECURITY

ISMF Guideline 2 - An approach to risk assessment using the ISMF

Background

Version 3 and later of the South Australian Information Security Management Framework (ISMF) introduced a requirement for government agencies to establish and maintain an Information Security Management System (ISMS) in alignment with the principles contained in the corresponding ISO 27001 standard. As a risk-based approach to security, protection efforts need to be applied to according to the level of residual risk that an agency is willing to tolerate. Protection efforts should be increased for those assets that are considered critical, and to information that is of high value to supporting the business’ ongoing operations and resilience (i.e. Agency Critical Infrastructure and State Government Critical Information Infrastructure). This guideline supports implementation of ISMF Policy Statement 2.

Pre-requisite documents

The following documents should be read in conjunction with this guideline:

- ISMF Guideline 1a details transition priorities and expectations for the scope of the ISMS deployment
- ISMF Guideline 1b provides a suggested approach to establishing an organisation wide ISMS including relevant roles and responsibilities of various participants
- ISMF Guideline 8b describes the new classification scheme for confidentiality and provides translation from the earlier scheme to the new markings
- Annex A of the ISMF lists the baseline policies and standards that should be applied in an agency or supplier whose contractual conditions require it
- Table 3 of the ISMF describes the availability and integrity classifications used by SA Government agencies
- ISMF Control Selection Tool is a spread-sheet based tool to facilitate the recording of agency decisions on what policies, standards and controls are in place against a particular system, workplace function or geographic location.

Guidance

This guideline describes a process flow for managing risk and recording risk treatments and applied controls from the ISMF. Individual systems, services, functions or locations that have been incorporated into the ISMS should then be documented in an agency (or organisational) register as described in ISMF Guideline 1b.
Role of the risk assessment

The business-driven risk-based approach to cyber security of the ISMF requires decisions to be recorded on how risks have been addressed in order to provide an adequate level of assurance to the business that cyber security controls and protection mechanisms are in place, being used and effective.

The risk assessment process and arising documentation underpins the entire ISMS process. It effectively permits the business to identify risks in given areas and the required steps to reduce the residual risks to an acceptable level. This is achieved by considering how risks will be treated, tolerated, transferred or terminated. By applying protection efforts to the most sensitive and/or critical parts of the business and reducing the overheads of a traditional and arbitrary compliance-based model:

• duplication of efforts and resource overheads may be eliminated over time
• funding to cyber security initiatives can be allocated in a more predictable and consistent manner
• productivity gains are realised by focusing workforce efforts where they are required
• prioritisation of security initiatives is directly aligned to business priorities and goals.

As a quality management system, the ISMS is an ongoing function that embeds a continual improvement cycle. This requires agencies to reconsider protection measures and assure themselves that these measures are still relevant, being applied, effective, communicated and understood by all relevant parties including suppliers to government. It provides an opportunity to remove measures that are no longer applicable or relevant and to modify any existing measures taken to protect information assets in light of contemporary or emerging threats.

A single risk assessment may be used for multiple purposes within an agency and its importance cannot be understated. The risk assessment is of particularly high value to the business when applied to:

• the establishment of new ICT systems, platforms or architectures
• machinery of government changes including mergers and separation of workforce functions
• the establishment of an ISMS
• business impact assessments
• business continuity and disaster recovery planning activities
• applications for exemption from whole of government ICT standards
• procurement undertakings
• contracting services to a third party
• obtaining services from a third party
• post incident reviews
• reviewing and improving the ISMS
• ICT audits.
Assessing, managing and recording risk based on the ISMF

The following process table presents an overview of the necessary process flow required to establish a value of the information or asset using a classification process, consider, manage and record the risks identified by the business using the ISMF as a control mechanism and to assure the business that the SA government cyber security baseline has been incorporated – including those external risks that need to be managed by other parts of the business or contracted service providers. The final step in the process is to ensure that the results of the risk treatments are rolled-up into the organisational ISMS, and as a consequence that executive management has been made aware of the risks and treatments and is satisfied with the protection efforts being applied to any given initiative in the agency:

<table>
<thead>
<tr>
<th>Determine information value</th>
<th>Work with Business Owners to ascertain the confidentiality requirements for the information being processed. Work with Business Owners and ICT platform owners to determine the availability and integrity requirements of the information to be processed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess risks incorporating classification</td>
<td>Classifications for platforms/services/systems or locations should be recorded using the ISMS SoA tool. Identify risks and determine which policies, standards and controls from the ISMF facilitate treating these risks. Business Owners may elect to terminate the risk (i.e. cease the activity or undertaking), tolerate the risk (i.e. the risk is so remote in likelihood or inconsequential that it does not require treatment) or transfer the risk (i.e. in which case, the risk is managed but onus remains on the Business Owners to ensure that these risks are being adequately treated and continually self-assessed by the third party).</td>
</tr>
<tr>
<td>Validate that baseline controls are in place</td>
<td>Annex A of the ISMF describes the baseline cyber security requirements for all Responsible Parties irrespective of classifications assigned to any undertaking of the business. Analyse the policies, standards and controls in Annex A and record those controls directly implemented by the Business Owner <em>AND</em> those external risks managed by other parties (such as personnel vetting for staff or physical security for facilities etc.)</td>
</tr>
<tr>
<td>Agree upon identified external risks</td>
<td>Ensure that other parts of the business and/or contracted suppliers are aware of, and agree to the measures being proposed in order to manage risks that are not in direct control of the Business Owner, but are managed on behalf of them.</td>
</tr>
<tr>
<td>Obtain approvals for the controls</td>
<td>Ensure that protection decisions are recorded in the ISMS SoA tool, and that they have been communicated and agreed to by all Responsible Parties. Communicate the findings to the custodian of the organisational ISMS or the ISMS Project Team. The recorded decisions will need to be rolled up into the organisational ISMS. Refer ISMF Guideline 13 for further information.</td>
</tr>
</tbody>
</table>
Additional considerations

Agencies should contact the Department of the Premier and Cabinet should they identify State Government Critical Information Infrastructure (refer ISMF Guideline 37a) as part of their ISMS.

Recommendations arising from independent audits of the agency ISMS should be prioritised for treatment by Business Owners taking into consideration value for effort exerted, achievability and criticality to reduce risks identified by the audit findings.

Detailed implementation guidance for developing and establishing an ISMS is contained in the ISO/IEC 27003 standard.

This guideline does not constitute an absolute or mandatory method for managing risk or maintaining an Information Security Management System. It is merely a good practice guideline applied to the protective security policy position and operating characteristics of the Government of South Australia at the time of writing. The individual requirements and operational characteristics of agencies will have direct bearing on what measures are implemented to mitigate identified risk(s) and how such outcomes are achieved.

References, links and additional information

- Information Security Management Framework
- PC030 Protective Security Management Framework
- ISO/IEC 27003:2010
- AS/NZS ISO 31000:2009
- IEC/ISO 31010:2010
- Australian Government Protective Security Policy Framework (PSPF)
Document Control

<table>
<thead>
<tr>
<th>ID</th>
<th>DPC/G4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Classification/DLM</td>
<td>Public-I1-A1</td>
</tr>
<tr>
<td>Compliance</td>
<td>Discretionary</td>
</tr>
<tr>
<td>Original authorisation date</td>
<td>February 2014</td>
</tr>
<tr>
<td>Last approval date</td>
<td>February 2019</td>
</tr>
<tr>
<td>Next review date</td>
<td>February 2020</td>
</tr>
</tbody>
</table>

Licence

With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a Creative Commons Attribution (CC BY) 4.0 Licence. To attribute this material, cite Department of the Premier and Cabinet, Government of South Australia, 2019.