2012 INDUSTRY ADVISORY PANEL

DRAFT RECOMMENDATIONS – SEPTEMBER 2012

1. 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/

2. 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.

Issues Paper, June 2012

The Panel released an Issues Paper in June 2012. The paper set out the detail of the current .au policy framework and invited comment on suggestions and options for change. The Panel received eight submissions and ten responses to its online survey. These are archived on the auDA website at: http://www.auda.org.au/2012iap/2012iap-index/

Draft Recommendations, September 2012

This report contains the Panel's draft recommendations to the auDA Board on the six main issues under consideration. The draft recommendations have been formed as a result of the Panel's own deliberations and the public consultation in June.

The draft recommendations represent the consensus view of the Panel.

Following a review of any submissions on the draft recommendations the Panel will complete its final report and provide it to the auDA Board in December 2012.

3. SUBMISSIONS TO THE PANEL

Stakeholders that would like to comment on the draft recommendations set out in this report are invited to send their submissions to:

auDA 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 as confidential.

Alternatively, respondents may wish to complete an online survey at: http://www.surveymonkey.com/s/PZ3JCJT

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

The closing date for submissions and survey responses is **Friday 19 October 2012**.

4. GLOSSARY

Term	Definition
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
ICANN	Internet Corporation for Assigned Names and Numbers – the global DNS administrator
ICAP	auDA's 2008 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
WHOIS	A public service that allows users to query a domain name to find its associated details, including registrant and registrar information.

5. EXECUTIVE SUMMARY

The Panel's draft recommendations are summarised below for ease of reference, however the Panel urges readers to consider each recommendation in conjunction with the explanatory text provided in the body of the report.

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

Draft Recommendation 1A:
The Panel recommends that:
a) the competitive registry model should be retained
b) auDA should initiate renegotiations with AusRegistry to extend contractual arrangements for 2, 3 or 4 years
c) if renegotiations with AusRegistry fail, auDA should proceed to conduct a formal RFT process; and
d) the auDA Board should publicly commit to undertaking a formal RFT process once the renegotiated registry agreement expires.

Draft Recommendation 1B:
The Panel recommends that auDA should retain the current single registry for existing .au 2LDs, while allowing the option for the introduction of multiple registries in the future.

Issue 2. The policy and process for registrar accreditation

Draft Recommendation 2A:
The Panel recommends that auDA should revise the fees for registrar accreditation, to better reflect the direct costs of the accreditation process and ongoing regulation.

Draft Recommendation 2B:
The Panel recommends that:
a) current requirements for ASIC and ATO registration for overseas-based registrars should be retained; and
b) overseas-based registrars should be required to bear the reasonable costs of a site visit by an auDA staff member during provisional accreditation.

Draft Recommendation 2C:
The Panel recommends that the requirement for applicants for registrar accreditation to act as a reseller of another registrar for 6 months, or show equivalent experience, should be retained.

Draft Recommendation 2D:
The Panel recommends that the registrar accreditation process and criteria should be the same for all applicants, regardless of their proposed business model.

Issue 3. Registrar security

Draft Recommendation 3:
The Panel recommends that the auDA Board adopt the auDA Information Security Standard (ISS) as a mandatory requirement for accredited registrars, and take appropriate steps to finalise the ISS documentation and processes and ensure its prompt and effective implementation.

Issue 4. The status and regulation of resellers

Draft Recommendation 4A:
The Panel recommends the retention of the current .au industry model for auDA, registrar and reseller inter-relationships.

Draft Recommendation 4B:
The Panel recommends that auDA develop a standardised agreement template for registrars to use as a basis for their reseller contracts.

Draft Recommendation 4C:
The Panel recommends that auDA develop and implement a system for adding a reseller "contact object" to the registry database, including a "reseller contact ID", name and email address, and that auDA should be responsible for managing this mechanism for recording resellers.

Issue 5. The policy and process for registrar transfers

Draft Recommendation 5A:
The Panel recommends that no changes be made to the current .au transfer authorisation process.

Draft Recommendation 5B:
The Panel recommends that bulk registrar transfers be allowed with auDA approval in the case of mergers and acquisitions, and that auDA ensure that the process includes appropriate registrant protections.

Draft Recommendation 5C:
The Panel recommends that bulk reseller transfers be allowed with auDA approval, and that auDA ensure that the process includes appropriate registrar and registrant protections.

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

Draft Recommendation 6:
The Panel recommends that auDA assume responsibility for facilitating regular review and updating of the .au Domain Name Suppliers' Code of Practice in consultation with relevant stakeholders.

6. 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.

Based on their discussions to date and the outcomes of the first public consultation, 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 recommendations 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.

7. DRAFT RECOMMENDATIONS

Issue 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 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 the 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.

Submissions to the Issues Paper – June 2012

The Panel notes that the public contributions received in response to the Panel's Issues Paper expressed a range of views with regard to the preferred method of registry operator selection and appointment. Most respondents favoured either a full RFT process or renegotiation with the incumbent, though there was no consensus. The Panel took all of these views into consideration as part of its deliberations.

The Panel also notes that two respondents to the Issues Paper declared their interest in competing for the .au 2LD registry. The Panel discussed these statements of interest at length and, in particular, the impact this stated competition may have on the Panel's decision and recommendations regarding this Term of Reference.

Views of the Panel

At a fundamental level, the Panel recognises its responsibility to arrive at a recommendation that reflects the needs of Australian Internet users and that delivers the best possible value to stakeholders at the current time. The Panel notes that the decision regarding a preferred registry selection method must be based upon full consideration and analysis of all relevant factors, including openness, transparency and probity of processes, competition effects, cost pressures, service provision levels, technical requirements and costs-of-change. Given the importance and implications of this decision, the Panel has determined to provide an expansive report, below, of its deliberations on this issue.

The Panel has focussed its discussions on the respective merits and drawbacks of the two main registry operator selection options: a full RFT in 2014 or alternatively a renegotiation with the incumbent contracted registry provider.

The Panel notes that there is currently an absence of stated industry dissatisfaction with the current registry provider. This conclusion is based upon the collective .au market experience of Panel members and auDA's advice that it has not received any registry-related complaints. The Panel notes that potential competitors would consider this when assessing their chances in the tender process.

In addition, to the best of the Panel's knowledge, the incumbent is still the only interested party with significant operational infrastructure established in Australia – a key requirement of performing the .au registry role. Given this, the Panel believes that the incumbent has a considerable competitive advantage over potential bidders, who would incur significant costs in establishing an Australian presence.

In this context, the Panel also notes that registry prices for .au domain names (e.g. $14.58 for two years in com.au) are already closely aligned with those in other namespaces such as .com (USD7.85 for one year).[1] The Panel's view is that the

---

[1] http://www.auda.org.au/registrars/accreditation/

current registry pricing model, and the significant start-up costs for a new entrant, may limit the ability of other interested parties to price their tender at lower rates than those currently available.

The Panel has also considered the potential impact of new gTLDs on registry competition in Australia. It would be expected that the expansion of the global domain marketplace may result in additional potential registry competitors and further interest in .au, though the Panel's view is that this could take 2-3 years to occur. Panel members have also discussed the possibility of high failure rates of new gTLDs, the resources other registry providers have committed to the new gTLD process, and the incumbent's significant involvement in Australian-based gTLD applications and concluded that these factors could work to diminish competitive effects in the near-term. On the whole, it is too soon to reasonably forecast the effects the new gTLD process may have, though the Panel believes that the process will provide a useful test for current and new registry operators, allowing some to establish market experience and track-record, while others' business models may falter.

Panel members have raised concerns that, irrespective of prevailing market conditions, a tender in 2014 may serve to "lock-in" the incumbent for a period of 6 to 8 years, potentially missing the opportunity for real competition in a shorter timeframe.

Another concern is that, whilst a poor tender response and absence of competitive registry alternatives would provide auDA with a clearer perspective on the state of the .au marketplace, it could also do the same for the incumbent, affording that party an advantage in renegotiation.

The Panel recognises that there would be a cost to auDA of running the tender process, and switching costs for registrars should the tender be awarded to a new registry provider. While these are not insurmountable issues and could be managed, they are factors that have been raised by Panel members in deciding whether or not to proceed to tender in 2014.

The Panel is aware of the recommendations of the 2008 Industry Competition Advisory Panel – for a renegotiation for "up to" four years and, if required, a tender process that would deliver contractual arrangements for a period of 6 to 8 years. The Panel also notes that ICAP members likely made these recommendations with the expectation that an open tender process would occur at the expiry of these arrangements, ie. in 2014.

The Panel has undertaken careful consideration of the potential benefits of conducting a tender process at this time – market transparency and confidence, reputational benefits for auDA, and tangible confirmation of either a build-up, or lack, of demand for competition. The Panel also notes that auDA processes could come under criticism if a tender is not undertaken, and all of these factors have been considered in determining which registry selection method is the most appropriate.

Balancing these pressures - both for and against a competitive tender process - the Panel has achieved general consensus upon recommending to the auDA Board that it initiate renegotiations with AusRegistry to extend the current contractual arrangements for 2, 3 or 4 years. This negotiating flexibility will allow auDA to determine which contractual period delivers the greatest value to the Australia Internet community. Should renegotiations fail, then the Panel recommends that auDA should proceed to conduct a full RFT.

The Panel has also agreed to recommend that the auDA Board commit to a formal RFT process following the expiry of the renegotiated registry agreement. Panel members feel that this would provide certainty to the market, allow for observation and informed assessment of the true competitive effects of the new gTLD process, and give potential competitors the confidence to commit resources and finances to position themselves for the process.

On the secondary question of single registry versus multiple registries, the Panel notes the consensus among community respondents and agrees to recommend the maintenance of the current model - i.e. retain a single registry for all existing .au 2LDs while allowing the option for the introduction of multiple registries in the future.

Draft Recommendation 1A:
The Panel recommends that:
a) the competitive registry model should be retained
b) auDA should initiate renegotiations with AusRegistry to extend contractual arrangements for 2, 3 or 4 years
c) if renegotiations with AusRegistry fail, auDA should proceed to conduct a formal RFT process; and
d) the auDA Board should publicly commit to undertaking a formal RFT process once the renegotiated registry agreement expires.

Draft Recommendation 1B:
The Panel recommends that auDA should retain the current single registry for existing .au 2LDs, while allowing the option for the introduction of multiple registries in the future.

Issue 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. 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 maintain domain name records for the lifetime of the domain name registration, manage renewals, and provide adequate customer support services, as well as being able to connect technically 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. auDA also sets a per domain name fee (currently $3.50), which is incorporated into the wholesale price that the registry charges registrars. Registrars are free to set their own domain name fees to resellers and retail customers; as at September 2012, the registrar retail price of a two year com.au domain name registration ranged from $19.95 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 38 and the market share of the top 4 registrars has grown from 60 to 65%.

<u>Submissions to the Issues Paper – June 2012</u>
The Panel notes that the public contributions received in response to the Issues Paper expressed general consensus with regard to many of the questions raised in the paper, such as the requirement for all potential .au registrars to act as a reseller for 6 months (or show equivalent experience) and the obligations required of overseas registrars.

However, on issues such as registrars seeking accreditation for the exclusive purpose of offering drop-catching services, there were a range of views expressed. The Panel has considered all of these in its discussions.

<u>Views of the Panel</u>
On the question of registrar fees, the Panel notes that accreditation fees have not increased since 2002, in accordance with the initial intent behind maintaining low barriers to entry to the .au marketplace (thereby stimulating competition in .au).

However, the Panel recognises the subsequent growth of the .au domain marketplace and the increasing costs borne by auDA in relation to registrar accreditation and compliance monitoring.

On balance, Panel members agree that auDA should revise its fees for registrar accreditation to ensure that they better reflect the direct costs incurred. The Panel considers that any fee changes resulting from this recommendation must be proportional and cost-based and should not result in an extreme increase in accreditation fees.

On the question of overseas registrars, the Panel agrees that the processes, rules, and assessment requirements should be the same for all registrars, irrespective of location. In this respect, Panel members agree that it is appropriate to retain current ASIC and ATO registration requirements for overseas-based registrars.

Panel members also note the importance of site visits in ensuring the effective ongoing regulation of registrars, and therefore believe that overseas-based registrars should bear the reasonable costs associated with the travel and accommodation of an auDA staff member to undertake a site visit during provisional accreditation.

With regard to the current requirement for all potential .au registrars to act as a reseller of another registrar for 6 months, or show equivalent experience, the Panel's view is that this is another important provision for ensuring the integrity of the .au space, and therefore this requirement should be retained.

On the question of registrars seeking accreditation for the exclusive purpose of offering drop-catching services (and subsequent accreditations for the sole purpose of improving the efficacy of these services), the Panel believes that no change should be made to current accreditation procedures. In arriving at this conclusion, the Panel notes that the purpose of accreditation is to determine an entity's capacity to perform as a registrar and that the criteria used (including customer service, security, complaints resolution etc) must remain consistent, irrespective of the business model and activities accredited parties chose to pursue.

> **Draft Recommendation 2A:**
> **The Panel recommends that auDA should revise the fees for registrar accreditation, to better reflect the direct costs of the accreditation process and ongoing regulation.**

> **Draft Recommendation 2B:**
> **The Panel recommends that:**
> **a) current requirements for ASIC and ATO registration for overseas-based registrars should be retained; and**
> **b) overseas-based registrars should be required to bear the reasonable costs of a site visit by an auDA staff member during provisional accreditation.**

> **Draft Recommendation 2C:**
> **The Panel recommends that the requirement for applicants for registrar accreditation to act as a reseller of another registrar for 6 months, or show equivalent experience, should be retained.**

> **Draft Recommendation 2D:**
> **The Panel recommends that the registrar accreditation process and criteria should be the same for all applicants, regardless of their proposed business model.**

Issue 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 specific requirements in relation to registrar security.

Submissions to the Issues Paper – June 2012
The Panel notes that nearly all responses received expressed strong support for the proposed draft auDA Information Security Standard (ISS). Importantly, the Panel notes that there were no objections to the proposed mandatory application of the auDA ISS to accredited registrars.

Views of the Panel
The draft auDA ISS is at **Attachment A.**

The Panel notes that the draft auDA 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. Panel members believe that the introduction of the auDA ISS is an important step in securing the infrastructure, processes and systems that underpin the stable operation of .au. To that end, the Panel would encourage auDA and the industry to ensure its prompt implementation.

The Panel endorses the draft auDA ISS as a mandatory requirement for accredited registrars. The Panel notes that finalisation of the ISS documentation and processes are implementation matters for the auDA Board to determine.

> **Draft Recommendation 3:**
> **The Panel recommends that the auDA Board adopt the auDA Information Security Standard (ISS) as a mandatory requirement for accredited registrars, and take appropriate steps to finalise the ISS documentation and processes and ensure its prompt and effective implementation.**

Issue 4. The status and regulation of resellers

<u>Current situation</u>
Many registrars use sales agents known as resellers. Resellers are not accredited by auDA and do not have a direct technical connection to the registry. Rather, resellers procure domain name registrations and manage names records for their customers through an interface with their 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. There are currently approximately 4750 resellers notified to auDA, although this number is thought to be much lower than the number of resellers actually operating in the marketplace.

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.

Also, under current policy resellers cannot enter their own information as part of a name registration. Therefore, the WHOIS record and certificate of registration reflect only the customer and the registrar-of-record. In many cases, this may be an entity that is not familiar to the registrant.

<u>Submissions to the Issues Paper – June 2012</u>
The Panel notes that the majority of the public contributions received in response to the Panel's Issues Paper expressed a general consensus among respondents, though there were a few topics on which views slightly diverged.

<u>Views of the Panel</u>
The Panel agrees that, with some refinements discussed below, the current reseller model works well, and recommends its retention. In making this recommendation, it is the view of the Panel that the establishment of a direct, formal regulatory relationship between auDA and all resellers is not in the best interests of all parties and would place inappropriate administrative burdens upon auDA staff.

As a refinement to the current model, the Panel recommends that auDA develop a standardised agreement template for registrars to use as a basis for their reseller contracts, similar to the template Registrant Agreement contained in the Registrar Agreement. It is felt that this document would help to provide consistency in registrar-reseller relationships and ensure predictability for customers of resellers.

The Panel has also considered the desirability of, and mechanisms for, the formal recognition and identification of resellers. The Panel understands that resellers want to be recognised "in the system" as a form of protection in the case of registrar failure, and to better facilitate portfolio portability. It has also been suggested that

some kind of formal recognition of resellers would make it easier for registrants to identify the entity that is managing their domain name.

With these benefits in mind, the Panel supports the introduction of a dedicated, standardised reseller field in WHOIS. Such a change is technically feasible and would be a relatively simple and effective way of providing the identification or recognition that resellers seek.

In order to provide appropriate identity verification and format standardisation, the Panel recommends that auDA should be responsible for issuing "reseller contact IDs", on application by a reseller. More specifically, the Panel recommends that auDA develop and implement a system for adding a reseller contact object to the registry database, including a reseller ID, name and email address. The Panel notes that the system could incur costs for registrars in modifying their own systems to accommodate reseller contact objects, that implementation is rightfully a business decision for each registrar and therefore should be developed as an "opt-in", rather than mandatory model.

In arriving at this recommendation, the Panel also considers that such a model would provide an opportunity for better engagement between auDA and resellers, and both improved consumer education from resellers (in the form of mandatory pro-forma consumer information) and education of resellers (through training and staff engagement). The Panel further notes that such a system would afford auDA some direct regulatory power over resellers – notably the ability to withdraw reseller contact IDs in case of breach of policy by a reseller – and agrees that this would be appropriate.

Draft Recommendation 4A:
The Panel recommends the retention of the current .au industry model for auDA, registrar and reseller inter-relationships.

Draft Recommendation 4B:
The Panel recommends that auDA develop a standardised agreement template for registrars to use as a basis for their reseller contracts.

Draft Recommendation 4C:
The Panel recommends that auDA develop and implement a system for adding a reseller "contact object" to the registry database, including a "reseller contact ID", name and email address, and that auDA should be responsible for managing this mechanism for recording resellers.

Issue 5. The policy and process for registrar transfers

<u>Current situation</u>
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.

Submissions to the Issues Paper – June 2012
The Panel notes the public contributions received in response to the Panel's Issues Paper and the general consensus among respondents on the issues raised.

Views of the Panel
In its Issues Paper, the Panel proposed a possible refinement to the current transfer authorisation process, whereby transfers are automatically processed by the registry after a 48 hour wait period unless the losing registrar approves the transfer earlier. The Panel considered whether losing registrars should be required to approve transfers more rapidly in cases where requested to do so by the registrant. Following public consultation, the Panel agrees that imposing such a requirement would be unnecessary, noting that the current mechanisms are efficient, operate more rapidly than in other TLDs (most notably the 5 day delay in .com transfers), and strike an appropriate balance between efficacy and registrant protection.

The Panel notes that public consensus exists on the issue of allowing bulk registrar-to-registrar transfers in the case of mergers or acquisitions. The Panel also notes that registrar change of ownership must be approved by auDA under the Registrar Agreement, therefore a bulk registrar transfer can only ever occur with auDA's prior knowledge and authorisation.

In accordance with this, the Panel recommends that bulk registrar transfers be allowed on the proviso that appropriate consumer protections are put in place. These protections include mandatory registrant notification and opportunity to "transfer out".

On the issue of bulk transfers by resellers, the Panel notes that such a mechanism is sought by resellers and supported by public comments. The Panel agrees that resellers should be afforded the ability to transfer their portfolios between registrars. As such, the Panel recommends that bulk reseller transfers be allowed along the same lines as bulk registrar transfers, though with additional protections in place including:

- The need for auDA to approve all bulk reseller transfer requests
- The restriction of bulk reseller transfer requests to resellers who have been issued a reseller contact ID (as discussed and recommended in the previous Term of Reference)
- The establishment of losing registrar objection mechanisms and criteria (using ICANN's transfer policy as an implementation guideline)
- The requirement for registrant notification and ability to opt out / transfer.

Draft Recommendation 5A:
The Panel recommends that no changes be made to the current .au transfer authorisation process.

Draft Recommendation 5B:
The Panel recommends that bulk registrar transfers be allowed with auDA approval in the case of mergers and acquisitions, and that auDA ensure that the process includes appropriate registrant protections.

> **Draft Recommendation 5C:**
> **The Panel recommends that bulk reseller transfers be allowed with auDA approval for resellers who have been issued with a reseller contact ID, and that auDA ensure that the process includes appropriate registrar and registrant protections.**

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

Current situation
The .au Domain Name Suppliers' Code of Practice was developed by a Drafting Committee of industry and consumer representatives in February 2002, following an open call for nominations. It is a compulsory Code that all name suppliers 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.

Submissions to the Issues Paper – June 2012
The Panel notes that few public comments were received in response to this Term of Reference, though there was a divergence in views between retaining the Code in its current form and subsuming the responsibility for maintaining the Code as part of the auDA policy development and review framework.

Views of the Panel
The Panel has considered the two main options available regarding the future of the Code of Practice. On one hand, the Panel recognises that the Code has been largely successful in preventing the undesirable marketplace behaviour that it had been established to address.

The Panel also notes that, currently, the Code sits outside of the auDA policy framework as it was supposed to be developed and "owned" by domain name suppliers. While a desirable arrangement, the Panel notes that the independent nature of the Code has led to it not being revisited or redrafted since 2004.

The Panel believes that bringing the Code into the auDA policy framework is the most efficient way to assure its regular review and ongoing currency. The Panel recommends this course of action, noting that auDA would maintain a largely administrative role, fostering and facilitating Code review, though the document would primarily remain a statement of industry stakeholders' undertakings and commitments.

> **Draft Recommendation 6:**
> **The Panel recommends that auDA assume responsibility for facilitating regular review and updating of the .au Domain Name Suppliers' Code of Practice in consultation with relevant stakeholders..**

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_MSRIT_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
- Accredit 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 certifications[2] in place. Provided the scope of the in-place certification(s) is

---

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

relevant[3] 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.
- 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.

---

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

- 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.
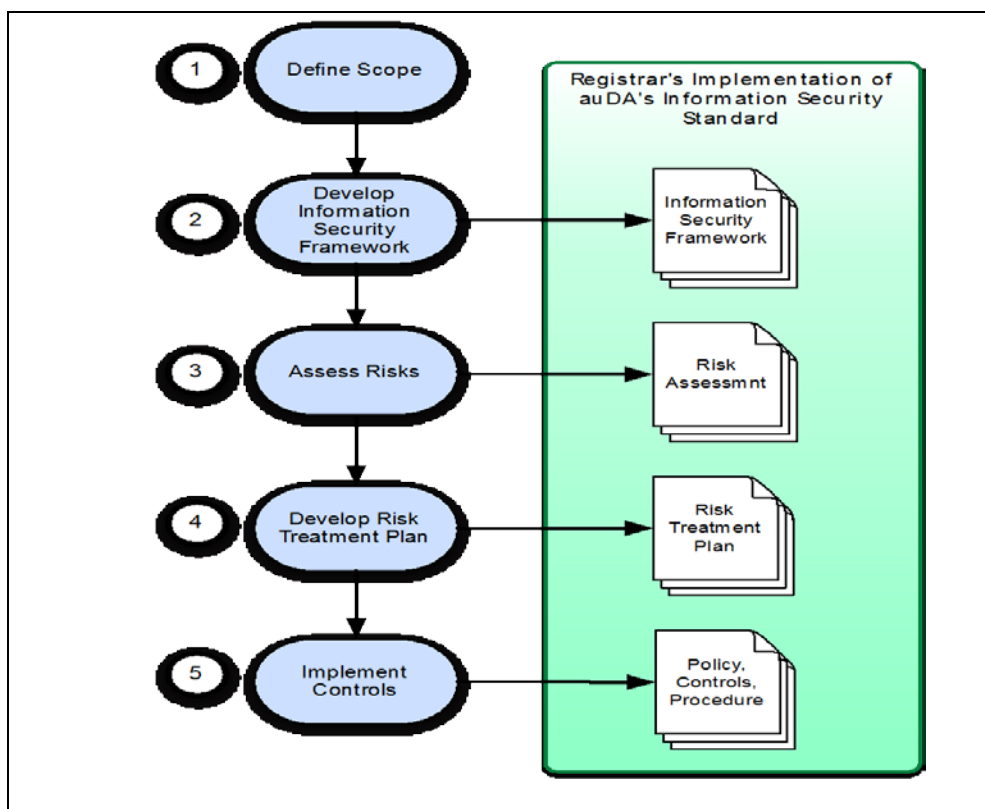

Figure 1 - Typical Development Process for auDA ISS at Registrar

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, catogorised and afforded appropriate protection.

The plan must address:

- Description of how assets are identified
- Up to date list of important assets[4] (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
- 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] 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.)

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 and 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-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
- 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 help 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.
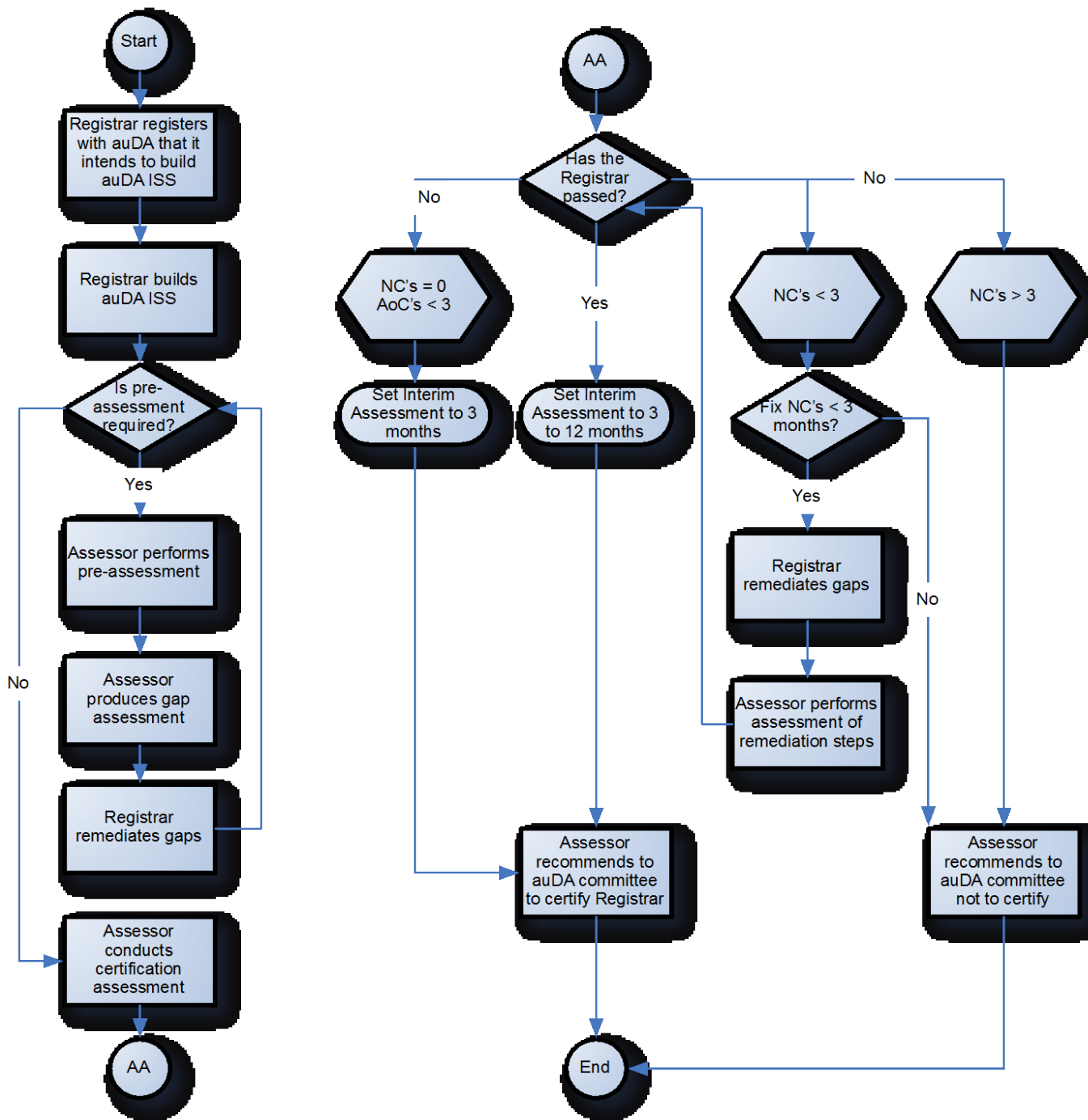
The regulatory compliance register must include:

- 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.	Registrar completes an application form. This form could be downloaded from auDA's website, or posted to the applicant from auDA. 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. 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.
2	Preparation – Registrar prepares documentation and processes as required by the auDA ISS	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. 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) 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.
3	Pre-Assessment – Registrar arranges with auDA to perform a pre-assessment of their auDA ISS implementation.	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. 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.
4	Certification Assessment – Registrar arranges with auDA to conduct the certification assessment of their auDA ISS implementation.	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. 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 discression 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

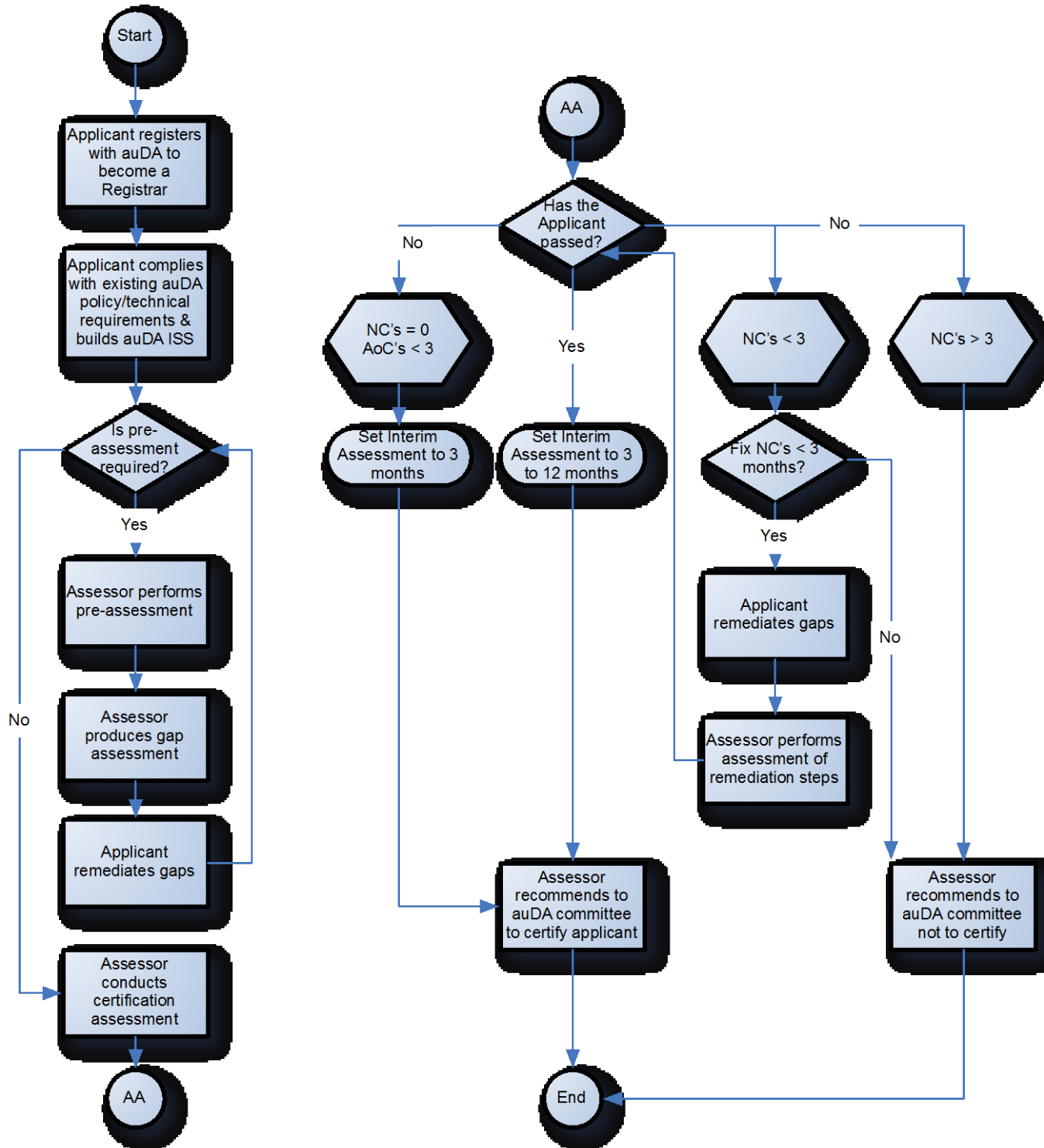|		auDA security committee that the Registrar is certified, and recommends an interim assessment interval between 3 and 12 months.
		4. The Registrar fails the assessment. The Registrar has multiple NC's and AoC's. The assessor needs to decide in conjunction with the Registrar whether it is worth continuing 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: 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.

Certification Process
New Applicant

Step	Description	Comments
1	Application – New applicant applies to auDA, to become a Registrar.	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. 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.
2	Preparation – Applicant prepares documentation and processes as required by the auDA ISS	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. 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) 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.
3	Pre-Assessment – Applicant arranges with auDA to perform a pre-assessment of their auDA ISS implementation.	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. 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.
4	Certification Assessment – Applicant arranges with auDA to conduct the certification assessment of their auDA ISS implementation.	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. 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 discression 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:
		  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.
		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.