



# ISS Assessment Process

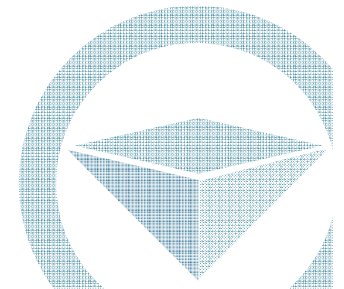
Prepared by: Kelvin Heath, Chief Security Officer

Vectra Corporation Ltd

17<sup>th</sup> October 2013

# ••• Vectra Corporation

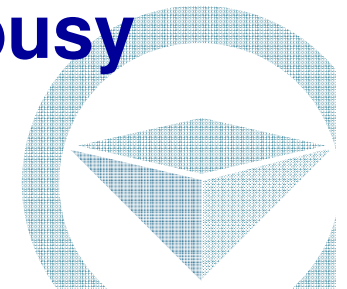
- Australian owned Security and Compliance company
- 30 years experience with regulatory compliance, information security and technology
- Services include
  - Security and compliance consulting
  - Security Validation Services
  - Managed Security Services
  - Provision of Security Technology
  - Forensic Investigations



# ∴ The Ostrich Approach to Compliance

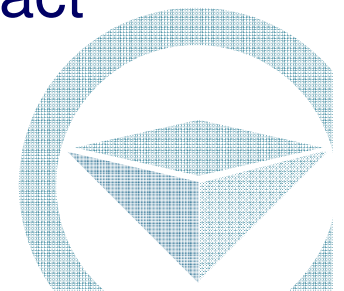


- **Bury your head in the sand**
- **Just sit on it and see what happens**
- **Run away and avoid it**
- **Form a committee and look busy**



# ❖❖❖ Ostriches are Delaying the Inevitable


- auDA ISS Compliance is not optional, it will be necessary to fully comply
- Take the opportunity to use it to improve your business
- A ‘best practice’ standard providing improved security for *all* information and business systems
- Alignment with and progress toward PCI DSS, ISO27001 and Australian Privacy Act
- Improved understanding and documentation of business processes, applications, data flows etc.
- Reduced likelihood of compromise, reduced impact
- Improved customer confidence



# auDA Compliance Portal

Welcome to TruComply - auDA Logged in as: Test Person. [Log Out](#) [Home](#) [My Account](#) [Help](#)

[Home](#) [Assessments](#)




## Welcome, Test!

You are accessing the TruComply Risk Management portal. TruComply allows you to assess threats and vulnerabilities, manage total cost of risk, assign and track risk mitigation, report on security posture and regulatory compliance, and develop decision-enabling reports.

- [auDA Information Security Standard](#)
- [auDA ISS Glossary of Terms](#)
- [Vulnerability Scanning](#)
- [auDA ISS Assessment Procedures](#)

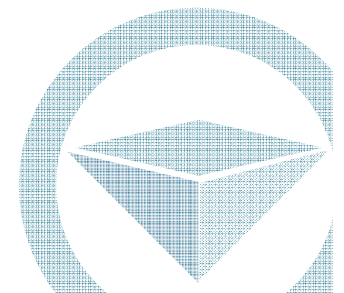
**Things you can do today:**

-  [Complete tasks assigned to you](#)  
You have **0** tasks to complete.

Copyright © 2013 .au Domain Administration Limited. All Rights Reserved. Version: 4.7.8

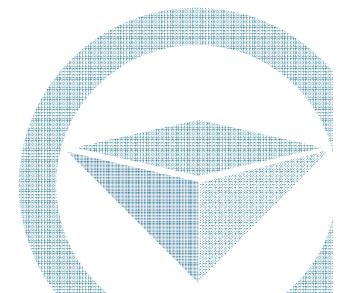
## ❖ Assessment Procedure

- Complete **Self Assessment** on auDA Portal
- Initiate the external vulnerability scan on auDA Portal
- Book On-site Assessment with auDA
- Assessor conducts **On-site Assessment**
- Initial ISS Compliance Report issued
- 3 month **Remediation** timeframe
- Revalidation of remediated items
- Issue of final **ISS Compliance Report**



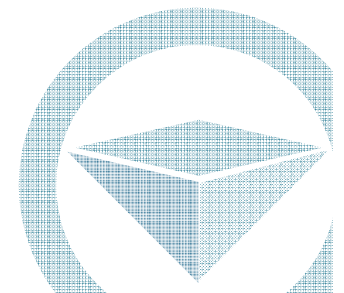
## Self Assessment

- Web based auDA Compliance Portal
- Answer each question
- Upload evidence where applicable
- Reference section or page number in comments
- Register for external vulnerability scanning



## ••• On-site Assessment Process

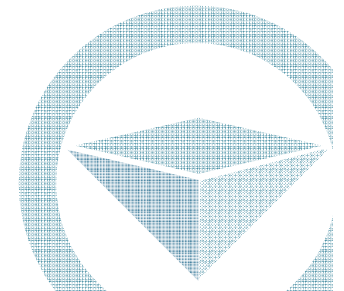
- Vectra Assessor 2 - 5 days onsite over a 2-3 week timeframe
- Determine the scope of the assessment
  - Logical or physical network segmentation
  - Network diagram
    - Flow of customer domain name registration data
    - Logical / physical devices
- Identify list of system components for sampling
  - Typically 10% of all in scope system components





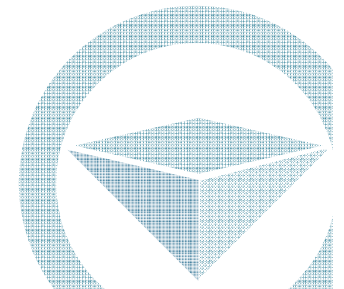
# ••• On-site Assessment Process

- Validation and confirmation that controls are in place
  - System configuration settings
  - Log files
  - Firewall / Router rule sets
  - Vulnerability scan results
  - Interview of relevant personnel
  - Process review
  - Personnel files



## ❖ On-site Assessment Process

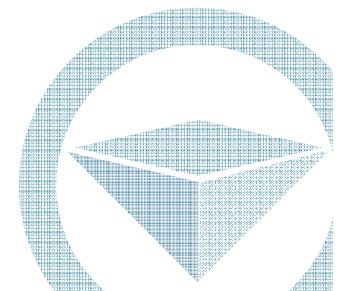
- Opportunity to clarify and understand requirements
- Remediation can be undertaken during the onsite assessment
- For periodic activities, if the process is documented and in place, will be assessed as compliant for the first assessment
- Initial ISS Compliance Report delivered



## Remediation

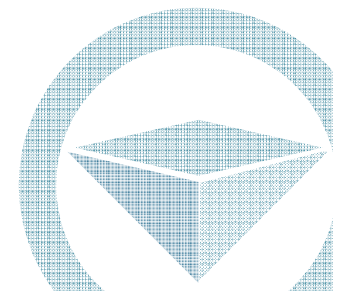
### **3 month timeframe to remediate non-compliant items**

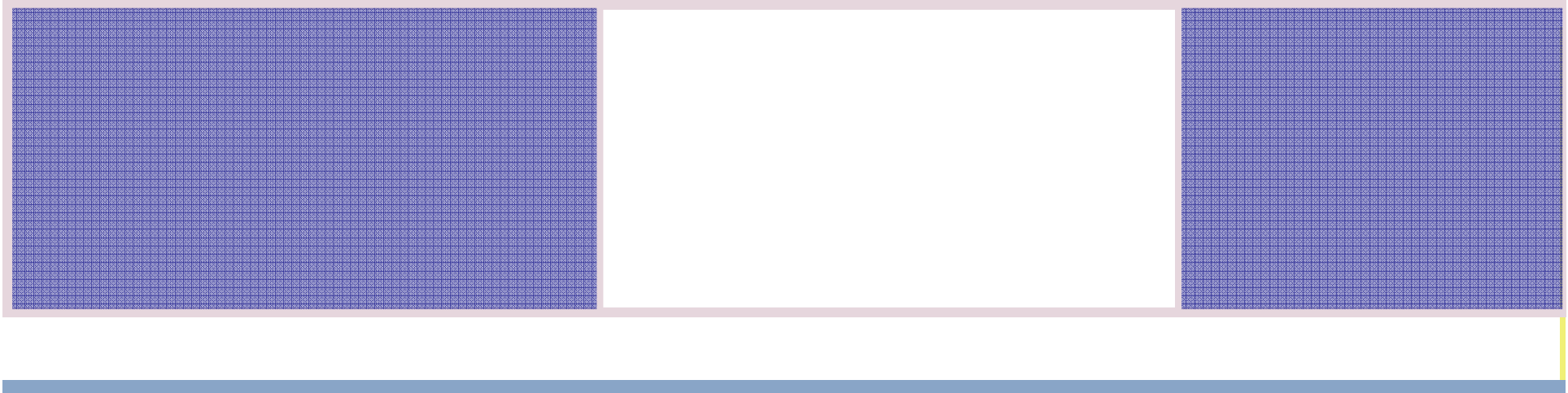
- Consider de-scoping using network segmentation
- Compensating controls will be considered
- Vectra Assessor telephone and email support available
- Evidence can be reviewed as completed
- Final ISS Compliance Report issued after 3 months, or earlier if remediation is completed early



## ⋮ Ongoing Improvement

- We welcome comments on the process
- ISS will evolve as threats and risks emerge
- Assessment process will undergo improvement
  - Areas of focus
  - Validation methods
  - Reporting





 Questions ?

[Kelvin.heath@vectra-corp.com](mailto:Kelvin.heath@vectra-corp.com)



**V E C T R A**  
CORPORATION

[\*\*www.vectra-corp.com\*\*](http://www.vectra-corp.com)