DPC/S4.14

ACROSS GOVERNMENT POLICY

Web application security standards

Purpose

The purpose of these standards is to secure the web presence and information assets of the Government of South Australia.

The objectives of these standards are to ensure that:

- the implementation or modification of web applications does not lead to the introduction of insecure code which may compromise the confidentiality or integrity of agency information assets
- baseline web application security controls are implemented to safeguard against unauthorised modification of web content and/or agency information assets
- software development and procurement processes incorporate adequate security so as to prevent adverse impact to agency information technology infrastructure, or the information assets housed within that infrastructure
- web applications that capture, store and process personal details consider the requirements of the Government of South Australia's Information Privacy Principles
- security requirements are considered in outsourced web development arrangements to ensure agencies are protected
- a whole-of-Government approach for developing and procuring secure web applications is established.

These standards are written to support the implementation of the AS/NZS ISO/IEC 27002 standard and the Government of South Australia Protective Security Management Framework (PSMF) versions 3.0 and later.

Background

The Government of South Australia has a large number of web applications that provide critical services to public and internal agency stakeholders. These web applications are developed by internal agency staff, and by external parties. Commercial off-the-shelf software is typically procured via existing agency processes. These web applications provide static or dynamic content for internal and external users.

Security requirements must be considered in all stages of the web development and procurement to ensure that effective security outcomes are achieved, leading to overall risk reduction to agencies.

This standard is intended to be independent of specific application development platforms or commercial applications and therefore does not define platform or vendor-specific requirements.

Scope

Scope inclusions

These standards apply to all web applications[1] used for SA Government business. This extends to:

- all bespoke, customised, and off-the-shelf web applications that require additional customised enhancements, including content management systems
- web based applications hosted by external providers (off-Net)
- all internal and public facing web applications hosted within StateNet (on-Net)
- web applications developed to be accessed from mobile devices including tablets and smartphones.

Scope exclusions

These standards do not apply to non-web-based software applications (e.g. desktop applications and operating systems).

Terms, abbreviations and conventions

Terms and abbreviations

Public facing	Web content that is accessible by the general public from the Internet.
SDLC	Systems Development Lifecycle
PSMF	Protective Security Management Framework
PCI DSS	Payment Card Industry Data Security Standard
OWASP	Open Web Application Security Project
ITSA	Information Technology Security Advisor

Conventions

The terms used in this document are to be interpreted as described in Internet Engineering Task Force (IETF) RFC 2119 entitled “Key words for use in RFCs to Indicate Requirement Levels”. The RFC 2119 definitions are summarised in the following table.

Term	Description
Must	This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement.
Must not	This phrase, or the phrase “SHALL NOT”, means that is an absolute prohibition.
Should	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
Should not	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
May	This word, or the adjective “OPTIONAL”, means that an item is truly optional.

[1] The term *web application* is a commonly used industry term (e.g. http://en.wikipedia.org/wiki/Web_application). It has not been defined specifically for this standard.

Standards

The requirements analysis, data classification and risk assessment activities defined within this document must be completed prior to the deployment of a web server.

Agencies must adopt a defence-in-depth approach to minimise the security risks to web applications. Security controls must be applied at each layer of the web application and associated web server to eliminate reliance on any single security control. Security controls must be selected based on the outcome of a risk assessment, and the classification of the information that will be processed by or stored on the web server.

These standards define a baseline of security controls that must be considered. They include a reference to the appropriate standard within the PSMF. Agencies should also note that particular requirements exist for public-facing web servers installed within StateNet.

Appendix 1 provides specific guidance for application developers to apply during software development (coding). This checklist extends the standards under *Standards - Development*[2].

Requirements analysis

	Standard	References
1	A Business Owner must be identified for each application and documented in an agency information asset inventory.	ISMF Standard 17 AS/NZS ISO/IEC 27002 7.1.2
2	Security requirements must be documented, particularly requirements for safeguarding information.	ISMF Standard 103 AS/NZS ISO/IEC 27002 12.1.1
3	Security requirements must be approved by a Business Owner, in consultation with the ITSA.	ISMF Standard 17 AS/NZS ISO/IEC 27002 7.1.2
4	A risk assessment must be undertaken and documented to establish a risk profile for each application.	ISMF Standard 1 AS/NZS ISO/IEC 27002 O 12.1.1
5	Information to be processed by the application must be classified by the application Business Owner.	ISMF Standard 19 AS/NZS ISO/IEC 27002 7.2.1
6	Applications that store, transmit, and/or process personal information must consider the requirements of the *Government of South Australia's Information Privacy Principles.*	ISMF Standard 127 AS/NZS ISO/IEC 27002 10.9.2
7	Business continuity and recovery plans must be updated or developed where business critical functions are being provided and/or as deemed necessary based on the established risk profile of the application.	ISMF Standard 130 AS/NZS ISO/IEC 27002 15.1.4
8	The Payment Card Industry Data Security Standard must be implemented for web applications that store, process or transmit payment card data[3].	ISMF Standard 127 AS/NZS ISO/IEC 27002 10.9.2 Payment Card Industry Data Security Standard
9	Segregation of systems that store, process or transmit payment card data should be considered to minimise the	ISMF Standard 127 AS/NZS ISO/IEC 27002 10.9.2

[2] Note that the checklist covers specific development requirements. A completed checklist does not indicate conformance with Standards).

[3] Bizgate is the SA Government's preferred ICT solution for payments. Please contact the Bizgate team for more information.

	scope of Payment Card Industry Data Security Standard compliance requirements.	Payment Card Industry Data Security Standard

Design

	Standard	References
10	Application security controls must be identified and documented. When selecting security controls, consideration must be given to both the risk assessment and assigned classification level of the application.	ISMF Standard 103 AS/NZS ISO/IEC 27002 12.1.1
11	Security controls must include, but not be limited to: separation of duties to restrict individuals from conducting inappropriate or unauthorised activities restricting access to application functionality to authorised users in accordance with business requirements or needs control of data input, output and processing within the application to ensure that data is protected from compromise of confidentially and integrity controls that are needed for maintaining the integrity of the application, including logging, authentication, and audit.	ISMF Standard 49 ISMF Standard 71 ISMF Standard 103 AS/NZS ISO/IEC 27002 10.1.1 AS/NZS ISO/IEC 27002 10.10.2 AS/NZS ISO/IEC 27002 12.2
12	Cryptographic systems and techniques must be used for the protection of information that is considered at risk. Cryptographic systems and techniques must implement DSD Approved Cryptographic Protocols and Algorithms as defined in the Australian Government Information Security Manual.	ISMF Standard 109 AS/NZS ISO/IEC 27002 12.3.1
13	Application security design documentation should be reviewed by an agency ITSA and approved by the Business Owner.	-
14	Based upon the risk profile web applications should implement a multitier architecture. This will ensure components of the application are securely separated.	-

Development

	Standard	References
15	Web applications must be developed according to applicable agency application coding procedures. Procedures must address common coding vulnerabilities, including: • injection flaws, particularly SQL injection • buffer overflows • insecure cryptographic storage and communications • improper error handling. Refer to *Appendix 1 – Web application coding checklist* for specific considerations when developing web application code.	ISMF Standard 103 AS/NZS ISO/IEC 27002 12.2 Appendix 1 – Web application coding checklist
16	Tested and approved code should be reused where possible when performing common programming tasks.	-

Outsourced development

	Standard	References
17	When entering into outsourcing arrangements for development, legal advice should be sought to ensure that agency rights and interests are protected.	ISMF Standard 120 AS/NZS ISO/IEC 27002 12.5.5
18	Agencies should utilise the existing eProjects Panel for engaging with approved third parties. The existing eProjects panel deed addresses a range of security and privacy requirements.	-
19	Security and privacy requirements must be formalised in contracts with external developers. Where applicable these standards should be referenced in Tender or Request for Quotation (RFQ) documentation.	ISMF Standard 120 AS/NZS ISO/IEC 27002 12.5.5
20	The right to audit should be included in all contracts to protect Government rights and interests.	ISMF Standard 120 AS/NZS ISO/IEC 27002 12.5.5
21	The use of software code escrow[4] should be considered for custom developed applications.	ISMF Standard 120 AS/NZS ISO/IEC 27002 12.5.5
22	Contracts with developers must consider the protection of the intellectual property of source code to protect Government interests.	ISMF Standard 128 AS/NZS ISO/IEC 27002 15.1.2

Testing

	Standard	References
23	Test plans should be developed and documented based on the outcomes of the risk assessment. Applications considered a 'high' risk must undertake additional testing to ensure implemented security controls are operating effectively. Test cases should consider attack and abuse use cases, with a specific focus on misuse of inputs and outputs to compromise the security of the application. Testing of complex applications with numerous inputs may be conducted on sample basis.	ISMF Standard 116 AS/NZS ISO/IEC 27002 12.5.1
24	Security testing (e.g. code reviews and penetration testing) should be performed based on the risk assessment. Testing should be performed at critical milestones to validate that controls operate as designed.	ISMF Standard 53 AS/NZS ISO/IEC 27002 10.3.2
25	Security testing must be performed by individuals other than the originating code author. Testing must be performed by individuals with qualifications that are deemed appropriate by the agency Business Owner.	ISMF Standard 118 AS/NZS ISO/IEC 27002 12.5.3
26	Security vulnerabilities identified during testing should be addressed prior to production implementation. Any untreated security vulnerabilities must be documented, and the documentation reviewed by the agency ITSA and approved by the Business Owner.	ISMF Standard 53 AS/NZS ISO/IEC 27002 10.3.2

[4] Source code escrow is the deposit of the source code of software with a third party agent, http://en.wikipedia.org/wiki/Source_code_escrow

27	Development and test environments must be kept separate from production environments.	ISMF Standard 50 AS/NZS ISO/IEC 27002 10.1.4
28	Personnel assigned to the development or test environments must not have access to the production environment or data unless authorised by the Business Owner.	ISMF Standard 50 AS/NZS ISO/IEC 27002 10.1.4
29	Production data should not be used for testing or development unless authorised by the Business Owner.	ISMF Standard 50 AS/NZS ISO/IEC 27002 15.4.2
30	Data supplied for development must not reveal or allow the recreation of sensitive information including personal information. If production data is to be used for testing, security controls must be implemented to adequately safeguard agency data.	ISMF Standard 50 AS/NZS ISO/IEC 27002 15.4.2

Implementation

	Standard	References
31	All documentation must be adequately protected from unauthorised access.	ISMF Standard 62 AS/NZS ISO/IEC 27002 10.7
32	Web application components and supporting services with known or published high risk or critical vulnerabilities must not be used, or must be patched within an acceptable timeframe of the vulnerability becoming known.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6
33	All unnecessary application content should be removed prior to application acceptance into production. This includes removing all test and default files, test user accounts and other unnecessary content.	ISMF Standard 53 AS/NZS ISO/IEC 27002 10.3.2
34	Application administration access interfaces (e.g. admin login pages) should be disabled or be restricted.	-
35	Agencies must not use internal user credentials on public facing systems.	-
36	Web applications must be configured to use a service account assigned the least privileges necessary to run the applications	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2

Hosting

	Standard	References
37	Where applications are being developed and/or hosted externally the Information Privacy Principles (Premier and Cabinet Circular PC012) must be considered. Outsourcers must be made aware of the Government continuing ownership of its data.	Information Privacy Principles
38	The requirements described in the document outlining the *StateNet Conditions of Connection,* and the guidelines covering *StateNet Public Access Web Services Deployment must* be considered when applications are deployed within the StateNet environment.	StateNet Conditions of Connection
39	Where applications are being hosted within StateNet, the application must support termination of encrypted services	-

	at a StateNet gateway. Application -level encryption, however, will be considered on a case-by-case basis.	
40	Hosting agreements with non-government hosting providers must define security requirements and responsibilities of the third party. The requirements of the *Web Server Security Standards* should be included as a baseline to address security requirements.	ISMF Standard 14 AS/NZS ISO/IEC 27002 6.2.3 Web Server Security Standards
41	Based on the established risk profile and classification, high risk web applications should not be hosted on shared infrastructure (including cloud-based solutions). Where shared infrastructure is used, contractual arrangements must establish service levels and appropriate security controls.	ISMF Standard 14 AS/NZS ISO/IEC 27002 6.2.3
42	All hosting agreements must adequately define security requirements and responsibilities in a concise manner to reduce potential misunderstandings.	ISMF Standard 14 AS/NZS ISO/IEC 27002 6.2.3
43	When entering into agreements with service providers, the agency should reserve the right to audit to the third party to ensure the ongoing effectiveness of security controls.	ISMF Standard 14 AS/NZS ISO/IEC 27002 6.2.3
44	All web application data must have an appointed data custodian who is responsible for maintaining integrity and protection of the data. This custodian can be the same as the appointed Business Owner.	
45	Mechanisms must be established for monitoring hosted applications to ensure agreed service levels are maintained and security controls are operating effectively.	ISMF Standard 14 AS/NZS ISO/IEC 27002 6.2.3
46	Security Incident management responsibilities must be established to ensure that incidents and weaknesses are reported and actioned according to existing agency procedures. Where applications are hosted by non-government hosting providers, agreements must establish responsibilities for incident reporting.	ISMF Standard 32 AS/NZS ISO/IEC 27002 13.2.1
47	Web applications' servers must implement appropriate security hardening and follow the *Web Server Security Standards*.	Web Server Security Standards

Operations and maintenance

	Standard	References
48	Version control must be maintained for all application updates and changes.	ISMF Standard 115 AS/NZS ISO/IEC 27002 12.4.3
49	All changes to applications, including updates and patches, must be reviewed and tested to ensure that there is no adverse impact on operation or security. This includes: 1 formal change control procedures must be established and documented, and evidence retained that the procedure is implemented and complied with 2 changes must be approved by the Business Owner or nominated delegate 3 systems must only be deployed on production and public facing networks after assessment and final approval by authorised parties	ISMF Standard 48 AS/NZS ISO/IEC 27002 10.1.2

	4 adequate testing must take place prior to changes being applied to production systems.	
50	Business continuity and recovery plans should be updated to reflect changes to production systems.	ISMF Standard 130 AS/NZS ISO/IEC 27002 15.1.4
51	When significant changes or enhancements are made, a risk assessment must be performed to consider the security implications of such changes. Additional security testing should be undertaken as deemed necessary by risk assessment.	ISMF Standard 116 AS/NZS ISO/IEC 27002 12.5.1
52	Agency vulnerability identification and patch management procedures, roles and responsibilities must be defined and followed to ensure security vulnerabilities in web applications are identified and patched.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6.1
53	Periodic penetration testing should be performed to ensure the ongoing effectiveness of application security controls as new threats emerge.	ISMF Standard 121 AS/NZS ISO/IEC 27002 12.6.1
54	Security incidents must be reported according to the agency incident management procedures. These procedures must incorporate the requirements of *ISMF Standard 140 – Notifiable Incidents*	ISMF Standard 30 ISMF Standard 140 AS/NZS ISO/IEC 27002 13.1.1
55	Web application monitoring tools should be implemented to detect breaches or misuse of web applications.	-

Protection of source code

	Standard	**References**
56	The reference copy of source code must be stored in a source code library approved by the Business Owner.	ISMF Standard 115 AS/NZS ISO/IEC 27002 12.4.3
57	Source code libraries must be adequately secured to protect against unauthorised or inappropriate access or changes.	ISMF Standard 115 AS/NZS ISO/IEC 27002 12.4.3
58	An audit log must be maintained of all access to program source libraries.	ISMF Standard 115 AS/NZS ISO/IEC 27002 12.4.3
59	The reference copy of source code must not exist on production web servers.	ISMF Standard 115 AS/NZS ISO/IEC 27002 12.4.3
60	Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational.	ISMF Standard 115 AS/NZS ISO/IEC 27002 12.4.3

Implementation

Implementation considerations

SA Government agencies, or external parties that develop, procure and implement web applications on behalf of the Government of South Australia, must implement the requirements of these standards.

The majority of agency web applications are hosted within the SA Government enterprise network StateNet which has a specific role-based network segment for hosting public-facing web applications. This segment includes a number of specific security functions including intrusion prevention, auto-vulnerability assessment and application security management technology. The conditions of use that apply to agency web servers deployed in this segment are covered in a separate document.

Exemptions

Exemptions to these standards must adhere to existing across-government ICT exemption policies.

Responsibilities

The following responsibilities are defined.

Role	Responsibility
Chief Information Officers	Are responsible for ensuring that these standards are implemented across web applications owned by the agency.
Agency Information Security Technology Advisors (ITSA)	Provide advice on the applicability, interpretation and implementation of cyber security standards and controls to treat or minimise the residual risks that have been identified by the Business Owner. The ITSA ensures that these requirements are communicated to the Project Manager(s) and embedded in project requirements.
Application Developers	Application Developers may be internal to agencies or a third party (i.e. external provider). In either case, application developers are responsible for meeting the requirements outlined in this standard.
Business Owners	Business Owners are responsible for conducting risk assessments and establishing and documenting risk profile prior to development being undertaken. Also responsible for classifying information stored and processed by web applications.
Project Managers	Project Managers of projects that introduce or modify web applications are responsible for the adoption of this standard in their projects.

References and links

- Information Privacy Principles Instruction
- Information Security Management Framework
- ISO/IEC 27002:2006, Standards Australia
- AS/NZS ISO/IEC 27001:2006, Standards Australia
- Key words for use in RFCs to Indicate Requirement Levels, Bradner, Scott, RFC 2119, Harvard University, March 1997.

Document Control

ID	DPC/S4.14
Version	1.3
Classification/DLM	Public-I1-A1
Compliance	Required
Original authorisation date	July 2014
Last approval date	February 2019
Next review date	February 2020

Licence

Appendix 1 – Web application coding checklist

The following checklist provides specific guidance for the secure coding of web applications.

These requirements directly extend standards area 0 Development.

Input validation

	Requirement		References	Check
A1	All client provided data (including query strings, cookies, HTTP header content, SOAP and other web services requests, automated post-back content, and redirected content) has been validated before processing.	Required	ISMF Standard 104 AS/NZS ISO/IEC 27002 12.2.1	
A2	All data has been encoded with a common character set (canonicalised) prior to validation.			
A3	All input validation is conducted on a trusted system (i.e. server-side, not client-side).			
A4	All input has been validated for expected range, length, format and data type.			
A5	All input has been validated against a “white list” of allowed characters (e.g. using regular expressions). In situations where a “white list” filter has not been used, all input has been validated against a “black list” filter to block any potentially hazardous characters. Examples of common hazardous characters include: < > “ ‘ ( ) & + \ \’ \” Null bytes (%00) New line characters (%0d, %0a, \r, \n) Path alteration characters (../ or ..\)			
A6	All input has been validated to ensure there has been no cross-site scripting forgery.			

Output validation

	Requirement		References	Check
A7	All untrusted output (e.g. input provided by users either directly or indirectly via another application) has been encoded before it is returned to the client (e.g. using .NET HtmlEncode/UrlEncode, Apache Jakarta Commons Lang Package).	Required	ISMF Standard 107 AS/NZS ISO/IEC 27002 12.2.4	
A8	All encoding occurs on a trusted system (i.e. server-side instead of client-side).			

Authentication and identity management

	Requirement		References	Check
A9	Users are identified with a unique user ID, and avoid the use of shared or group accounts, dependent on data classification.	Required	ISMF Standard 94 AS/NZS ISO/IEC 27002 11.5.2	
A10	Users are provided with a mechanism for selecting their own passwords.	Required	ISMF Standard 95 AS/NZS ISO/IEC 27002 11.2.3	
A11	Password length and complexity requirements are enforced for new passwords and password resets as stipulated in applicable agency Password Standards.	Required	ISMF Standard 95 AS/NZS ISO/IEC 27002 11.2.3	
A12	Authentication controls are enforced on a trusted system (i.e. server-side instead of client-side).	Required	-	
A13	High value transactions utilise message integrity checks to ensure that data has not been modified by an unauthorised party.	Recommended	-	
A14	Passwords are stored using cryptographically strong one-way hashes (e.g. ASP.NET hash setting).	Required	-	
A15	Existing password and authentication mechanisms (e.g. ASP.NET membership providers) are used instead of custom-developed authentication mechanisms.	Required	ISMF Standard 95 AS/NZS ISO/IEC 27002 11.2.3	
A16	Generic responses are returned for all authentication failures such that they do not indicate which part of the authentication data was incorrect.	Required	-	
A17	All passwords and authentication tokens are sent over an encrypted connection (e.g. SSL). Temporary passwords (or links to temporary passwords) are an exception, which may be transmitted unencrypted.	Required	ISMF Standard 109 AS/NZS ISO/IEC 27002 12.3.1	
A18	If temporary passwords (or links to temporary passwords) are used, the following are enforced: • a short expiration time • password change on first use.	Recommended	ISMF Standard 95 AS/NZS ISO/IEC 27002 11.2.3	
A19	Passwords on the user’s screen are obscured so that they cannot be viewed by ‘shoulder surfing’.	Required	ISMF Standard 95 AS/NZS ISO/IEC 27002 11.2.3	
A20	Password caching or auto-complete features are disabled, e.g. the auto-complete attribute is set to the value ‘off’.	Required	-	
A21	For critical, sensitive or high value transactions, users are required to re-authenticate or multi-factor authentication is enforced prior to performing the transaction.	Recommended	ISMF Standard 94 AS/NZS ISO/IEC 27002 11.5.2	

Access controls

	Requirement		References	Check
A22	The application operates on the principal of “least privilege” (i.e. the user or service account assigned the minimum level of access to perform the task).	Required	ISMF Standard 99 AS/NZS ISO/IEC 27002 11.6.1	
A23	Role-based access controls are designed to ensure consistent access levels for job or role are applied for user access.	Recommended	-	
A24	Any uses of the “super user” or privileged accounts are restricted to agency-controlled networks only.	Required	ISMF Standard 78 AS/NZS ISO/IEC 27002 11.2.2	
A25	Authorisation controls are enforced on every request to the application, including those made by server-side scripts and requests from rich client-side technologies like AJAX and Flash.	Required	-	
A26	Restrict access to all resources (including files, protected URLs, protected functions, services and application data) to authorised users.	Required	-	
A27	Where long-term authentication sessions are allowed, authorisation is periodically re-validated to ensure that privileges have not changed, and if they have, force the user to logout and re-authenticate.	Recommended	-	

Cookies and session management

	Requirement		References	Check
A28	Web platform session management mechanisms are used where possible, instead of custom-developed mechanisms.	Recommended	-	
A29	Logout mechanisms are available to users from all screens that are protected by authorisation to terminate the associated session or connection.	Required	-	
A30	Session inactivity timeouts are configured to be as short as practical, with consideration of risk and business functional requirements.	Required	ISMF Standard 97 AS/NZS ISO/IEC 27002 11.5.5	
A31	Persistent authentication sessions or cookies are disallowed.	Required	-	
A32	All data is stored in session variables instead of client-side cookies.	Required	-	
A33	The “Secure” and “HttpOnly” attributes are set on all session cookies.	Required	-	
A34	All session identifiers and cookies are sent over encrypted connections.	Required	-	

A35	Session identifiers and cookies are never sent to the web server as HTTP GET parameters.	Required	-	
A36	A new session identifier must be created when a user logs on.	Required	-	

File management

	Requirement		References	Check
A37	Cryptographic mechanisms are used in accordance with the applicable agency Cryptographic Standards.	Required	ISMF Standard 109 AS/NZS ISO/IEC 27002 12.3.1	
A38	All hard-coded passwords from source code have been removed.	Required	-	
A39	Cached and temporary copies of sensitive data stored on the server are protected from unauthorised access, and such files are purged as soon as they are no longer required.	Required	-	
A40	All sensitive information is encrypted when it is stored.	Recommended	ISMF Standard 109 AS/NZS ISO/IEC 27002 12.3.1	
A41	Server-side source code is protected from being downloaded by unauthorised users.	Required	-	
A42	Security-relevant data (e.g. passwords, connection strings) are stored server-side rather than client-side.	Required	-	
A43	Client-side caching is disabled on pages containing sensitive information (e.g. using “Cache-Control: no-store” and “Pragma: no-cache” headers).	Required	-	

Logging and auditing

	Requirement		References	Check
A44	All of the following events are logged: functions on user accounts/records • input validation failures • authentication attempts • access control failures • tampering events • attempts to connect with invalid/expired session tokens • system and communication exceptions.	Required	ISMF Standard 71 AS/NZS ISO/IEC 27002 10.10.1	
A45	Logging information is stored in a format that can be easily interrogated.			
A46	Log files are retained in accordance with the applicable agency Standards.			

A47	Access to logs is restricted to only authorised individuals.			
A48	Sensitive information is not stored in logs.			
A49	At a minimum, all logged audit events should record: Date and time of the event Subject identity (e.g. user identification or IP address) Event type identification/description			

Error handling

	Requirement		References	Check
A50	Sensitive information including system details, session identifiers and account information in error responses is withheld from error pages.	Required	-	
A51	Generic error pages and global handlers are used to catch unhandled exceptions.	Required	-	