

2012 INDUSTRY ADVISORY PANEL

ISSUES PAPER – JUNE 2012

BACKGROUND

In February 2012 the auDA Board established the Industry Advisory Panel to:

- review the structure and regulation of the Australian domain name industry; and
- provide recommendations to the auDA Board about what changes (if any) should be made to the competition model.

The Panel is considering the following issues:

- The method of 2LD registry operator selection/appointment post-2014.
- The policy and process for registrar accreditation.
- Registrar security.
- The status and regulation of resellers.
- The policy and process for registrar transfers.
- The status and operation of the .au Domain Name Suppliers' Code of Practice.

Full text of the Panel's Terms of Reference, a list of Panel members and Minutes of Panel meetings to date are available on the auDA website at:

<http://www.auda.org.au/2012iap/2012iap-index/>

PUBLIC CONSULTATION

The Panel is required to undertake at least two rounds of public consultation, to ensure that its recommendations to the auDA Board have been properly canvassed with, and informed by, key stakeholders and the general community.

This Issues Paper reflects the general discussion by the Panel of the main issues under consideration. The purpose of the Issues Paper is to set out the current situation and canvass the issues and possible options for change that the Panel has identified in its deliberations to date.

Following this first phase of consultation, the Panel will publish its draft recommendations for further public comment before providing its final report to the auDA Board.

SUBMISSIONS TO THE PANEL

If you would like to comment on the issues discussed in this paper, please send your submission to:

auDA 2012 Industry Advisory Panel
Email: paul.szyndler@auda.org.au
Fax: 03 8341 4112

Electronic submissions are preferred. All submissions will be posted to the auDA website within 2 working days of receipt, unless clearly marked confidential.

Alternatively, respondents may wish to complete an online survey at: <http://www.surveymonkey.com/s/KXH7J36>

A compendium of survey responses will be published on the auDA website at the close of the public consultation period.

The closing date for all submissions and survey responses is **Friday 20 July 2012**.

GLOSSARY

<i>Term</i>	<i>Definition</i>
2LD	Second Level Domain, ie. a name at the second level of the .au domain name hierarchy (eg. com.au)
3LD	Third Level Domain, ie. a name at the third level of the .au domain name hierarchy (eg. domainname.com.au)
auDA	.au Domain Administration Ltd – the .au domain administrator
auDA ISS	auDA Information Security Standard (proposed)
ccTLD	Country Code Top Level Domain (eg. .au, .uk)
Domain monetisation	Registering a domain name in order to earn revenue from click-through advertising
DNS	Domain Name System
EOI	Expression of Interest
ICANN	Internet Corporation for Assigned Names and Numbers – the global DNS administrator
ICAP	auDA's Industry Competition Advisory Panel
gTLD	Generic Top Level Domain (eg. .com, .biz)
Registrant	An entity or individual that holds a domain name licence
Registrar	An entity that registers domain names for registrants and is accredited by auDA
Registry operator	An entity that maintains the authoritative 2LD name servers and the database of domain name registrations
Reseller	An entity that acts as an agent for a registrar
RFP	Request for Proposals
RFT	Request For Tender
RLA	Registry Licence Agreement

COMPETITION OBJECTIVES

The Panel notes that auDA has an overarching responsibility to ensure the security and stability of the .au DNS, and it also has certain constitutional obligations with respect to both supply and demand sides of the industry. Within this context, the Panel believes that the Australian domain name industry structure and competition model should aim to achieve the following outcomes:

- continuity and certainty of DNS service provision
- level-playing field for domain name suppliers
- low pricing, at wholesale and retail levels
- consumer choice
- consumer protection.

The current industry structure is based on a three-step supply chain – registry, registrar and reseller – with competition occurring to varying degrees at each step. A consideration for the Panel is whether the costs of providing competition at each step outweigh the public benefits to be gained.

At this early stage in the Panel's work, the general view among Panel members is that the current model is working well and delivering value to industry participants and consumers alike. However, as outlined in the Discussion of Issues below, there are aspects of the model that the Panel believes could be refined to better meet auDA's responsibilities and the needs and expectations of industry participants and the broader Australian Internet community.

DISCUSSION OF ISSUES

1. The method of 2LD registry operator selection/appointment post-2014

Current situation

The .au domain is divided into a number of different second level domains (2LDs) (eg. com.au, org.au, gov.au etc). While auDA has direct technical management and control of the .au TLD, the 2LDs are run by a separate, private registry operator. This is in contrast to the approach of many other country code top level domains (ccTLDs), where the domain administrator and the registry operator are one and the same. In .au, it is considered desirable to maintain a clear separation of policy and operations, to ensure that auDA's ability to act as an independent industry regulator is not compromised.

The current .au industry model provides for competition at the registry level in two ways:

- competition in the selection of registry operator(s), through an open tender process
- competition between multiple 2LD registry operators (eg. the registry operator for com.au competing for domain name registration sales against the registry operator for net.au).

While the model provides for multiple 2LD registry operators, the registry tender processes held in 2001 and 2005 demonstrated that a single registry for all current 2LDs was the most efficient option given market conditions at the time.

The current 2LD registry operator, AusRegistry Pty Ltd, holds a Registry Licence Agreement (RLA) with auDA, due to expire on 30 June 2014. Under the RLA, AusRegistry:

- charges a per domain name fee to registrars which varies according to 2LD and includes a reducing sliding scale based on cumulative number of domain names registered in com.au and net.au
- paid a one-off “sign-on” fee on being awarded the licence, and also pays an annual registry licence fee to auDA calculated according to the number of domain names registered in each 2LD.

Issues for consideration

1.1 How to extract the best value for the Australian Internet community, through whichever registry selection mechanism, beyond 2014.

As noted above, auDA has, in the past, undertaken two full public tenders (2001 and 2005) for the execution of the .au registry function. Based upon the recommendations of the 2008 Industry Competition Advisory Panel (ICAP), auDA determined that a re-negotiation of the existing agreement with AusRegistry was the most effective mechanism for ensuring the provision of services through to 2014.

The Panel notes that, whilst competition at the registry level is achieved, in theory, via periodic re-tendering of the registry licence, experience to date shows that the incumbent operator has a clear infrastructure advantage. This is due mainly to the significant capital costs for a new entrant in meeting auDA’s registry technical specification, especially given the requirement for registry operations to be located in Australia.¹

The Panel also notes that there are transition costs for the rest of the industry in switching to another registry operator. Whilst industry participants may be willing to bear some level of cost in order to reap greater benefits in terms of price and service, this is not likely to be the case in the current environment where the performance of the incumbent registry operator is widely well-regarded and .au pricing is largely on par with other TLDs.

With these observations in mind, the Panel has discussed a range of alternative market approaches and their respective pros and cons. These discussions have noted the evolution and growth of the .au marketplace since the last renegotiation (2008) and last tender (2005), and been focussed upon whether the competition model should be modified to ensure that competition objectives at the registry level continue to be met.

.....

¹ While neither political nor policy barriers limit the operation of the .au registry to an Australian company, eligible tenderers must retain an Australian presence through which the .au registry will operated. This is not an arbitrary decision. Rather, [RFC 1591](#) prescribes that: *“The key requirement is that for each domain there be a designated manager for supervising that domain's name space. In the case of top-level domains that are country codes this means that there is a manager that supervises the domain names and operates the domain name system in that country.”*

Request For Tender (RFT)

The Panel understands that the execution of a full RFT process would incur significant costs (both financial- and human resource-related) and may not deliver the greatest efficacy in a depressed or geographically-limited marketplace. However, as it is the most public, comprehensive and thorough mechanism for testing the market, an RFT would provide the greatest assurance and evidence that auDA was meeting its commitment to principles of competition.

Expression of Interest (EOI) or Request for Proposals (RFP)

Alternatives to a full RFT include more graduated market approaches such as an EOI or RFP. Neither process would require auDA to issue a prescriptive statement of service requirements, nor bind auDA to selecting a successful service provider. Both processes are also less cost- and resource-intensive than a full RFT, and would allow respondents to propose creative and unique value-proposition models.

However, both processes are more typically utilised in circumstances where the specifications and work required are unclear, undeveloped or flexible – which is not the case with the .au registry function. Also, if undertaken in advance of an RFT, either of the above approaches may limit auDA's leverage for re-negotiations with AusRegistry, should they result in low, or no, market interest.

On this point, however, the Panel notes that there are some commercial constraints on AusRegistry which would prevent it from seeking to raise its prices unreasonably, for example the risk that high prices would drive registrars and registrants to other comparatively cheaper domain spaces.

One option the Panel has discussed is for auDA to enter re-negotiations with AusRegistry in advance of an announced intention to launch an EOI or RFP. This course of action potentially would allow auDA to derive the best-possible value proposition from AusRegistry, while reserving the right to further test the market in the event that renegotiations fail.

Contract re-negotiation

In 2008 the ICAP considered that the registry marketplace was not expansive enough at that time to warrant another tender process and, as such, recommended a re-negotiation with AusRegistry.

The Panel notes that whilst contract renegotiation would be a commercial matter between auDA and AusRegistry, there are wider implications for the Australian domain name industry and consumers. If it was to recommend contract renegotiation, Panel members would wish to suggest some parameters for negotiation as part of its final report to the auDA Board.

The Panel is aware that, while cost effective, another re-negotiation process would further enshrine the incumbent operator and could raise the possibility of decreasing competitive pricing pressures in the future. To address these problems, the Panel suggests that a recommendation to re-negotiate the contract in 2014 should include the condition that auDA must go to full tender in 2018.

The Panel invites comments on Issue 1.1.

1.2 Pros and cons of maintaining the provision allowing for multiple registries.

The Panel notes that, while the .au competition model has always allowed for the existence of multiple 2LD registry operators, the tender processes in both 2001 and 2005 showed that a single registry for all 2LDs was the most effective option, given prevailing market conditions.

Since 2005, the .au market has grown exponentially. In April 2005, there were 527,000 names registered in .au. By March 2012, total registrations grew to 2.37 million names. While a larger market could possibly accommodate greater diversity in registry operations, a number of factors limit the utility of such an arrangement. Most notably, in 2005, 87% of total names were registered in com.au. Currently, this figure is still at 86%.

The Panel agrees that the dominance of com.au means that it is highly unlikely that registries operating the other 2LDs (approximately 300,000 domain names in total) would be able to maintain a commercially viable operation. Although these 2LDs could be operated on a not-for-profit basis, the limited number of registrations and revenue would likely limit the registry operator's ability to invest in the development and maintenance of technical and customer-facing systems, to the standard required by the RLA. In other words, only the registry operator of com.au would have the resources to maintain, and to a large extent subsidise, the operation of the other existing 2LDs.

Conversely, the retention of policy supporting multiple registries in .au facilitates the possibility of a level of competition beyond that which exists at the registrar level. The removal of this provision could limit flexibility in the future, when many more names are registered in .au and when a greater number of niche registry providers may be operating in Australia (for example following the introduction of new gTLDs). A single registry model could also place constraints upon the likelihood of the introduction of new 2LDs.

Irrespective of the future model, the Panel notes the importance of ensuring that the "closed" 2LDs (edu.au/gov.au/csiro.au) can be catered for – either by a requirement, or option, for the registry operator(s) to include these 2LDs.

After balancing all of these competing tensions, the Panel's preliminary view is that the process for registry selection in 2014 should solicit a single registry provider, though auDA should retain the possibility of multiple registries in future selection processes.

The Panel invites comments on Issue 1.2.

1.3 Possible effect of the introduction of new gTLDs.

ICANN's intention to introduce further new gTLDs has the potential to significantly re-structure the global domain marketplace. ICANN has set a limit of delegating 1000 new gTLDs per year, and has recently reported that it has received approximately 1900 applications for new names, which will be evaluated starting in June 2012. The successful launch of even a small percentage of new gTLDs could significantly expand and dilute the domain name market.

As mentioned above, it is possible this development will facilitate the creation of registry operators that leverage their infrastructure across a number of TLDs, allowing them economies of scale and scope. Some could commence operation in Australia. These operators could specialise in brand, geographic, or community-based TLDs, and could position themselves to apply to operate .au 2LDs that currently appear economically unviable.

Alternatively, the new gTLDs process could result in a substantial failure rate and the subsequent recovery of failed registries by established operators could serve to consolidate current market share levels.

It is also worth noting that, of the known Australian-based gTLD applications, the .sydney, .melbourne, .afl TLD registry operators are all clients of ARI Registry Services, a wholly owned subsidiary of AusRegistry.

In summary, the Panel believes that the introduction of new gTLDs may have some future effect on the .au marketplace, registry and registry competition, particularly if some new gTLDs are Australian-based. However, this is too great an unknown at this stage, and cannot practically impact upon current policy development deliberations.

The Panel invites comments on Issue 1.3.

1.4 Scope of competition amongst potential registry operators in Australia.

The Panel currently believes there is no evidence of pent-up demand for registry competition in .au (ie. potential competitors prevented from competitive access since 2005). Given that the RLA requires the registry operator to maintain a local presence and operate the registry from within Australia, only a limited number of large, international registries would have the resources to establish and manage an Australian operation. However, irrespective of their size, such a development would incur considerable investment and start-up costs that would limit the competitiveness of their tender participation.

The Panel invites comments on Issue 1.4. In particular, the Panel invites potential registry competitors to express their informal interest (either publicly or on an in-confidence basis) in response to this paper.

The Panel invites any other comments or suggestions in relation to the method of 2LD registry operator selection/appointment post-2014.

2. The policy and process for registrar accreditation

Current situation

The current .au industry model allows for multiple registrars who have a direct technical connection to the registry and compete in the marketplace to provide customer sales and support services to registrants. Many .au registrars also operate substantial DNS hosting, web hosting and email hosting infrastructures at high levels of reliability. Domain names are used as identifiers to resources hosted on this infrastructure.

Registrars are accredited by auDA and operate under a Registrar Agreement which requires compliance with auDA policies and an industry Code of Practice. The purpose of the accreditation process is to ensure that registrars are able to perform policy compliance checks on domain name applications and provide adequate customer support services, as well as being able to connect technically and securely with the registry.

Accredited registrars pay an annual fee to auDA of \$3,300, and there is also a \$2,200 non-refundable accreditation application fee and a requirement for \$10,000 opening balance with AusRegistry. Registrars are free to set their own domain name fees to resellers and retail customers; as at April 2012, the registrar retail price of a two year com.au domain name registration ranged from \$24.00 to \$140.00. Notably, this pricing range is similar to April 2008 rates (during the ICAP process). Over the same period, the number of accredited registrars has grown from 27 to 37 and the market share of the top 4 registrars has grown from 60 to 65%.

Issues for consideration

2.1 The current accreditation fees and processes.

The Panel notes that the registrar level is where most competitive market activity and regulation occurs within the current industry structure. When registrar accreditation was introduced in 2002, the main objective was to expedite the effective transition from monopoly to competition. Over the last decade, domestic and global domain name markets have undergone significant changes, which have impacted on the business case for seeking accreditation. With the advent of new gTLDs the marketplace will grow and evolve even further.

Over the same timeframe, registrar fees (\$2,200 application plus \$3,300 annual) have not changed. The Panel understands that these fees do not reflect the actual costs incurred by auDA, which mainly relate to the cost of staffing resources to initially process applications and undertake site inspections, and maintain a registrar liaison and compliance function, in the longer term.

While increasing fees beyond a cost-recovery level would be inconsistent with auDA's not-for-profit status, there may be merit in increasing initial costs to create a more appropriate entry standard. However, the value of doing so must be assessed against the effects on competition that such a change would cause.

The issue of fees is also relevant to the Panel's consideration of the ongoing regulation of registrars, particularly in relation to registrar security (see Issue 3 below). The Panel notes that other tools, such as contractual obligations, the proposed registrar security standard, and expectations regarding registrar insurance,

may prove more effective (than application fee increases) in maintaining high standards of registrar accreditation and performance. The Panel also notes that auDA receives most of its revenue from a fee of \$3.85 (incl GST) for each registered .au domain name. As the volume of .au name registrations continues to increase, additional revenue will be generated that auDA could use to cover additional costs associated with improving the regulation of registrars.

The Panel invites comments on Issue 2.1.

2.2 The accreditation of overseas-based registrars.

Up until 2008, there was no restriction on a foreign company (ie. one that is not located or registered in Australia) becoming an accredited registrar. Concerns were raised by the ICAP that foreign registrars may be unfamiliar with Australian laws and market practices, and their lack of local presence and time zone differences may pose customer service problems. At the time, it was also argued that only Australian entities should be allowed to apply for registrar accreditation, which would be consistent with policy rules that allow only Australian entities to register .au domain names.

In delivering its final report, the ICAP recommended that it would not be appropriate to restrict registrar accreditation to Australian entities. Such a limitation may have had anti-competitive effects and contravened a number of bi-lateral trade agreements. However, the ICAP did recommend that overseas entities should be required to register with the Australian Securities and Investment Commission and the Australian Taxation Office to trade in Australia. This had the effect of making them subject to Australian laws and regulations including the requirement to collect and remit GST subject to turnover. These requirements also meant that overseas registrars had to maintain a local agent.

Since the recommencement of the registrar accreditation process (after implementation of the ICAP's recommendations) a number of international registrars have been accredited. Currently, of the 37 accreditations, six are overseas entities.

The Panel notes that limitations still exist with regards to the accreditation process for foreign entities. Most notably, auDA does not have the resources to undertake site inspections at overseas registrars, unless such a visit may coincide with other staff travel. While many accredited foreign registrars are large entities that operate across a number of domain spaces, they are not currently subject to the same initial scrutiny as local registrars.

The Panel invites comments on Issue 2.2.

2.3 The accreditation of registrars for drop-catching purposes.

In the gTLD space, many registrars hold more than one ICANN accreditation, often for the purpose of maximising their connections to the registry and increasing their chances of picking up domain names as they drop. Some are "private" registrars, which register domain names only for themselves and their associates, and do not offer service to the general public. Others, through the process of acquisitions and market consolidation, have also gained multiple registry connections.

Over the last five years, these business models have appeared in the Australian market. One drop-catching service utilises shared registry connections of six registrars and another utilises three shared connections. In addition, five entities hold more than one registrar accreditation, including one entity which owns seven registrars.

The Panel understands that auDA's current registrar accreditation criteria and process are focussed on ensuring that registrars have adequate systems in place for dealing with customer service, billing, complaints and so on. The accreditation process does not envisage a scenario where the registrar is not selling domain names to the public in the 'normal' way, but is instead using its registry connections solely for the purpose of operating a drop-catching service. This may apply either to a new market entrant, or to an existing registrar seeking to accredit a related entity solely for drop-catching purposes.

Given the existence of drop-catching services in the .au market, the Panel questions whether the registrar accreditation criteria and/or process, including application fees, needs to be modified to accommodate this particular business model. Should the requirements be the same, or more or less onerous than for registrars with a 'normal' business model?

The Panel invites comments on Issue 2.3.

2.4 The requirement for potential registrars to act as resellers for six months or show equivalent experience.

Currently, registrars applying for accreditation must show at least six months' experience as a reseller of an existing registrar. For established local and international registrars, this requirement may be waived if they can demonstrate "an alternative, equivalent level of experience". It should be noted that, for overseas registrars, this includes experience operating in a similarly policy-rich TLD space. auDA also conducts policy examinations in assessing new registrars.

The Panel understands that auDA introduced this requirement in 2004 in order to address problems at that time with some applicants for accreditation having insufficient understanding of the .au regulatory environment. Panel members have questioned whether the requirement is still necessary.

The Panel invites comments on Issue 2.4.

The Panel invites any other comments or suggestions in relation to the policy and process for registrar accreditation.

3. Registrar security

Current situation

Under the Registrar Agreement, all registrars are obliged to immediately give auDA notice of any security breaches affecting any part of their systems. There are currently no other requirements in relation to registrar security.

Issues for consideration

Following a serious security incident involving an accredited registrar in mid-2011, which caused major disruption to registrants and the industry in general, auDA has been working with a group of industry participants to develop the first draft of a proposed mandatory security standard for registrars. This work has now been handed over to the Panel under its Terms of Reference, to enable broader stakeholder input and community consultation.

The draft auDA ISS Compliance Policy – including the draft ISS itself and the draft certification process – is at Attachment A.

The Panel notes that the proposed draft auDA Information Security Standard (ISS) is intended to assist registrars to manage and improve the security of their own businesses in a way that also protects the integrity and stability of the .au domain space. The draft auDA ISS is intentionally flexible, to accommodate a range of registrar business models. It is risk-based, in that it requires registrars to undertake their own risk assessment and select the security controls that are most appropriate for their business.

The draft certification process is designed to help each registrar to achieve certification with as much or as little assistance as they require. Certification assessments will be conducted by auDA's nominated assessor. The intention is that all registrars will be required to undertake full certification assessment every three years, with interim assessments to be conducted annually or as otherwise recommended by the assessor. It is proposed that registrars who fail any of their assessments will have their accreditation suspended, and then terminated if they have not passed their assessment within three months of being suspended.

The Panel is aware that the introduction of a mandatory security standard for registrars would be a 'world-first', and would represent a significant change to the industry – not just for existing accredited registrars but also for prospective applicants for accreditation.

The Panel notes that, while the auDA ISS will be mandatory for accredited registrars, it is flexible enough to apply to other industry participants such as resellers, who may wish to gain certification to improve their own systems and create a point of market differentiation. Similarly, registrars may also choose to apply it to other aspects of their businesses, such as hosting.

The Panel also notes the need to ensure that the auDA ISS does not become a simple compliance exercise, and emphasises the importance of robust enforcement mechanisms and regular reviews to ensure the auDA ISS remains relevant and effective.

The Panel invites comments on Issue 3, as well as any other comments and suggestions in relation to registrar security.

4. The status and regulation of resellers

Current situation

Resellers are not accredited by auDA and do not have a direct technical connection to the registry. Rather, resellers buy domain names and manage domain name records for themselves and/or their customers through an interface with their registrar.

Many resellers will select a registrar to work with in much the same way that a registrant selects a registrar, taking a decision based on factors such as price, customer service, technical systems and other bundled services. These resellers set their own retail prices for customers and simply negotiate a wholesale price from the registrar.

Under the Registrar Agreement, registrars must notify auDA when they appoint a reseller, and must ensure that their resellers comply with auDA policies and the industry Code of Practice under a complaints-based approach. There are currently approximately 4,750 resellers notified to auDA, although this number is thought to be much lower than the number of resellers actually operating in the marketplace.

Issues for consideration

4.1 The definition of “reseller” and mechanisms for identifying as a reseller.

Currently, the Registrar Agreement defines a reseller as:

“a person appointed by the Registrar to sell domain name services and provide customer services to Registrants on behalf of the Registrar”

While this definition is intended to reflect that some registrars may choose to utilise resellers as a sales channel, it does not capture those engaged in activities such as bulk-buying or those that purchase names on behalf of clients and do not identify as agents of the registrar.

The Panel is considering whether the current definition of resellers is accurate and reflective of the marketplace, or whether it should be amended to reflect the activities of others who may be considered “resellers”.

A related matter is how and when an entity is formally recognised as a “reseller”. In the Panel’s initial discussions, it has been noted that many resellers choose to self-identify as such when they commence selling names and enter an agreement with a registrar. However, the Panel also notes that, from an operational perspective, auDA may deem an entity to be a reseller (due to their market activity) and treat them in accordance with reseller policies and principles. Short of entering into a registrar-reseller agreement, none of these are formalised, consistent mechanisms, and the Panel is unclear as to whether this is an issue of concern for auDA, the registry, registrars or resellers themselves.

The Panel invites comments on Issue 4.1.

4.2 The benefits and difficulties associated with a formalised auDA-reseller relationship.

The Panel notes that, while a formalisation of the role of resellers in the .au marketplace may be desirable for many reasons, centralised accreditation would generate significant logistical and staffing overheads for auDA.

Previous panels have considered proposals such as a voluntary “registered reseller program”, under which resellers would choose to pay a fee to register with auDA and in return would receive the following benefits:

- listing in the WHOIS database as the “reseller of record”
- use of an official reseller logo or registered certification mark
- direct contact with auDA, including access to education and training.

Ultimately, these proposals were not advanced, partly because they would require that self-nominating resellers (ie. not all resellers) would be subject to direct regulation by auDA. Legally, this would require auDA to enter into some form of agreement with resellers, similar to the Registrar Agreement.

Currently, reseller-related complaints are dealt with by auDA via their registrar. That is, the registrar is responsible for ensuring that the reseller responds to the complaint and takes any necessary corrective action. The decentralisation of the model allows for more effective compliance and enforcement by auDA and obviates the need for auDA to hold thousands of individual agreements.

However, the current process may also have the effect of isolating resellers. Also, the inclusion of a third party (the registrar) can slow and complicate communications and lessen the effectiveness and promptness of enforcement actions.

The Panel notes that the implementation of any more formal regulatory measures would add costs for resellers, raising the barrier of market entry. It could create a gap between “specially-accredited” and other resellers and would represent a shift in market dynamics.

The Panel invites comments on Issue 4.2.

4.3 The desirability of listing resellers in WHOIS.

Currently, there is no formal listing of resellers in WHOIS, although resellers are permitted to list themselves as the technical contact for a domain name. This can lead to customer confusion, for example when registrants don't recognise the name of the registrar of record for their domain name. In the recent past it has also caused significant difficulties for resellers attempting to manage and transfer their customer bases in the event of registrar failure.

The Panel's preliminary view is that there may be benefits to both industry and consumers in listing resellers in the WHOIS record. The Panel understands that the current 2LD registry database has the potential and capacity to include additional or varied fields that may be able to accommodate resellers.

While this has been raised as a possibility by the Panel, the costs, technical feasibility and policy desirability have not been fully discussed. For example, would resellers be able to list themselves in WHOIS as and when they wish, or should they

be required to register on an official reseller list held in the registry and managed by auDA?

The Panel invites comments on Issue 4.3.

The Panel invites any other comments and suggestions relating to the status and recognition of resellers.

5. The policy and process for registrar transfers

Current situation

The ability of registrants to transfer the management of their domain name from one registrar to another is a fundamental tenet of the competitive .au marketplace. auDA's policy governing this activity is the [Transfers \(Change of Registrar of Record\) Policy \(2003-03\)](#). It is one of the oldest current policies in the .au framework. It stipulates that a registrant may transfer their domain name at any time, and the losing registrar must not charge a transfer fee or otherwise impede the transfer process.

While the 2008 ICAP considered a range of policy issues, it ultimately noted that submissions to their Issues Paper and draft recommendations generally agreed to maintain the status quo, and therefore the Panel made no recommendation regarding changes to the transfer policy or the password recovery process.

Issues for consideration

5.1 The current process for authorisation of registrar transfers.

Currently, the procedure for a registrar transfer requires that the gaining registrar must receive a written request for transfer, use the provided domain name password to retrieve the full domain name record from the registry and then send another confirmation message to the listed registrant contact. The gaining registrar cannot act until an affirmative response is received. It can then take up to 48 hours for the change to take effect in the registry database, unless the losing registrar chooses to approve the transfer earlier. In the meantime, no changes can be made to the domain name record.

This process was designed to ensure the integrity of the .au database and to protect against unauthorised transfers. From a security perspective, the two-step process means clients will be notified that a change has been requested, and the 48-hour delay in registry update also allows for intervention or notification to auDA of fraudulent requests.

However, the Panel believes that in the vast majority of cases, the registrar is simply seeking re-confirmation from the very person who initiated the request in the first place. The Panel further considers that there is currently a low rate of unauthorised or fraudulent requests and that contested transfers are more likely to arise from circumstances such as a falling out between business partners, between resellers and their clients, or resellers and a registrar.

On balance, the Panel is inclined to think that the current registrar transfer process strikes a reasonable balance between convenience and security.

However, from a practical perspective, the Panel notes that the process can suffer from a number of possible issues or delays, most notably when the registrant provides an incorrect password for the domain name they wish to transfer, or if their registrant contact details are incorrect. The 48-hour delay can also cause problems for registrants, particularly where name server records need to be updated (a common issue, given that many registrar transfers take place as a result of changing web hosts).

As such, the Panel is considering the possibility of changing the policy so that losing registrars would be required to approve a transfer-out, if requested by the registrant to do so. Such a policy refinement would, for the sake of registry integrity, retain the requirement for gaining registrars to seek confirmation from the registrant, but would provide a mechanism for registrants to accelerate the process if they wish to do so.

The Panel invites comments on Issue 5.1.

5.2 Bulk domain name transfers between registrars, specifically upon acquisition.

Currently, auDA policy does not expressly facilitate the bulk transfer of domain names between registrars. The cited policy rationale is:

“ . . . each registrant has an existing domain name licence agreement with the losing registrar, and this agreement cannot be reassigned to the gaining registrar. Each registrant must enter into a new domain name licence agreement with the gaining registrar.”

More generally, the prohibition on bulk transfers (in association with other clauses of the policy) also protects against mass loss of domain names through unauthorised transfers and lessens the likelihood of domain name churning for the purpose of “shopping” cheaper renewal prices. At all times, the issue of registrant consent remains paramount within the policy.

However, these prohibitions do impose considerable restrictions, particularly in instances where a registrar has acquired another accredited registrar. Currently, the acquiring registrar must retain the acquired registrar’s registry account until all domain names have expired, or been transferred out. The Panel believes that, in general, a prohibition on bulk transfers under these circumstances is not practical and leads to registrar accounts having to be maintained for no useful reason.

The Panel notes there are models for the facilitation of bulk transfers in comparable environments, notably with regard to gTLDs (ICANN policy²) and Internet Protocol addressing blocks (Regional Internet Registry policy³). However, the Panel also notes potential limitations in the implementation of these policies, for example the provision in the ICANN policy that any transfers of over 50,000 domain names are charged USD50,000, while transfers of less than 50,000 domain names are free.

The Panel’s preliminary view is that bulk transfers in the event of registrar acquisition should be allowed, in clear, well-defined circumstances where both registrars consent to the transfer and where appropriate measures are put in place to inform registrants and allow them sufficient time to transfer to a different registrar if they do not wish their domain name to be transferred to the acquiring registrar.

The Panel invites comments on Issue 5.2.

² <http://www.icann.org/en/resources/registrars/transfers/policy-01jun12.htm>

³ For example: <http://www.apnic.net/policy/transfer-policy> or <https://www.arin.net/policy/nrpm.html#eight>

5.3 Bulk domain name transfers by resellers.

In conjunction with the previous discussion issue, the Panel has specifically considered the current limitations placed upon resellers with regard to bulk transfers and their decreased ability to move their portfolios between registrars.

Panel members believe that the prohibition on bulk transfers as it applies to resellers has the effect of limiting competition and reseller mobility, and that resellers should be recognised as informed users and distinct entities in the marketplace and not as clients that “belong” to one registrar.

To that end, the Panel is inclined to the view that bulk reseller transfers be allowed, subject to similar mandatory notification and opt-out provisions for registrants as those mentioned in Issue 5.2.

The Panel notes that, while marketplace flexibility and choice are important, any proposed refinements to policy should protect the interests of registrants and prevent possible “gaming” of liberalised transfer rules (such as registrar “shopping” for cheaper renewal prices). The Panel therefore considers that the policy may need to include some protective measures, such as limits on bulk transfer frequency. Another possibility may be to restrict bulk transfers to resellers who are notified to auDA and/or listed in WHOIS (refer to Issue 4.3).

The Panel invites comments on Issue 5.3.

The Panel invites any other comments and suggestions regarding the policy and process for registrar transfers.

6. The status and operation of the .au Domain Name Suppliers' Code of Practice

Current situation

The [.au Domain Name Suppliers' Code of Practice \(2004-04\)](#) was initially developed by a drafting committee of industry and consumer representatives in February 2002, following an open call for nominations. It has since been reviewed twice, most recently in 2004. It is a compulsory Code that all .au domain name suppliers (ie. registrars and resellers) must adhere to. It covers issues such as the conduct of market participants, how and when participants may contact customers and guidelines and best practices for advertising.

Issues for consideration

Consistent with the industry self-regulatory model, the Code of Practice was intended to be developed, updated and "owned" by the Internet community. As an industry code, it had the potential to be registered by appropriate entities such as the ACCC, giving it force in law, and it could exist independently of the auDA policy framework.

The Code is not an auDA policy and therefore not subject to the same regular review cycle. Rather, it was scheduled to be reviewed if, and when, the need arose. To date, the current framework of auDA policies appears to have met users' needs and demands and, as such, no calls for review have been forthcoming. Notably, much of the fraudulent behaviour (such as misleading renewal notices) appears to have ceased in the .au marketplace, over the period the Code has been in place.

The Panel notes that, despite original intentions to implement a Code-based system in .au, the vast majority of regulatory activity is achieved through auDA policies. These policies are developed and reviewed with stakeholder input and can be enforced by auDA through binding agreements with registrars.

The Panel has considered the possibility of absorbing the content of the Code into auDA policy, noting that doing so would facilitate regular review, while retaining mechanisms for stakeholder input. The Panel is inclined to the view that the Code should continue as a separate regulatory mechanism but that "ownership" should rest with auDA – ie. auDA should be responsible for maintaining and reviewing the Code as if it were an auDA policy.

The Panel invites comments on Issue 6, as well as any other comments and suggestions on the status and operation of the .au Domain Name Suppliers' Code of Practice.

The Panel invites any other comments and suggestions on issues relevant to the Terms of Reference that are not covered in this paper.

**auDA ISS COMPLIANCE POLICY
Draft May 2012**

1. Background

The auDA Information Security Standard (ISS) is intended to assist auDA accredited registrars to manage and improve the security of their own businesses in a way that also protects the integrity and stability of the .au domain space.

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

2. auDA ISS

Refer to Attachment A (draft auDA ISS for Registrars).

3. Implementation of auDA ISS

The auDA ISS will be implemented as an auDA Published Policy. The Registrar Agreement mandates compliance with all auDA Published Policies; non-compliance may result in the suspension or termination of registrar accreditation.

3.1 New Applicants for Registrar Accreditation

From the date that the auDA ISS becomes a Published Policy, all new applicants for registrar accreditation will be required to gain certification before they are granted full accreditation. They will then be required to undertake interim assessments and re-certification every 3 years, as per the standard certification process.

3.2 Existing Registrars

As mentioned above, registrars are required to comply with all auDA Published Policies. The Registrar Agreement provides a 30 day timeframe for compliance with new or varied policies. Clearly, this timeframe is inappropriate for the introduction of the auDA ISS. Rather, the auDA ISS will be phased in for existing registrars over a 24 month period.

The aim will be to have all registrars achieve certification, or be in the process of achieving certification, by the end of the 24 month period. To that end, there will be a cut-off date for applications 12 months before the end of the 24 month period (to allow sufficient time for the registrar to prepare for certification, and for auDA to allocate assessment resources). This means that registrars will have a 12 month window to apply for certification after the auDA ISS is introduced.

4. Certification Process

Refer to Attachment B (draft Certification Process for Existing Registrars and Certification Process for New Registrar).

The aim of the Certification Process is to help each registrar to achieve certification in the way that is most suited to their own business. It allows registrars to receive as much or as little assistance as they require. Some registrars may choose to do both the Preparation and Pre-Assessment stages, others may choose to do either the Preparation or Pre-Assessment stages, and others may choose to do neither and proceed straight to the Certification Assessment. It is up to each registrar to decide what is the most appropriate course of action for their own business.

The timeframes specified in the Certification Process are intended to provide a reasonable opportunity for registrars to prepare for certification and to address any non-conformances or areas of concern during the assessment process.

5. Certification and Interim Assessments

5.1 auDA ISS Committee

The Certification Process provides for the assessor to make a recommendation to the auDA ISS committee, which will be responsible for making the final decision on certification. The purpose of the committee is to ensure that there is appropriate oversight of the process and that decisions are not being made by a single assessor. It is intended that the auDA ISS committee will comprise a senior representative from auDA, a senior representative from AusRegistry and an independent person.

Registrars who pass the Certification Assessment will be certified for 3 years, but will need to undertake interim assessments annually or as otherwise determined by the assessor, to ensure that they continue to meet the auDA ISS during the 3 years.

5.2 Use of “auDA ISS Certified” Mark

Certified registrars will be notated as such on the auDA website, and may display the “auDA ISS Certified” mark on their website if they wish. Registrars who have chosen to certify the non-registrar aspects of their business (eg. their web hosting business) may display the mark on the websites that relate to the certification (eg. their web hosting website).

5.3 Change of Registrar Ownership

Under the Registrar Agreement, change of ownership of a registrar requires the prior written consent of auDA. Following the introduction of the auDA ISS, auDA will need to consider on a case-by-case basis what effect a change of ownership has on the registrar's certification. For example, if the purchaser already owns other accredited and certified registrars then auDA may determine that it is acceptable for the next certification assessment to take place as per the existing schedule. On the other hand, if the purchaser is new to the registrar business then auDA may determine that there needs to be a certification assessment within a set time of sale or even prior to auDA's consent being granted.

6. Consequences of Non-Certification

6.1 New Applicants for Registrar Accreditation

New applicants for registrar accreditation who do not achieve certification during their provisional accreditation will not receive full accreditation.

6.2 Existing Registrars

During the phase-in period:

- Registrars who do not apply for certification before the cut-off date will have their accreditation suspended until such time as they apply.
- Registrars who apply for certification but do not pass the Certification Assessment will have their accreditation suspended until they pass.

After the phase-in period, registrars who do not pass either their interim assessments or their 3 yearly Certification Assessment will have their certification revoked and their accreditation suspended until they pass the assessment. The suspension will be announced publicly by auDA.

If a registrar has not passed their assessment within 3 months of being suspended, then their accreditation will be terminated on the grounds that auDA can have no confidence in the registrar's ability to protect the security of their registry connection or their registrant data.

NB: Suspension of accreditation means that the registrar will not be able to create new domain names or accept transfers, but they will be able to manage their existing domain names.

7. Costs

auDA will bear the main cost of implementing the auDA ISS, including:

- Certification Assessments and interim assessments of registrars, using auDA's nominated assessor, up to a capped amount (tbd)
- Pre-Assessments of registrars, using auDA's nominated assessor, up to a capped amount (tbd)
- Preparation for registrars, if the registrar chooses to use auDA's nominated assessor, up to a capped amount (tbd). If the registrar chooses to use their own consultant then they must bear the cost.



Information Security Standard
for
Registrars

DRAFT

Version	0.7
Version Date	April 2012
Author	David Dornbrack - Vectra Corporation
Project Name	Information Security Standard for Registrars

1. Reference Documents

1	auda-2004-04	.au Domain Name Suppliers' Code of Practice
2	auda-2009-01	Registrar Accredited Criteria
3	auda-registrar-agreementv4	Registrar Agreement
4	auDA Info-Sec SOW 011211 V1.0	Vectra Statement of Work
5	PPG_PPG234_MSRIIT_012010_v7	Security risk in information
6	ISO 27002:2006	Security Techniques – Code of Practice
7	ISO 27001:2006	Information Security Requirements
8	PCI DSS V2.0	Payment Card Industry Data Security Standard
9	Strategic_Plan_April_08	auDA Strategic Plan 2008-2010
10	auDA_strategic_plan_2010-12	auDA Strategic Plan 2010-2012

2. Background

2.1 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.

auDA performs the following functions:

- Develop and implement domain name policy
- License 2LD registry operators
- Accredite and license Registrars
- Implement consumer safeguards
- Facilitate .au Dispute Resolution Policy
- Represent .au at ICANN and other international forums

ICANN's (Internet Corporation for Assigned Names and Numbers) is responsible for the coordination of the global Internet's systems of unique identifiers and for ensuring its stable and secure operation.

2.2 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.

2.3 Information Security Responsibilities

Current agreements between auDA and the 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

2.4 auDA Information Security Standard (auDA ISS)

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

The auDA Information Security Standard (auDA ISS) sets a baseline for information security for Registrars. The auDA ISS is aligned to well-established international security standards that 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 auDA ISS.

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

The auDA ISS is intended to assist registrars 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 auDA ISS.

auDA also requires that Registrars who use third party service providers (e.g. for IT support, software development or hosting) also meet the auDA 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 facilitate the sale of and administration of domain names to resellers, are required to provide facilities in a manner that meets the auDA ISS.

2.5 Provision for In-Place Information Security Certifications

auDA recognises that some Registrars may already have relevant information security certifications⁴ in place. Provided the scope of the in-place certification(s) is

⁴ Examples include AS/NZS 27001 and/or PCI DSS

relevant⁵ and current, auDA will recognise those certifications in lieu of the auDA ISS.

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

3. auDA ISS Requirements

3.1 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 auDA 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

3.2 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.

⁵ Relevance: Scope of in-place certification must meet or exceed the auDA ISS certification requirements

- 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.

3.3 Development Process

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

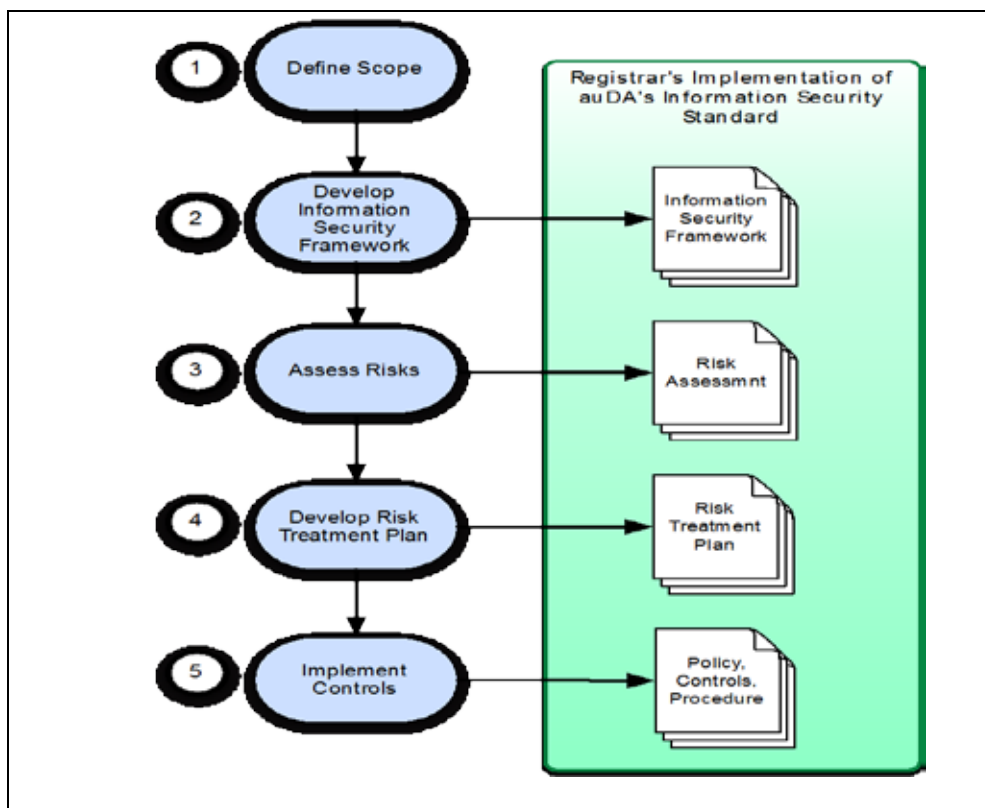


Figure 1 - Typical Development Process for auDA ISS at Registrar

4. 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.

4.1 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 senior management
- Be reviewed at least annually or if significant changes occur
- Be made available to and communicated to employees and external parties where relevant

The information security policy must address:

- 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
- The requirement to comply with relevant legislative, regulatory and contractual obligations

4.2 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:

- Management's commitment to information security through acknowledgement and assignment of information security responsibilities
- Co-ordination 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
- Contacts with authorities (e.g. Federal Police)

4.3 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:

- Description of how assets are identified
- Up to date list of important assets⁶ (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)
- Information classification (How do employees and contractors identify the value of information and how are they meant to protect that information. E.g. Confidential, Public, Secret)

4.4 Human Resources

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

The process must include:

- Background verification checks
- Description of security roles and responsibilities for the job role
- Information security responsibilities in Terms and Condition of employment
- Information security awareness education

⁶ Do 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.)

- Disciplinary process in the event of committed security breaches
- Responsibilities in the event of termination or change of employment conditions (including removal of access rights and return of assets)

4.5 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:

- 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)
- Secure disposal of equipment (removal of sensitive data)

4.6 Operations Management

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

The operation manual must include:

- 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
- Capacity management

4.7 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:

- Agreed security controls
- Service definitions and delivery levels
- Monitoring requirements and expectations (e.g. reports and audits)
- Managing changes to services and/or requirement

4.8 Malicious Code and Vulnerability Management

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

The controls must include:

- 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
- Business continuity plans for recovering from malicious code attack or errors resulting from vulnerabilities

4.9 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:

- 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
- File integrity monitoring – Monitoring of files that should not change.

4.10 Access Control

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

The access control policy must include:

- 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
- Minimal access per role. (i.e. default deny all. Access based on expressly defined rules)

The access control procedures must include:

- User access management procedures for user registration
- Unique ID's for users (no using redundant user ID's)
- 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
 - Password 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)
- Conditions and required security practices under which remote access is permitted

4.11 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:

- 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.
- 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.

4.12 Cryptographic Controls

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

The cryptographic control must include:

- 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.
- Procedures dealing with key management, roles and responsibilities, and development and maintenance of standards.

4.13 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 formal appointment of a point-of-contact 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
- The requirement to immediately notify the relevant authorities and regulators including auDA and AusRegistry

4.14 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:

- 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
- Periodic testing and updating of the plan

4.15 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:

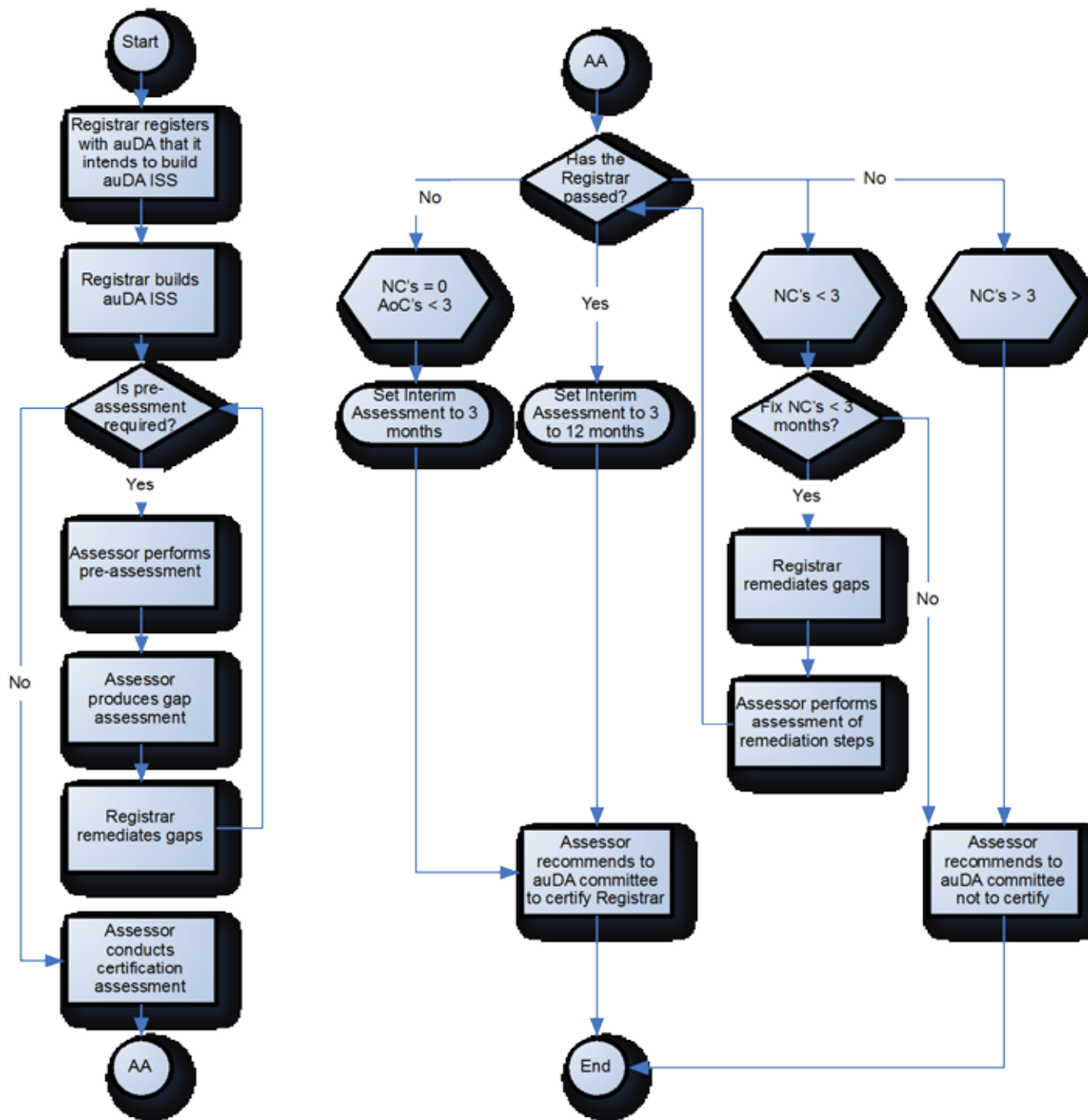
- Compliance relating to intellectual property rights
- Compliance relating to protection of company records (e.g. accounting, database, audit logs, transaction logs, operational procedures)
- Compliance relating to the retention of records
- Compliance relating to protection and privacy of personal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

Certification Process for Existing Registrars


Overview.

The following table and accompanying flow chart describes the certification process for existing registrars. The steps in the table closely follow the process shown in the flow chart. (Note: The AA bubbles in the flow charts are used to allow the whole process to be described on a single page).

Certification Process Existing Registrar



Step	Description	Comments
1	Application – Registrar applies to auDA, signifying its intention to comply with the standard and be assessed at some date in the future.	<p>Registrar completes an application form. This form could be downloaded from auDA’s website, or posted to the applicant from auDA.</p> <p>In the process of completing the application form the Registrar needs to indicate when they will be ready for the pre-assessment, and the actual assessment. auDA needs to “lock in” the pre-assessment and assessment resources.</p> <p>For some Registrars they will know what they need to do to setup their auDA ISS. Others may have little to no idea. At this point in time, the Registrar can request assistance from auDA in preparing their auDA ISS.</p>
2	Preparation – Registrar prepares documentation and processes as required by the auDA ISS	<p>Some registrars will be proficient at setting up and preparing the documentation. They will be mature and potentially have security personnel on board that could do this.</p> <p>Some Registrars will have no idea where to start. auDA can engage Vectra can help them, or the Registrar can use their own resources or external consultants. The Vectra (or external consultant) consulting arrangements can vary from doing it for them completely or providing guidance on how to approach it. (The latter is preferable, because the Registrar will own the process if they develop it themselves. If it is done for them, they might tend to distance themselves from the process)</p> <p>The process of establishing the auDA ISS at a Registrar could take anything from 3 months to 12 months. Variables include: Business model, security maturity, and existence of processes/procedures, scope and size of the organisation.</p>
3	Pre-Assessment – Registrar arranges with auDA to perform a pre-assessment of their auDA ISS implementation.	<p>This step is not compulsory, but highly recommended, as it prepares the Registrar for the certification assessment, and subsequently reduces the risk of failing the certification audit.</p> <p>auDA’s nominated assessor visits the Registrar to perform the pre-assessment. Assessments should take between 3 and 5 days. Gap assessment reports (2 days) are completed and sent to Registrar for discussion. Nominated assessor explains the report to the Registrar. If gaps are minor, then Registrar has up to 3 months to fix/remediate. If gaps are significant, Registrar must start again, and assessment of the entire auDA ISS for that Registrar is done again.</p>
4	Certification Assessment – Registrar arranges with auDA to conduct the certification assessment of their auDA ISS implementation.	<p>auDA’s nominated assessor attends the Registrar’s site to perform the Certification Audit. The Registrar should be prepared with all the documentation ready for the assessor. If the Registrar has been through the pre-assessment, they should be familiar with the assessment process.</p>



The certification assessment should take anything from 3 to 5 days. The deliverable is a certification assessment report and should take about 2 days to produce. It will be discussed with the Registrar as it is being developed. There should be no disagreement with the contents of the report.

A checklist should be developed for the Registrar that prompts them to check and make sure they have everything in place and ready for the assessment. They should have this list ready on the day of the assessment, together with all the other documentation as per the checklist. (Vectra can assist in developing this checklist, but to make it workable, this should be done after a few pilot assessments have been done)

There are several possible outcomes to the Certification Assessment:

1. The Registrar passes the assessment with flying colours. The assessor writes up the certification report, recommending that the auDA security committee approve the certification of the Registrar. The auDA security committee meets (monthly, quarterly) to consider assessment reports. (This process needs to be documented) One of the inputs to this decision should be the Registrar Exposure Value (REV). The assessment report should be consistent with the REV. The Registrar is certified for 3 years, and will need interim assessments conducted annually by the assessor. (i.e. 2 interim assessments before the next certification assessment). The Registrar is issued a certificate for auDA ISS certification.
2. The Registrar passes the audit, because they have no Non Conformances (NC's) and no more than 3 Areas of Concern (AoC's). The assessor writes the assessment report and recommends certification. The committee assesses the report and the REV and usually approves the certification. The interim assessment interval is set to 3 months. If after 3 months the AoC's are cleared, then interim assessment is reset to between 3 months and 12 months (at the discretion of the assessor) and validated by the auDA ISS committee. There must be no NC's. A Registrar will generally not be certified if they have any NC's.
3. The Registrar does not pass the assessment but they are close to passing because they have less than 3 NC's, and it is the opinion of the assessor and the Registrar, that the NC's can be remediated within 3 months. The assessor writes up the report, and recommends that the NC's are remediated and the assessment repeated within a

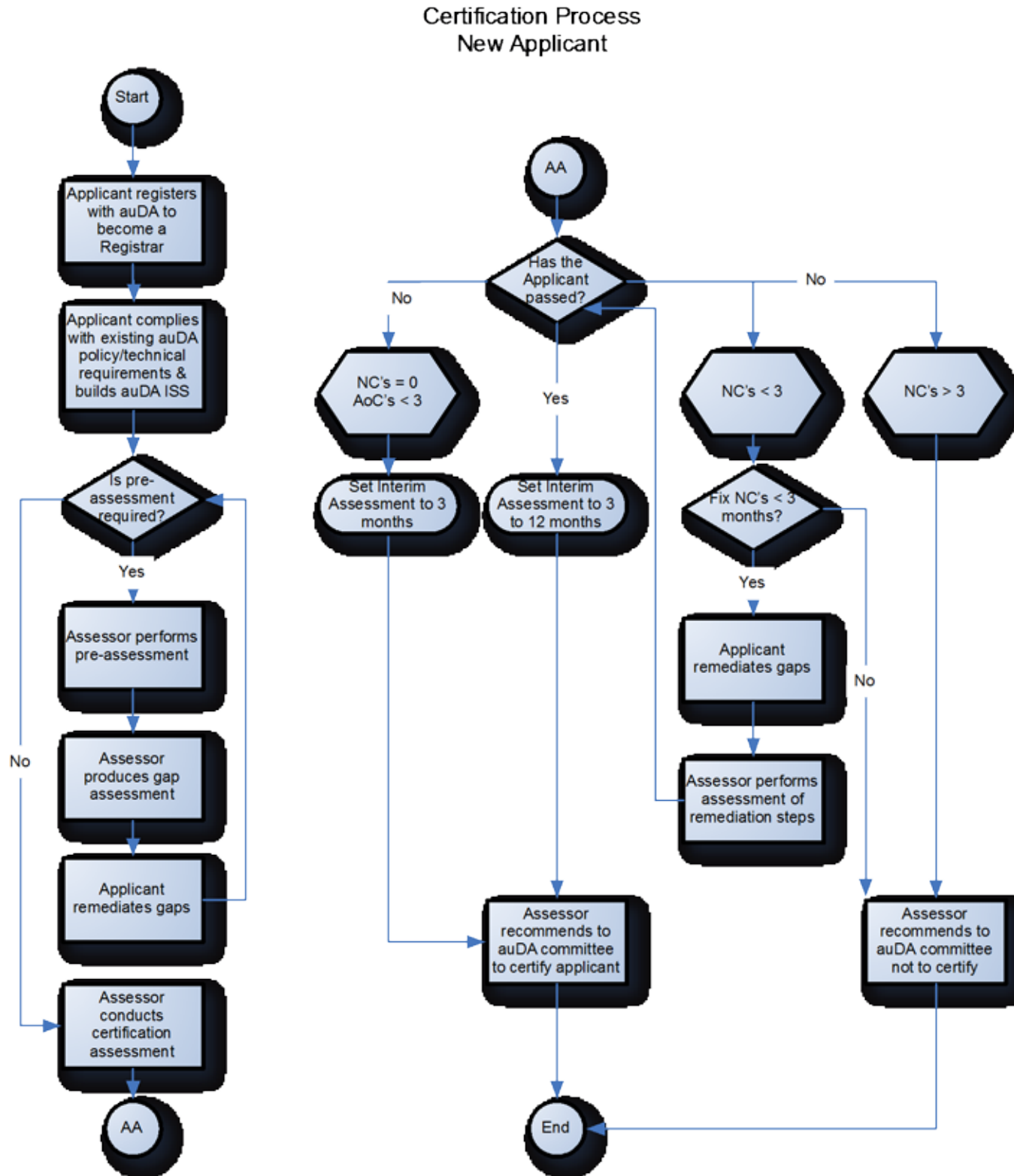
period of 3 months. Within 3 months the assessor validates that none of the previous findings are invalidated, and that the NC's have been rectified. The assessor recommends to the auDA security committee that the Registrar is certified, and recommends an interim assessment interval between 3 and 12 months.

4. The Registrar fails the assessment. The Registrar has multiple NC's and AoC's. The assessor needs to decide in conjunction with the Registrar whether it is worth continuing the assessment. The assessor recommends to the auDA security committee that the Registrar not be approved for certification.


5	Interim Assessments – auDA informs the Registrar that their interim assessment is due on date dd/mm/yyyy. The Registrar agrees or finds a suitable alternative date.	An interim assessment is a light touch assessment conducted by the assessor to make sure that the auDA ISS system is still operational and is operating as planned. Depending on the size of the and scope and complexity, it should take between 0.5 and 1 day to perform the assessment, and up to 1 day to write up the report. Same rules apply: <ol style="list-style-type: none"> 1. If no NC's and no AoC's then all is good. 2. If no NC's and up to 3 AoC's then all is good, but remediate the AoC's. 3. If < 3 NC's then certification is determined to be "provisional" and NC's must be remediated within 3 months. 4. If > 3 NC's then certification is revoked.
6	Tri-annual certification Assessment.	Same as step 4. Assessor conducts full assessment. If the assessor is familiar with the setup of the Registrar, then the time taken should be less than when the audit was first conducted.

Certification Process for New Registrar

This process is similar to the process for an existing Registrar, except that the applicant is required to conform with all the requirements of the auDA ISS (including the current tests) before being allowed to operate as a fully accredited Registrar.



Step	Description	Comments
1	Application – New applicant applies to auDA, to become a Registrar.	<p>Applicant completes all current auDA processes (policy knowledge and technical test). Applicant is now additionally required to comply with the auDA ISS. Applicant needs to indicate when they will be ready for pre-assessment and certification assessment. This allows auDA to lock in resources.</p> <p>For some new applicants will know what they need to do to setup their auDA ISS. Others may have little to no idea. At this point in time, the applicant can request assistance from auDA in preparing their auDA ISS.</p>
2	Preparation – Applicant prepares documentation and processes as required by the auDA ISS	<p>Some applicants will be proficient at setting up and preparing the documentation. They will be mature and potentially have security personnel on board that could do this.</p> <p>Some applicant will have no idea where to start. auDA can engage Vectra can help them, or the applicant can use their own resources or external consultants. The Vectra (or external consultant) consulting arrangements can vary from doing it for them completely or providing guidance on how to approach it. (The latter is preferable, because the applicant will own the process if they develop it themselves. If it is done for them, they might tend to distance themselves from the process)</p> <p>The process of establishing the auDA ISS at a new applicant's site could take anything from 3 months to 12 months. Variables include: Business model, security maturity, and existence of processes/procedures, scope and size of the organisation.</p>
3	Pre-Assessment – Applicant arranges with auDA to perform a pre-assessment of their auDA ISS implementation.	<p>This step is not compulsory, but highly recommended, as it prepares the applicant for the certification assessment, and subsequently reduces the risk of failing the certification audit.</p> <p>auDA's nominated assessor visits the applicant to perform the pre-assessment. Assessments should take between 3 and 5 days. Gap assessment reports (2 days) are completed and sent to applicant for discussion. Nominated assessor explains the report to the applicant. If gaps are minor, then applicant has up to 3 months to fix/remediate. If gaps are significant, the applicant must start again, and assessment of the entire auDA ISS for that applicant is done again.</p>
4	Certification Assessment – Applicant arranges with auDA to conduct the certification assessment of their auDA ISS implementation.	<p>auDA's nominated assessor attends the applicant's site to perform the Certification Audit. The applicant should be prepared with all the documentation ready for the assessor. If the applicant has been through the pre-assessment, they should be familiar with the assessment process.</p>



The certification assessment should take anything from 3 to 5 days. The deliverable is a certification assessment report and should take about 2 days to produce. It will be discussed with the applicant as it is being developed. There should be no disagreement with the contents of the report.

A checklist should be developed for the applicant that prompts them to check and make sure they have everything in place and ready for the assessment. They should have this list ready on the day of the assessment, together with all the other documentation as per the checklist. (Vectra can assist in developing this checklist, but to make it workable, this should be done after a few pilot assessments have been done)

There are several possible outcomes to the Certification Assessment:

5. The applicant passes the assessment with flying colours. The assessor writes up the certification report, recommending that the auDA security committee approve the certification of the applicant and they can become a fully accredited Registrar. The auDA security committee meets (monthly, quarterly) to consider assessment reports. (This process needs to be documented) One of the inputs to this decision should be the Registrar Exposure Value (REV). In the case of an applicant, the REV may not be fully complete. The assessment report should be consistent with the REV. The Applicant (now a Registrar) is certified for 3 years, and will need interim assessments conducted annually by the assessor. (i.e. 2 interim assessments before the next certification assessment). The Applicant (now a Registrar) is issued a certificate for auDA ISS certification.
6. The applicant passes the audit, because they have no Non Conformances (NC's) and no more than 3 Areas of Concern (AoC's). The assessor writes the assessment report and recommends certification. The committee assesses the report and the REV and usually approves the certification. The interim assessment interval is set to 3 months. If after 3 months the AoC's are cleared, then interim assessment is reset to between 3 months and 12 months (at the discretion of the assessor) and validated by the auDA ISS committee. There must be no NC's. An applicant will generally not be certified if they have NC's.
7. The applicant does not pass the assessment but they are close to passing because they have less than 3 NC's, and it is the opinion of the assessor and the applicant, that the NC's can be remediated within 3 months. The assessor writes

up the report, and recommends that the NC's are remediated and the assessment repeated within a period of 3 months. Within 3 months the assessor validates that none of the previous findings are invalidated, and that the NC's have been rectified. The assessor recommends to the auDA security committee that the applicant is certified, and recommends an interim assessment interval between 3 and 12 months.

8. The applicant fails the assessment. The applicant has multiple NC's and AoC's. The assessor needs to decide in conjunction with the applicant whether it is worth continuing the assessment. The assessor recommends to the auDA security committee that the applicant not be approved for certification.

5	Interim Assessments – auDA informs the Registrar (formally an applicant) that their interim assessment is due on date dd/mm/yyyy. The Registrar agrees or finds a suitable alternative date.	An interim assessment is a light touch assessment conducted by the assessor to make sure that the auDA ISS system is still operational and is operating as planned. Depending on the size of the and scope and complexity, it should take between 0.5 and 1 day to perform the assessment, and up to 1 day to write up the report. Same rules apply: <ol style="list-style-type: none"> 5. If no NC's and no AoC's then all is good. 6. If no NC's and up to 3 AoC's then all is good, but remediate the AoC's. 7. If < 3 NC's then certification is determined to be "provisional" and NC's must be remediated within 3 months. <p>If > 3 NC's then certification is revoked.</p>
6	Tri-annual certification Assessment.	Same as step 4. Assessor conducts full assessment. If the assessor is familiar with the setup of the Registrar, then the time taken should be less than when the audit was first conducted.