auDA PUBLISHED POLICY

Policy Title: auDA INFORMATION SECURITY STANDARD (ISS) FOR ACCREDITED REGISTRARS
Policy No: 2013-03
Publication Date: 17/10/2013
Status: Current

1. BACKGROUND

1.1 The auDA Information Security Standard (ISS) forms part of auDA's Registrar Accreditation Criteria (2013-04) and compliance is mandatory for all auDA accredited registrars. The ISS was developed in consultation with registrars and other industry participants through the 2012 Industry Advisory Panel, and was approved by the auDA Board in February 2013.

2. TERMINOLOGY

2.1 This policy uses the following terms:

a) "ISS Assessment Procedures" means the assessment procedures to be followed by the ISS Assessor, available on the ISS Compliance Portal;

b) "ISS Assessor" means an assessor nominated by auDA to provide ISS assessment services;

c) "ISS Committee" means the committee of senior representatives from auDA and AusRegistry and an independent person, responsible for making the final decision on ISS compliance, on the recommendation of the ISS Assessor;

d) "ISS Compliance Certificate" means the certificate issued to the registrar by the auDA ISS Committee;

e) "ISS Compliance Mark" means the mark made available by auDA for ISS compliant registrars to display on their website if they wish; and

f) "ISS Compliance Portal" means the online portal used by registrars to manage their ISS compliance and assessment (also referred to as the TruComply portal).

3. OBJECTIVES OF THE ISS

3.1 auDA's objectives in introducing the ISS are:

a) to encourage and assist registrars to manage and improve the security and resiliency of their own businesses; and

b) to protect .au registrants, and the overall integrity and stability of the .au DNS.

4. OVERVIEW OF THE ISS

4.1 The ISS is at Schedule A of this document. It provides a set of technical, operational and policy requirements designed to protect the confidentiality and integrity of sensitive domain-related data held by registrars.

4.2 Section 3 of the ISS defines 15 Information Security Controls, as follows:

a) Information Security Policy
b) Information Security Organisation Framework
c) Asset Management Plan
d) Human Resources
e) Physical Security Plan
f) Operations Management
g) Service Provider Security
h) Malicious Code and Vulnerability Management
i) Monitoring Controls
j) Access Controls
k) Systems Development
l) Cryptographic Controls
m) Incident Management
n) Business Continuity Management
o) Regulatory Compliance

4.3 auDA recognises that not all registrar business models operate in the same way and accordingly, not all registrars will be required to implement all of the Information Security Controls listed above. It is up to each registrar to conduct their own risk assessment in order to guide the implementation of the ISS within their own business model.

5. ISS COMPLIANCE PROGRAM

5.1 auDA has engaged Vectra Corporation to provide assessment services for the ISS Compliance Program. auDA will bear all costs of the ISS compliance program[1].

5.2 The ISS Compliance Program comprises two assessment processes:

a) registrar self-assessment through the online ISS Compliance Portal; and

b) on-site assessment by the ISS Assessor.

5.3 All registrars will be provided with an ISS Compliance Portal account to manage their ISS compliance and assessment. The ISS Assessment Procedures and related documentation and support information is available on the ISS Compliance Portal.

Initial ISS compliance

5.4 Registrars must complete the self-assessment process through the ISS Compliance Portal, and then notify auDA that they are ready for the on-site assessment. auDA will arrange for the on-site assessment to take place as soon as possible, having regard to the registrar's location and other resource or logistical considerations.

5.5 The ISS Assessor will conduct the assessment in accordance with the ISS Assessment Procedures. If the assessment report is compliant, then it will be provided to the auDA ISS Committee for sign-off. On sign-off, the ISS Committee will issue the registrar with an ISS Compliance Certificate. Registrars may choose to display the ISS Compliance Mark on their website if they wish.

5.6 If the assessment report is non-compliant, the registrar will be given 3 months for remediation and revalidation of all open items. If the registrar does not remediate and revalidate all open items to the satisfaction of the ISS Assessor within 3 months, then the ISS Assessor will provide the auDA ISS Committee with a non-compliant report. The consequences of non-compliance are outlined in section 6 below.

[1] Not including: 1) internal costs for registrars in meeting the ISS, and 2) travel expenses for an ISS Assessor to conduct an on-site assessment for new registrar applicants who are overseas-based.

Subsequent ISS compliance

5.6 Registrars must complete the full ISS Compliance Program (as described in paragraphs 5.2-5.6 above) every 3 years. Registrars may also be required to undertake one or both of the assessment processes of the ISS Compliance Program annually or at other intervals as determined by the ISS Committee, to ensure that they remain ISS compliant during the 3 years.

5.7 In addition, auDA may require a registrar to undertake one or both of the assessment processes of the ISS Compliance Program in the following circumstances:

a) Change of registrar ownership or effective control: Under the Registrar Agreement, a change of ownership or effective control of a registrar requires the prior written consent of auDA. auDA will determine on a case-by-case basis whether the proposed change requires the registrar to undertake any ISS assessment prior to auDA's consent being granted;

b) Security breach: Under the Registrar Agreement, registrars are required to notify auDA immediately if there is a security breach affecting any part of their their systems. auDA will determine on a case-by-case basis whether the registrar is required to undertake any ISS assessment as a consequence of the security breach; and

c) Formal complaint to auDA: If auDA receives and investigates a formal complaint that a registrar is not (or may not be) ISS compliant, and auDA upholds the complaint, then auDA will require the registrar to undertake one or both of the assessment processes of the ISS Compliance Program.

6. CONSEQUENCES OF NON-COMPLIANCE WITH ISS

6.1 Pursuant to paragraphs 5.4-5.7, if a registrar:

a) fails to complete either of the assessment processes, including the 3 month remediation phase, of the ISS Compliance Program; or

b) having completed the ISS Compliance Program, including the 3 month remediation phase, is assessed as non-compliant by the ISS Assessor and the ISS Committee;

then auDA reserves the right to:

c) suspend the registrar's accreditation until the registrar has been issued with a current ISS Compliance Certificate by the ISS Committee; and/or

d) post a notice on the auDA website, and require the registrar to post a notice on their own website, that the registrar is non-compliant, until the registrar has been issued with a current ISS Compliance Certificate by the ISS Committee.

6.2 If the registrar has not been issued with a current ISS Compliance Certificate within 3 months of being suspended, then auDA reserves the right to terminate the registrar's accreditation for breach of this policy, auDA's Registrar Accreditation Criteria (2013-04) and the Registrar Agreement.

7. ISS PHASE-IN PERIOD FOR EXISTING ACCREDITED REGISTRARS

7.1 Existing accredited registrars as at the Publication Date of this document must be issued with an ISS Compliance Certificate within 24 months of the Publication Date (ISS phase-in period). During the ISS phase-in period, auDA will maintain a list of ISS compliant registrars on its website and registrars may choose to display the ISS Compliance Mark on their website if they wish.

7.2 If an existing registrar has not been issued with an ISS Compliance Certificate before the end of the ISS phase-in period, then auDA reserves the right to suspend the registrar's accreditation until they have been issued with an ISS Compliance Certificate. If the registrar has not been issued with an ISS Compliance Certificate within 3 months of being suspended, then auDA reserves the right to terminate their accreditation for breach of this policy, auDA's Registrar Accreditation Criteria (2013-04) and the Registrar Agreement.

7.3 The ISS phase-in period does not apply to new applicants for registrar accreditation. From the Publication Date of this document, new applicants must achieve ISS compliance during their 12 month provisional accreditation or they will not be granted full accreditation.

8. REVIEW OF ISS

8.1 From time to time, auDA may update this document for the purposes of clarification or correction.

8.2 auDA will conduct a full review of the ISS following the ISS phase-in period for existing registrars (ie. 24 months from the Publication Date of this document).

SCHEDULE A

auDA INFORMATION SECURITY STANDARD (ISS) FOR ACCREDITED REGISTRARS

1. BACKGROUND

1.1 auDA

.au Domain Administration Ltd (auDA) is the policy authority and industry self-regulatory body for the .au domain space and was formed to provide a market driven self-regulatory regime.

auDA was formed in April 1999 and in December 2000 received formal endorsement from the Australian Federal Government.

1.2 Registrars

Registrars are organisations accredited by auDA to provide services to people who want to register a new domain name, renew their existing domain name, or make changes to their domain name record.

1.3 Information security responsibilities

The Registrar Agreement between auDA and Registrars, requires that Registrars be responsible for information security. In particular Registrars are required to:

- Take all reasonable or prudent actions to preserve the confidentiality and security of all Registrant Data.
- Have adequate capability for providing information security procedures to prevent system hacks, break-ins, data tampering and other disruptions to its business.
- Promote and protect the stability and integrity of the Australian DNS.
- Ensure the effective and efficient operation of the domain name registration system.

1.4 auDA Information Security Standard (ISS)

A practical set of controls is required to manage information security risks at Registrars.

The ISS sets a baseline for information security for Registrars. The ISS is aligned to well-established international security standards that have matured over time in line with emerging information security threats. Organisations, including Registrars, conducting business activities in a responsible manner, should already be familiar with the concepts of the ISS.

auDA recognises that not all Registrar business models operate in the same way and accordingly the ISS can be adapted to suit individual Registrar business operating models.

The ISS is intended to assist registrars to manage and improve the security in their own businesses in a way that also protects the integrity and stability of the .au domain space. auDA requires that all Registrars deploy and maintain the ISS.

auDA also requires that Registrars who use third party service providers (eg. for IT support, software development or hosting) also meet the ISS. In cases where Registrars use third party service providers, the Registrar must demonstrate how those service providers comply with the security controls in this standard.

Registrars, whose business model facilitates the sale of and administration of domain names to resellers, are required to provide facilities in a manner that meets the ISS.

1.5 Provision for in-place information security certifications

The auDA recognises that some Registrars may already have relevant information security certifications[2] in place.

auDA will, through the services of its nominated ISS assessment services provider, work with the Registrar to confirm that in-place certifications meet the requirements of the auDA ISS.

2. ISS REQUIREMENTS

2.1 Information security definition

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk and maximise return on investments and business opportunities.

The ISS defines Information Security in terms of **key concepts** and **key characteristics**.

Key Concepts

Concept	***Description***
Confidentiality	Preventing disclosure of information to unauthorised systems or individuals
Integrity	Preventing unauthorised or accidental modification of data
Availability	Ensuring that information is available when required

Key Characteristics

Characteristic	***Description***
Authenticity	Ensuring that data, transactions, communications or documents (electronic or physical) are genuine and ensuring that parties involved in communication are who they claim to be
Non-Repudiation	Ensuring a party conducting an action is not able deny having conducted that action

2.2 Business context

The Registrar will document the following in terms of the definition of Information Security provided above:

- Describe the importance of information security taking into account the organisation, its location, its assets, its technology and its culture.
- Describe the scope and boundaries of the information security systems. At a minimum, Registrars must protect their systems in line with the security requirements in this standard.
- Describe the approach in determining and establishing security requirements.
- Describe the methodical assessment of security risks including the risk assessment approach and methodology used (Risk Management Framework) and the criteria for accepting risks. The risk assessment process must define who signs off the risk assessment.
- Describe the selection of controls in a risk treatment plan and how they are used to treat risks.
- Describe how security is organised in the organisation, including roles and responsibilities. (Who makes what decisions? Who approves what?)
- List the documentation set that describes security in the organisation. (Security documentation register.)
- Describe document control, creation and approval.

[2] Examples include AS/NZS 27001 and/or PCI DSS

2.3 Development process

The diagram (Figure 1) shows the typical process a Registrar will need to go through in order to produce the ISS documentation. The steps are shown on the left and the outputs are shown on the right.

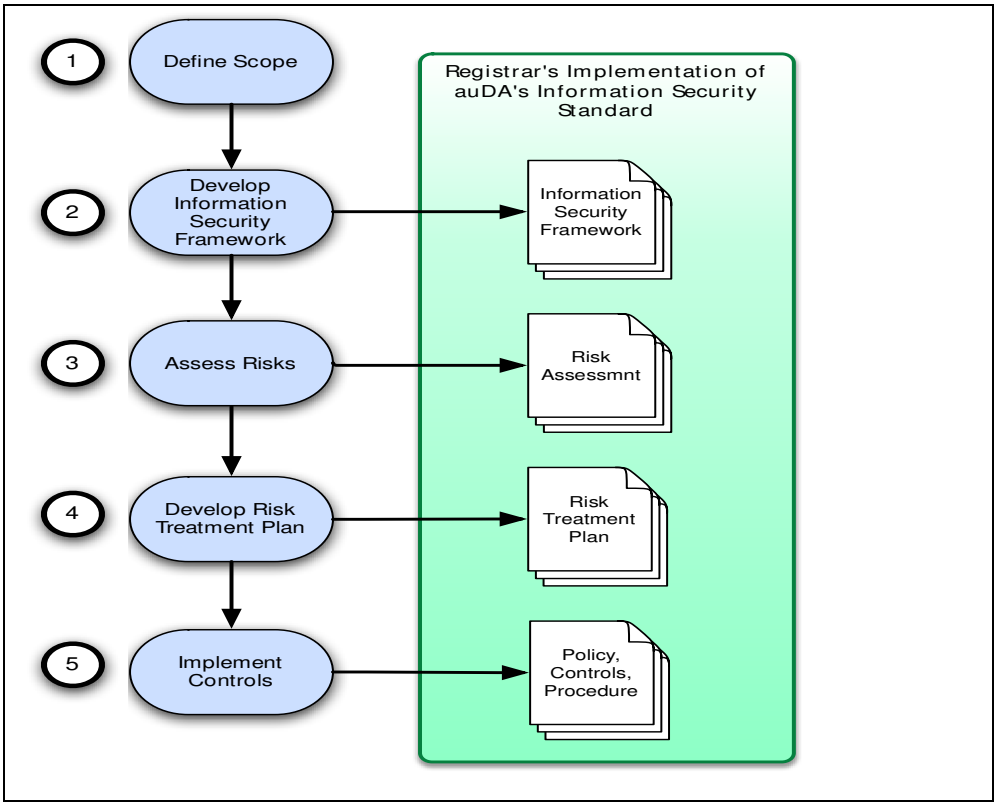

Figure 1 - Typical Development Process for ISS at Registrar

3. INFORMATION SECURITY CONTROLS

As a result of the risk assessment, the risk treatment plan and the Registrar business model, the Registrar must select applicable information security controls from the list of controls below. The Registrar must provide an explanation for any controls that are excluded.

The Registrar will implement security controls as they apply to business operations. For example: if a Registrar does not develop its own software, but outsources development to a third party service provider, the Registrar will not need to implement its own security controls for software development, but must ensure that the third party service provider does. The security control in such a case would be contained in the service agreement with the third party service provider.

3.1 Information Security Policy

The Registrar will produce, publish and maintain an Information Security Policy that demonstrates management commitment supporting information security in accordance with business requirements, laws and regulations.

The information security policy must be:

- approved and authorised by senior management;
- reviewed at least annually or if significant changes occur; and
- made available to and communicated to employees and external parties where relevant.

The information security policy must address the following:

- define information security, its objectives and its importance to the business;
- management's commitment supporting the goals of information security from a business context;
- the framework for evaluating and managing risk;
- accountability and responsibility for information security;
- security education, training and awareness requirements;
- business continuity management;
- consequences for policy breaches; and
- the requirement to comply with relevant legislative, regulatory and contractual obligations.

3.2 Information Security Organisation Framework

The Registrar will document and maintain an Information Security Organisation Framework that describes how information security is managed within the organisation and external to the organisation.

The framework must address the following:

- management's commitment to information security through acknowledgement and assignment of information security responsibilities;
- coordination of information security activities, functions and relevant roles by representatives within the organisation;
- information security accountability, responsibility and delegation;
- identification and management of risks related to information processing services offered or tendered by external parties;
- identification of security requirements relevant to customer access and customer information; and
- contacts with authorities (eg. Federal Police).

3.3 Asset Management Plan

The Registrar will document and maintain an Asset Management Plan that describes how organisational assets are identified, categorised and afforded appropriate protection.

The plan must address the following:

- description of how assets are identified;
- up-to-date list of important assets[3] (these are the assets that need protection within the framework of this security standard, including databases, contracts, service agreements, relationships);
- description of who owns the assets, or how ownership is determined;
- description or policy on acceptable use of assets (employees, contractors need to know what the acceptable use of these assets are); and
- information classification (How do employees and contractors identify the value of information and how are they meant to protect that information? Eg. Confidential, Public, Secret).

[3] Registrars should not only consider traditional fixed assets, such as computers and databases. Consider important assets in the context of the business, such as suppliers. Consider what could happen to those suppliers (the relationship, viability, trustworthy, responsiveness, etc.)

3.4 Human Resources

The Registrar will document and maintain an employee management process that describes how candidates for employment are assessed.

The process must include the following:

- background verification checks;
- description of security roles and responsibilities for the job role;
- information security responsibilities in Terms and Conditions of employment
- information security awareness education;
- disciplinary process in the event of committed security breaches; and
- responsibilities in the event of termination or change of employment conditions (including removal of access rights and return of assets).

3.5 Physical Security Plan

The Registrar will document and maintain a physical security plan commensurate with identified risks that describe how important information processing equipment and services are protected by defined security perimeters and controls.

The plan must include the following:

- physical security arrangements (barriers, entry/exit controls) that protect information processing facilities;
- protection against environmental threats (fire, flood, civil unrest, power failures);
- equipment maintenance;
- security of network cabling;
- security of equipment taken off site (include authorisation and tracking process); and
- secure disposal of equipment (removal of sensitive data).

3.6 Operations Management

The Registrar will document and maintain a communications and operations manual that describes how the information processing facilities and managed and maintained.

The operations manual must include the following:

- scheduling requirements (batch jobs, patching, backups etc);
- error handling procedures and support contacts;
- escalation procedures;
- system recovery and restart procedures;
- audit logs for tracking purposes;
- change management procedures;
- segregation of duties (prevention of unauthorised modifications);
- description of separation of development, test and production environments (if Registrar performs development);
- system planning and acceptance;
- media handling;
- exchange of information with external parties; and
- capacity management.

3.7 Service Provider Security

The Registrar will document and maintain a process for tracking agreements with third party services providers to ensure the security of services.

The process must include the following:

- agreed security controls;
- service definitions and delivery levels;
- monitoring requirements and expectations (eg. reports and audits); and
- managing changes to services and/or requirements.

3.8 Malicious Code and Vulnerability Management

The Registrar will document and maintain controls to protect against malicious code and vulnerability management.

The controls must include the following:

- formulation of a policy (or policy statement) against using/installing unauthorised software;
- measures in place to scan files for malicious content obtained from external sources;
- additional measures in place to protect system user's equipment who have administrative access to critical assets;
- roles and responsibilities for vulnerability monitoring compared against asset configuration database (inventory);
- applying patches roles and responsibilities – if patches are available, assessment of the risks of patching and/or not patching;
- external (and potentially internal) vulnerability scans of Internet-facing environments and associated processes for ensuring that open vulnerabilities are addressed; and
- business continuity plans for recovering from malicious code attack or errors resulting from vulnerabilities.

3.9 Monitoring

The Registrar will document and maintain a system for recording information security events in order to detect unauthorised information processing activities.

The system must include the following:

- an audit logging system recording user activities, exceptions and information security events for an agreed time period (no less than six months unless justification is provided for a smaller period);
- audit information that can trace:
    - user ID and location of user (network address)
    - date and time of event
    - use of privileges (admin, root, su, sudo etc)
    - de-activation and activation of protection systems (e.g. Anti-virus or IDS/IPS)
    - systems usage;
- mechanisms that protect audit log information;
- a mechanism whereby all critical system clocks are synchronised with an accurate time source; and
- file integrity monitoring – monitoring of files that should not change.

3.10 Access Control

The Registrar will establish and publish an access control policy and related procedures.

The access control policy must include the following:

- the requirement for access to information on a 'business-needs-to-know' basis;
- requirement for role based access;
- requirement for privileged access to be restricted to non-internet facing interfaces;
- formal authorisation requests for access to information;
- periodic review of access rights and access controls;
- removal of access rights when roles change, upon dismissal and/or resignation; and
- minimal access per role (ie. default deny all, access based on expressly defined rules).

The access control procedures must include the following:

- user access management procedures for user registration;
- unique IDs for users (no using redundant user IDs);
- removal of users when roles change, upon dismissal and/or resignation;
- users to sign statements indicating their understanding of conditions of use;
- privilege management – use appropriate accounts for appropriate functions (don't use admin accounts for normal day-to-day use);
- password management
    - keep passwords confidential
    - no shared user accounts
    - change passwords on first use
    - passwords not displayed in the clear on screens
    - passwords may not be stored or transmitted in the clear
    - default (vendor) passwords to be changed
    - admin passwords to be changed when admin staff leave
    - passwords to be changed at agreed times based on risk profile
    - password length and complexity and history to be based on risk profile (minimum requirement: length at least 8, history at least 4, complexity to include uppercase and lowercase and at least 1 numeric);
- process for reviewing access rights and access controls;
- protection of unattended equipment (screen saver with password and session time outs); and
- conditions and required security practices under which remote access is permitted.

3.11 Systems Development

The Registrar will establish and publish information systems acquisition, development and maintenance processes and procedures to ensure that security forms an integral part of all information systems.

The process and procedures must include the following:

- determination of security requirements based on business requirements for new systems or changes to existing systems. Systems include operating systems, infrastructure, applications, purchased off-the-shelf software and services and in-house developed applications;
- checking and validating the correct (expected) processing in applications prior to being promoted to production environments. Checks could include: code reviews and application code software checks, penetration testing, testing of use defined use cases, data validation, memory usage, internal processing, message integrity, file updates and patching;
- protection of source code and test data;
- process defining system release cycles and notifications;
- processes describing development, test and production environments;
- formal change control procedures;

- data loss prevention or information leakage procedures;
- where software development is outsourced, controls covering: licensing, ownership, intellectual property rights, quality assurance, escrow, audit rights, security functionality and testing; and
- configuration standards that address known security vulnerabilities and that are consistent with industry-accepted system hardening standards, including the minimal set of services required for system components and the removal of all non-essential services.

3.12 Cryptographic Controls

The Registrar will establish and publish cryptographic controls for protecting the confidentiality, authenticity and integrity of information.

The cryptographic control must include the following:

- a policy (or policy statement) on the use of cryptographic controls. Consider, general principles for protecting sensitive information, type and strength of algorithms v/s sensitivity of information; and
- procedures dealing with key management, roles and responsibilities, and development and maintenance of standards.

3.13 Incident Management

The Registrar will establish and publish a formal event reporting and escalation procedure to ensure that information security events are communicated in a timely manner.

The event reporting procedure must include the following:

- the formal appointment of a point-of-contract for reporting security events to, who is known throughout the organisation and who is always available and able to provide appropriate advice;
- the requirement for employees and contractors to note and report security events or security weaknesses;
- established management responsibilities for ensuring timely, orderly and effective response to incidents, including: classification of incidents, contingency plans, reporting to relevant authorities, evidence collection and recovery from failures;
- processes for learning from incidents and implementing corrective/preventive actions to prevent similar occurrences; and
- the requirement to immediately notify the relevant authorities and regulators including auDA and AusRegistry.

3.14 Business Continuity Management

The Registrar will establish and publish a business continuity management plan that includes information security requirements in order to counteract interruptions to business activities in the event of failures to information systems or disasters.

The business continuity management plan must include the following:

- identification of information and services at risk. Must include information not held in the Registry database;
- consideration of information security and associated events as part of the overall business continuity plan (a single business continuity planning framework);
- identification of potential events, including probability and impact, that can cause interruptions to business processes;
- processes for restoration of information services to required levels within defined time limits; and
- periodic testing and updating of the plan.

3.15 Regulatory Compliance

The Registrar will identify and document into a register all relevant statutory, regulatory and contractual requirements in order to avoid relevant information security breaches.

The regulatory compliance register must include the following:

- compliance relating to intellectual property rights;
- compliance relating to protection of company records (eg. accounting, database, audit logs, transaction logs, operational procedures);
- compliance relating to the retention of records; and
- compliance relating to protection and privacy of personal information.