Government of **Western Australia**
Office of the **Government Chief Information Officer**

Whole-of-Government
Digital Security Policy

A supplementary guide.

Document Control

The Western Australian Whole of Government
Digital Security Policy: A Supplementary Guide
Version 1 – 13 June 2017

Produced and published by: the Office of the Government Chief Information Officer

Acknowledgements: The guide was developed in collaboration with Western Australian public sector agencies.

Contact: Office of the Government Chief Information Officer

2 Havelock Street

WEST PERTH WA 6005

Telephone: (08) 6551 3901

Email: policy@gcio.wa.gov.au

Document version history

Date	Author	Version	Revision Notes
June 2017	Office of the GCIO	1	First Release

Introduction

This document is to be read in conjunction with the Office of the Government Chief Information Officer (GCIO) whole-of-government Digital Security Policy (the Policy).

The purpose of this document is to provide:

- additional context to the Policy;
- guidance on how to meet the requirements of the Policy; and
- advice in achieving appropriate digital security outcomes.

The audience of this document is:

- those accountable for agency risk management;
- business representatives accountable for service delivery; and
- Information and Communications Technology (ICT) personnel responsible for digital security.

Why is digital security important?

Agencies are custodians of important information about the State, businesses and citizens, and have a moral and legislative obligation to safeguard these assets. For the community to fully utilise digital services, agencies must be trustworthy custodians of information.

Background

The *Digital WA* ICT Strategy is driven by a vision of better services delivered to the community, supported with innovative uses of technology, by a public sector that is mature in its digital capabilities. Digital security capability is fundamental to achieving this vision and the Policy seeks to support agencies in building their capability to identify, assess and treat digital security risks.

This guide will be supplemented and extended by further digital security initiatives from the Office of the GCIO that will support the public sector in building its digital security capability.

This guide is intended to support agencies to properly assess their digital security risks and baseline their security maturity over a 12 month period. This is in preparation for a more comprehensive, whole-of-government security capability building program currently being developed by the Office of the GCIO.

Policy Requirement One: Implement an Information Security Management System

At the core of a mature and responsive digital security capability is a structured approach to information security risk through an Information Security Management System (ISMS). As per Policy Requirement One, agencies must implement an ISMS.

Agencies are strongly encouraged to utilise *the* ISO/IEC 27000 series, particularly *ISO/IEC 27001: Information technology – Security Techniques – Information security management systems – Requirements* as the basis for their ISMS. The tools and guidance provided with this document are aligned with ISO27001.

What is ISO27001? Why should an agency adopt it?

ISO27001 is an industry standard, set by the International Organisation for Standardisation (ISO), which specifies requirements for establishing, implementing, maintaining and continually improving an information security management system.

ISO27001 is widely adopted across industry and government jurisdictions in Australia and overseas, and its requirements are generic and applicable to all organisations regardless of type, size and nature.

An agency should adopt ISO 27001 if it is appropriate for the organisation, and compatible with their business needs and existing risk frameworks.

What other standards can an agency use?

There are a range of standards available to assist agencies in managing their information security risks. Agencies can use any approach that enables them to meet the Policy requirements.

Protective Security Policy Framework

Commonwealth government agencies are required to implement the Protective Security Policy Framework (PSPF). For WA agencies with an identified business need to share data with Commonwealth government that is at a Classified level[1], implementing the requirements of the PSPF may be appropriate.

The PSPF has a broad focus beyond digital security; it is intended to manage security risks to people, information and assets. However, it is important to note that the PSPF is designed around the needs, context and legislative requirements of the Commonwealth government.

[1] As per the Commonwealth Government Data Classification scheme

Information Security Manual

The Australian Signals Directorate (ASD) publishes the Australian Government Information Security Manual (ISM). The ISM is used for the risk–based application of information-specific security controls, within the overarching structure of the PSPF. The ASD encourages all Australian state government agencies to apply the considered advice within the ISM.

Implementing the PSPF and ISM is a significant undertaking, and agencies will need to weigh up the costs and effort of customising and implementing these standards within a Western Australian context against their business needs. Providing standards that will assist Western Australian government agencies in sharing information easily and securely with the Commonwealth Government is an area of future focus of the Office of the GCIO.

Planning

For those agencies who do not have an ISMS, or have an incomplete approach to digital security (for example, security policies, but no formal security risk governance), the implementation of an ISMS should be managed like a project. Key considerations in the undertaking of this project will be:

- What standards does the agency have, and which should it use? In determining an approach for information security, an agency should consider the approach's compatibility with its relevant frameworks – such as risk management and business continuity.
- What existing security arrangements does the agency have? Does the agency have a security policy, and if so, how does it need to be amended to fit the agency's ISMS? If a new policy is required, what will it need to contain?
- Who will be responsible for developing and managing a program for the implementation of an ISMS (or reviewing the existing implementation)?
- What budget will be required?
- Is the corporate executive engaged and supportive of digital security? What can be done to get them on board?

Policy Requirement Two: Governance and Accountability

Governance

Governance establishes who does what, and who is responsible. An agency's digital security capability should be built upon a risk-based decision making approach that is driven by business needs. Good governance can support this and facilitate accountability and decision-making, and is at the heart of effective risk management. Good governance should be used to ensure that risks are allocated and corporate risk managers are informed and accountable for treating and accepting agency risks.

Executive oversight is fundamental to ensuring that digital security is afforded the appropriate level of attention and investment. Agencies should ensure that custodians of digital assets lead the conversation in identifying and assessing the risks with their digital assets.

Management should ensure that responsibilities and authorities for roles relevant to information security are assigned and communicated. Key roles should include ensuring that the ISMS conforms to the standard or rules governing it, and reporting on the performance of the ISMS to management.

Policy Requirement Three: Assess and Treat Security

Trust is earned over years – but lost in a moment.

The consequences of a failure to manage digital security risks can be immense. On 9 August 2016 – census night – the Australian Bureau of Statistics prevented households from logging onto the census website, a decision precipitated by a denial of service attack that was not adequately protected against. This incident resulted in $30 million in additional costs[2].

Risks

Risk Assessment

Digital Security is a risk management activity driven by the identification, assessment and prioritisation of risks - followed by the application of resources to minimise, monitor, and control the probability and/or impact of unforeseen events. Understanding digital security through this lens will help ensure alignment with agencies' existing risk management obligations and frameworks.

Data classification will allow agencies to be informed about the potential consequences regarding the loss of integrity, access or confidentiality of their data assets. Agencies should refer to the Office of the GCIO Data Classification Policy for more information regarding the data classification process.

ICT practitioners will need to work together with business representatives to assess the potential threats, vulnerabilities and attacks faced by the organisation.

[2] Source: *2016 Census: issues of trust*. Senate Economics References Committee. November 2016

Risk Assessment tools

A template risk register is available on the Office of the GCIO website. This will assist agencies in assessing, recording and reporting risks.

Agencies which wish to utilise a tool designed specifically for digital security risks – or who do not yet have a digital security risk register – may find this template useful.

Risk treatments and security controls

An agency's ISMS should contain a base level of controls to be applied in order to treat digital security risks. Agencies are strongly encouraged to utilise the controls detailed in Appendix 1 of ISO 27001, guided by the code of practice for their implementation which is detailed in *ISO 27002: Code of practice for information security controls*.

Agencies are also strongly encouraged to utilise the eight controls detailed with the ASD's *Essential Eight* strategies for the mitigation for cybersecurity risk. For more information on the *Essential Eight*, agencies can refer to the ASD published *Strategies to Mitigate Cyber Security Incidents* and the ASD *Essential Eight*.[3]

Digital Security Controls Checklist

Agencies are also strongly encouraged to utilise the Digital Security Controls Checklist which is available on the Office of the GCIO website. This checklist will allow agencies to make an assessment of their digital security controls against those stipulated in ISO27001.

This document can be utilised as a benchmark for agency risk treatment, and as a basis for corrections to existing risk treatments in order to improve risk management outcomes.

Policy Requirement Four: Continuous Improvement

Digital security deals with a dynamic threat environment that changes on a daily basis. Agencies must ensure that their risk treatments remain relevant and contemporary to the threats faced by their organisation, and that their skills and capabilities are commensurate. This should be a core function of the ISMS.

Any testing plans and activities, and their results, should be escalated to the risk management body, so they can be informed about changes to risk and ensure appropriate action is taken.

[3] https://www.asd.gov.au/infosec/mitigationstrategies.htm

What about auditing and certification?

Annual audit of agency security capability is recommended. This should be performed in alignment with the agencies capability and requirements. For some agencies, an internal audit may be deemed adequate, whereas for those with significant risks to manage, or to whom stakeholder validation and approval is a priority, an independent auditor may be required.

Whatever the case, agencies should ensure that their security activities are documented against their ISMS in order to ensure risks are managed and digital security capability is kept up to date.

Overall Maturity Progress

Data Classification, ICT Disaster Recovery for Business Continuity and Digital Security are core, interrelated policies, and are foundational in building the Western Australian public sector's digital security capability and maturity.

An Executive ISMS Progress Report for assessing overall digital security maturity (including Data Classification and ICT Disaster Recovery) is available on the Office of the GCIO website

The Report uses a defined maturity scale from 0 (*Non-Existent*) to 5 (*Proactive*), for measuring agency maturity to transforming its business in relation to digital security. This is aligned with the overall goals, and benchmarking, of the *Digital WA* Strategy.

Security Compliance does not equal security capability!

Simply implementing the controls provided within a standard or publication will not protect an agency from risk. Only a holistic approach to security risk management that includes a focus on capability building and good security outcomes will ensure an agency's risks are within its risk appetite.

Additional support information

More detailed information to support agencies in implementing this Policy can be found at:

Western Australia Police, Technology Crime investigations can be contacted for advice on and reporting of technology crime offences at: ACORN@police.wa.gov.au

ANZPAA publishes various relevant education and training guidelines, including:

- ANZPAA – Information Guide – Responding to a Technology Crime Event
- ANZPAA – Information Guide – Making your Company Technology Crime Resistant

These can be requested at:

https://www.anzpaa.org.au/professionalisation/access-requests