

Presentation to the
INTOSAI Working Group on IT Audit

Protecting our Cyber Future

May 2017

Cyber Attacks: Securing Agencies' ICT Systems

Cyber Resilience

Have entities achieved
compliance with
Australian Government
requirements and
are entities cyber resilient?

Overview of the IT Audit Branch

Vision: *To be the best IT Audit Group in Australia*

Align to support Financial and Performance audits by:

- Integrating the audit activities of IT and financial audits; and
- Supporting 20+ performance audits, with a focus on data analytics; and
- Undertaking IT-heavy performance audits, such as the cyber security audits.

Australian Government Information Security Core Policy

Agencies (non-corporate Commonwealth entities) are required to:

- appropriately safeguard all official information to ensure its confidentiality, integrity, and availability by applying safeguards so that:
 - only authorised people access information through approved processes
 - information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
 - information is classified and labelled as required
- ensure information created, stored, processed, or transmitted in or over government information and communication technology (ICT) systems is properly managed and protected throughout all phases of a system's life cycle.
- There are seven overarching mandatory requirements covering information security underpinned by high level controls.

INFOSEC 4 requires the following:

Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual.

Compliance Requirements

- Entities must comply with the Protective Security Policy Framework (PSPF)
- There are 36 requirements under the PSPF and they are divided into four categories:
 1. Governance
 2. Personnel Security
 3. Information Security
 4. Physical Security

Compliance Requirements

The *Top Four* mitigation strategies are included in the Information Security category labelled INFOSEC 4.

The *Top Four* strategies to mitigate targeted cyber intrusions are:

To prevent malware running:

- Whitelisting
- Patching applications

To limit the extent of incidents and recover data:

- Patching operating systems
- Minimising administrative privileges

Essential Eight

The following four mitigations have been added to the *Top Four* strategies:

To prevent malware running:

- Disable untrusted Microsoft Office macros
- User application hardening

To limit the extent of incidents and recover data:

- Multi-factor authentication
- Daily backup of important data

Cyber Resilience

Cyber resilience is the ability to continue providing services while deterring and responding to cyber attacks. Cyber resilience also reduces the likelihood of successful cyber attacks.

- Cyber resilience requires entities to:
 - Effectively implement the Top Four
 - Have a sound entity-wide ITGC framework

ANAO Reports

- The ANAO has issued three reports on Australian Government entities' compliance with the ISM and their overall cyber resilience
 1. No.50 2013-14 *Cyber Attacks: Securing Agencies' ICT Systems*
 2. No.37 2015-16 *Cyber Resilience*
 3. No.42 2016-17 *Cybersecurity Follow-up Audit*
- Copies of these reports are available from the ANAO website:
www.anao.gov.au

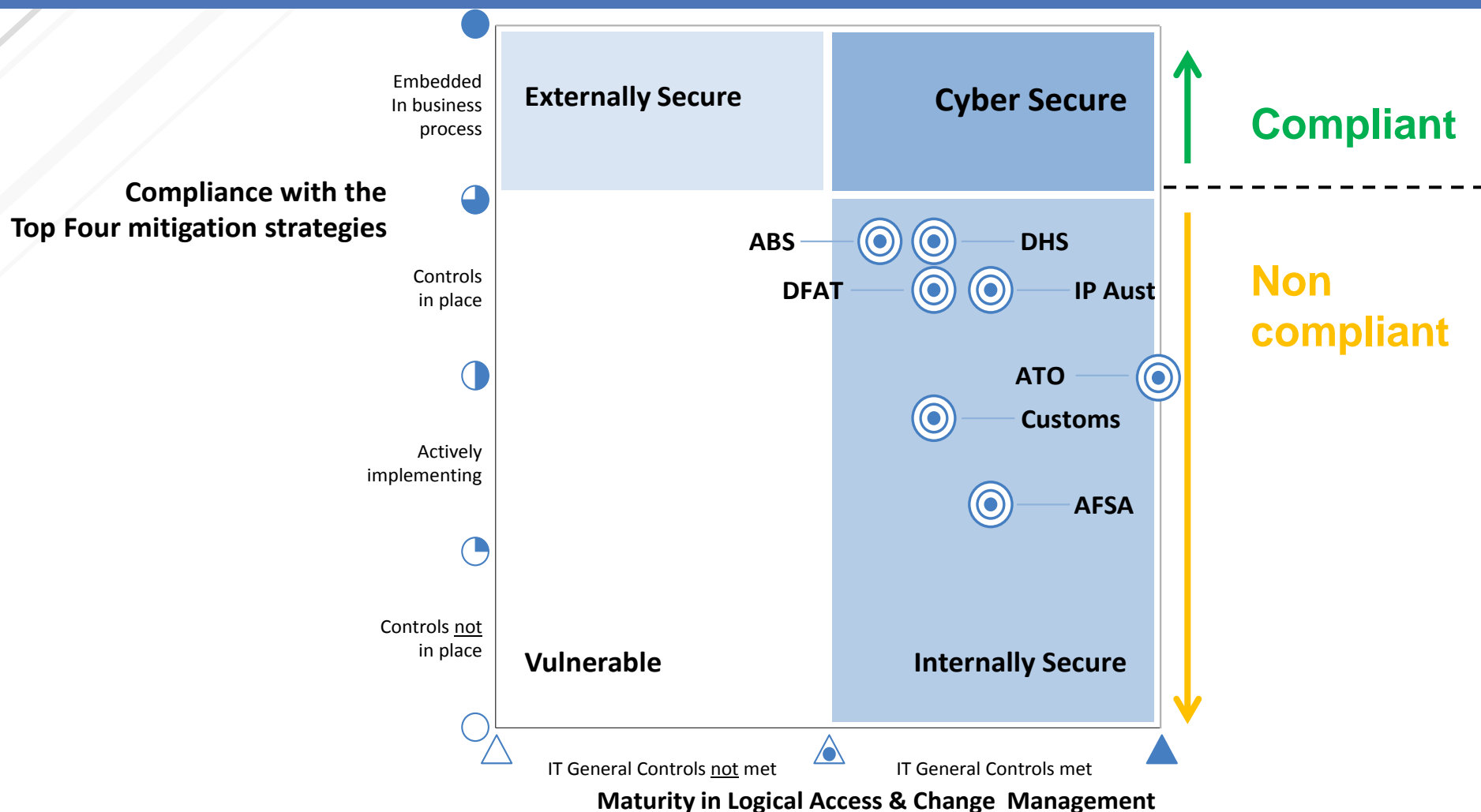
The Joint Committee of Public Accounts and Audit was particularly interested in the audit findings

- ... and expressed concern about the agencies' security posture and management arrangements to implement mandated IT security controls across their enterprise ICT systems.
- On 2 March 2015, the JCPAA recommended that the **ANAO consider including regular audits**, in its schedule of performance audits, of Commonwealth entities' compliance with the top four mitigation strategies as well as Commonwealth entities' overall security posture.

Since June 2015, the JCPAA further:

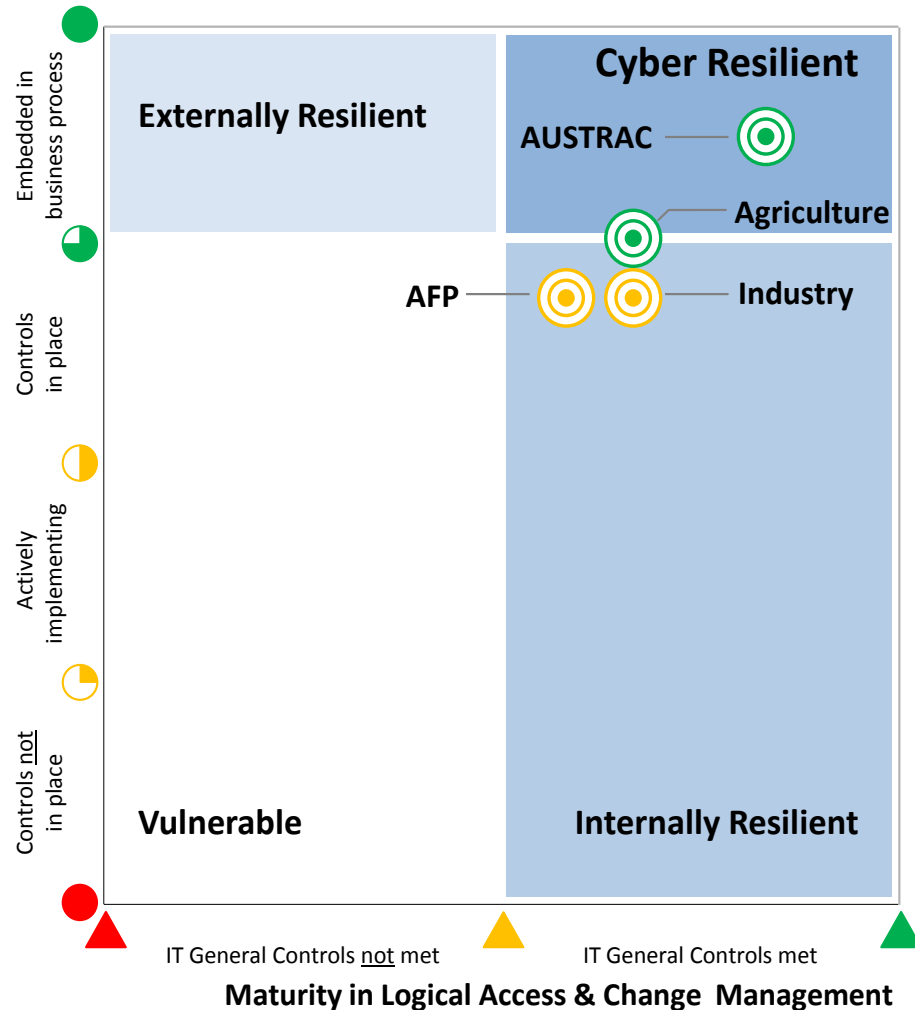
- was interested in the audit findings
- recommended additional cyber security audits
- will conduct a review of the most recent audit findings

Entities' ICT posture - 2013

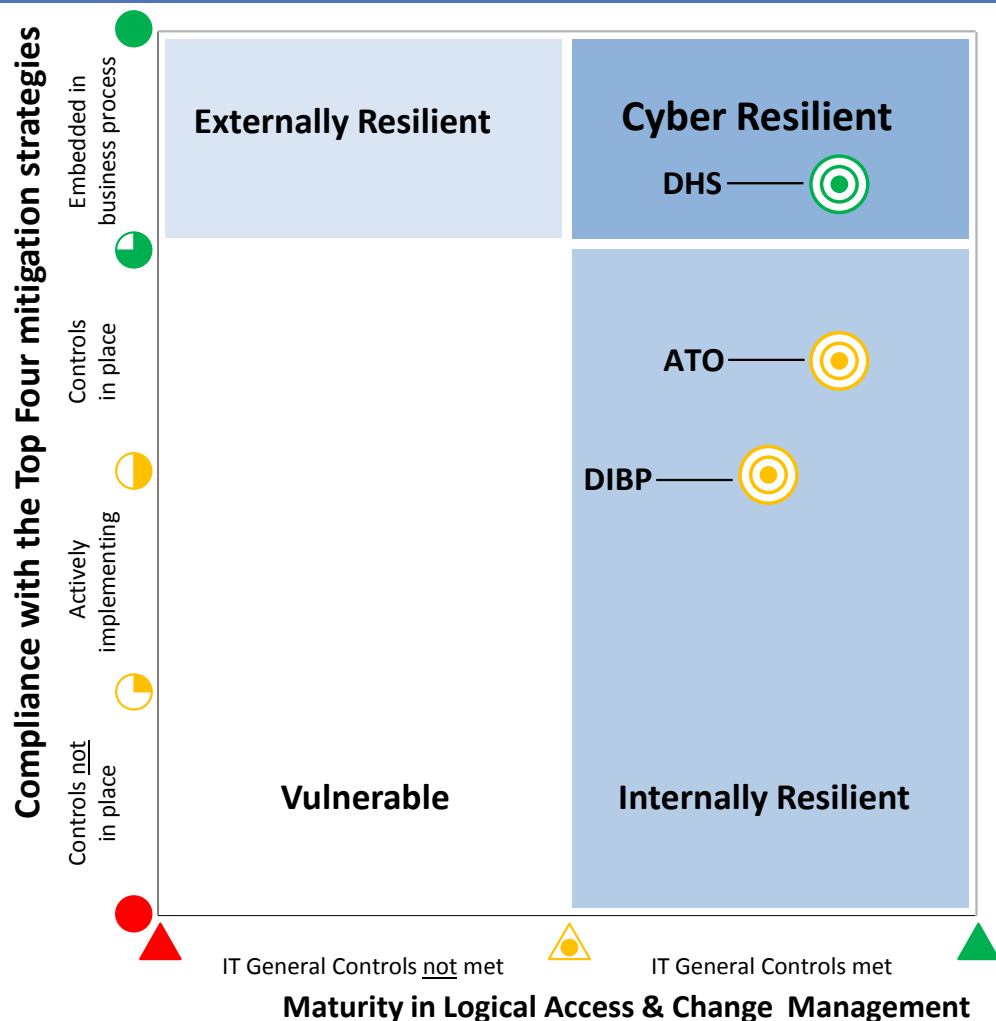


Entities' ICT posture - 2015

Compliance with the
Top Four mitigation strategies

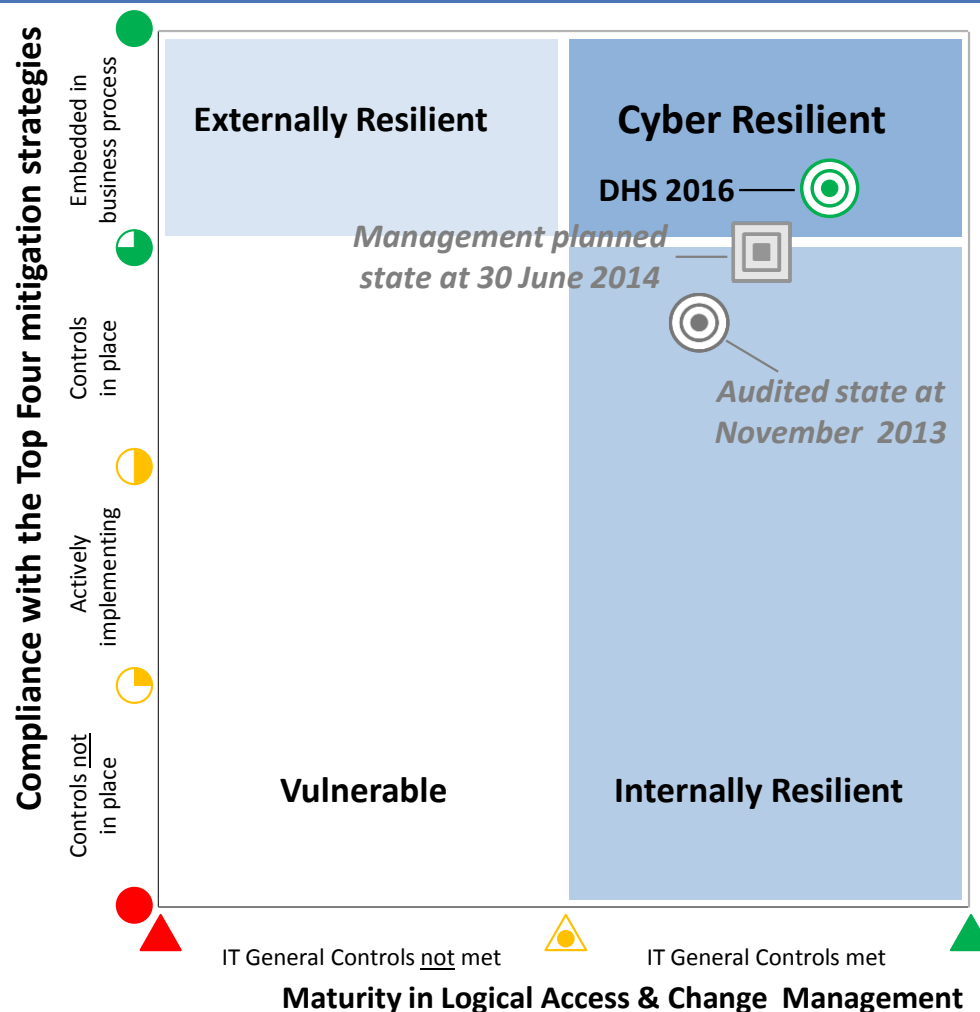


Entities' ICT posture - 2016



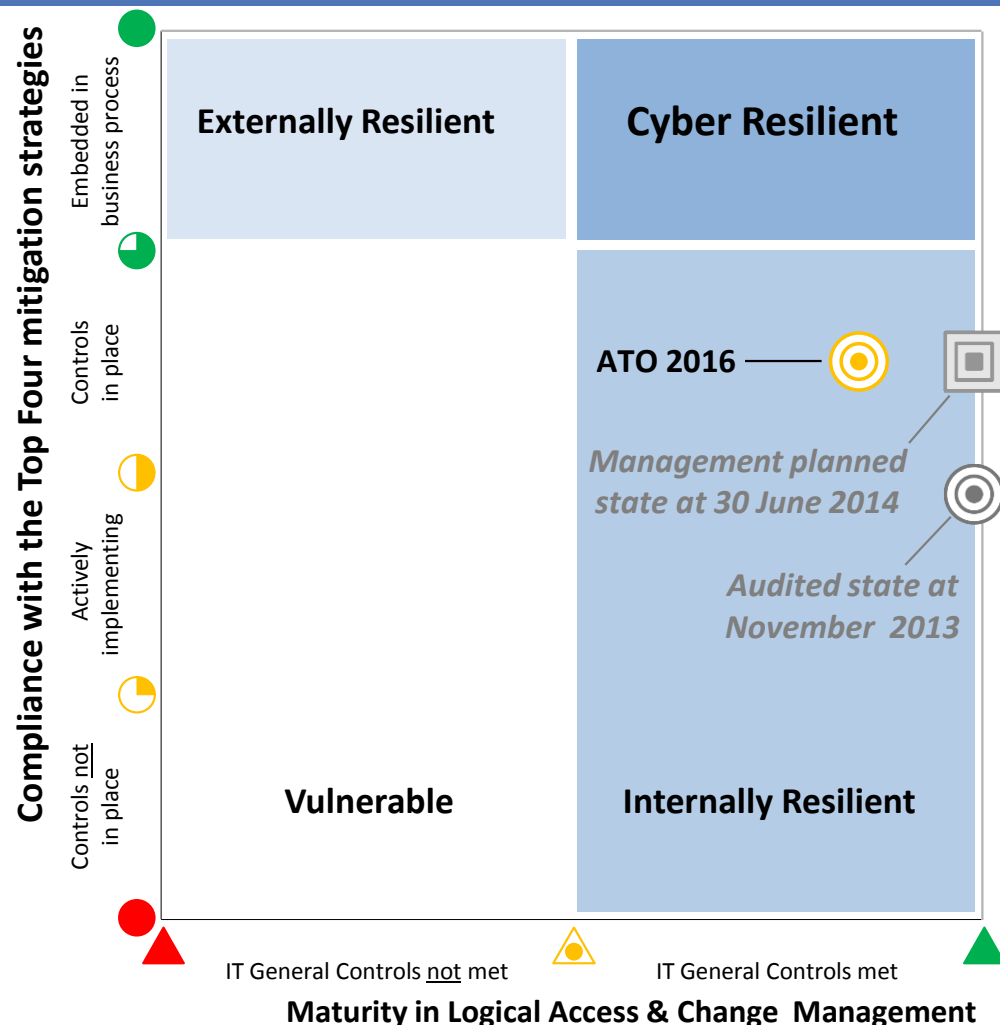
Comparing 2013 to 2016 by Entity

Department of
Human Services



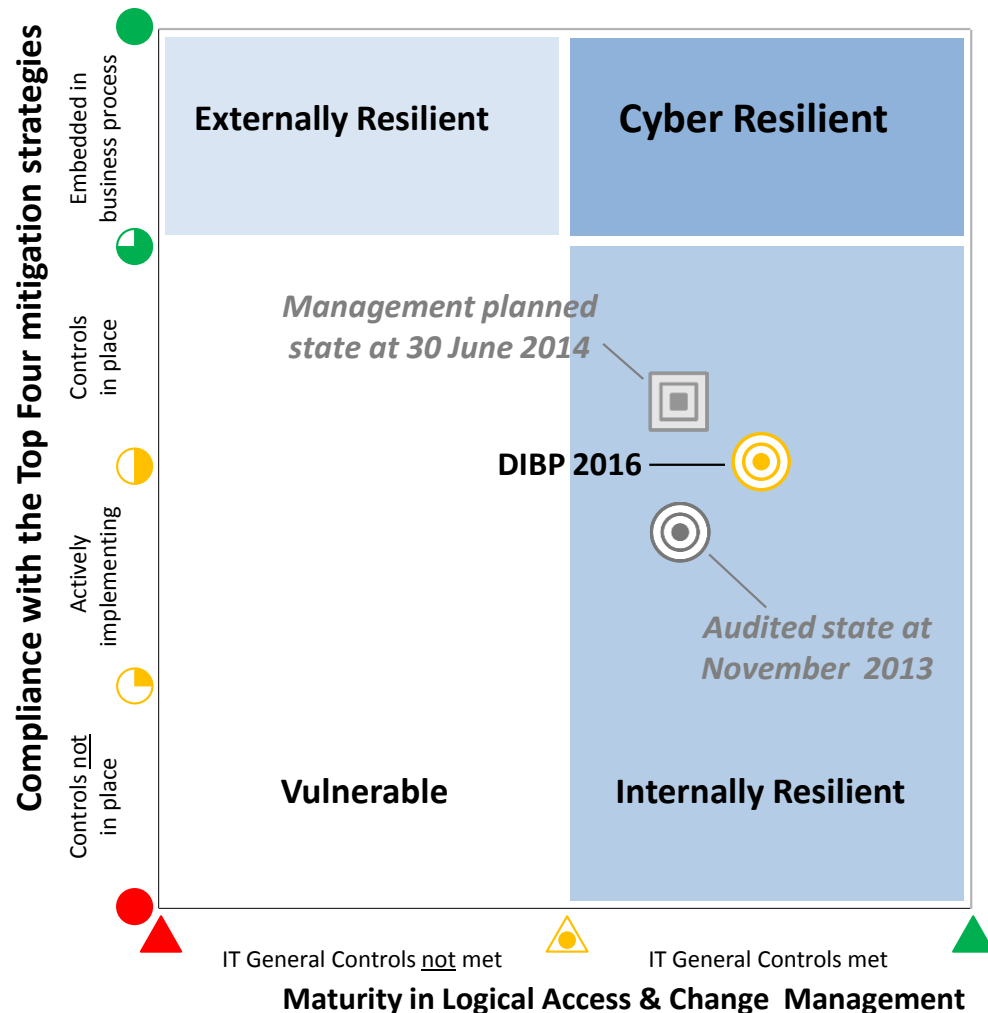
Comparing 2013 to 2016 by Entity

Australian
Taxation Office



Comparing 2013 to 2016 by Entity

Department of
Immigration and
Border Protection



Lessons learnt

Entities that choose to prioritise cybersecurity are better positioned to achieve cyber resilience. Being cyber resilient will help entities to effectively deter and respond to cyber attacks while still focusing on delivering business outcomes.

Entities that do not manage cybersecurity as a strategic priority and that do not have effective governance arrangements in place will find it increasingly difficult to be cyber resilient.