

Cyber Resilience

Across Entities

© Commonwealth of Australia 2016

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-149-8 (Print)

ISBN 978-1-76033-150-4 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit

<http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <http://www.itsanhonour.gov.au/>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Executive Director

Corporate Management Branch

Australian National Audit Office

19 National Circuit

BARTON ACT 2600

Or via email:

communication@anao.gov.au.



Canberra ACT
5 May 2016

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit across entities titled *Cyber Resilience*. The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—<http://www.anao.gov.au>.

Yours sincerely



Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Fax: (02) 6203 7777
Email: ag1@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Contents

Summary and recommendations.....	7
Background	7
Audit approach	7
Conclusion.....	7
ICT security posture matrix	8
Recommendations.....	10
Summary of entities' responses	10
Audit Findings.....	13
1. Background	15
Introduction	15
Audit approach	17
2. Have entities achieved compliance with Australian Government requirements?	19
Are mandatory information security strategies effectively deployed?	19
Are entities Cyber Secure?	29
3. Have entities achieved their overall information security posture?	35
What comparisons can be made between audited entities in 2013 and 2015?.....	35
What are the characteristics of an entity in the Cyber Resilient zone?	39
Appendices	43
Appendix 1 Responses from the selected entities.....	45
Appendix 2 Glossary	51
Appendix 3 Audit criteria and compliance statement.....	52

Summary and recommendations

Background

1. In June 2014, the Australian National Audit Office tabled in Parliament ANAO Audit Report No.50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems*. The report examined implementation of the mandatory strategies in the *Australian Government Information Security Manual* (ISM).
2. The Joint Committee of Public Accounts and Audit (JCPAA) held a public hearing to examine Report No.50 on 24 October 2014. The Committee was concerned that the seven entities audited were not compliant with the 'Top Four' strategies in the ISM. And that none of the entities were expected to achieve compliance by the mandated target date of 30 June 2014.
3. In light of concerns about entities' shortcomings to achieve compliance, the JCPAA asked the Auditor-General to extend the coverage of the audit to include other entities. In response to the JCPAA, a performance audit was scheduled to assess another four selected entities' compliance with Australian Government requirements.¹ This report is the outcome of the audit.

Audit approach

4. The audit objective was to assess selected entities' compliance with the four mandatory ICT security strategies in the *Australian Government Information Security Manual* (ISM).
5. To form a conclusion against the audit objectives, the selected entities' administration was assessed against the following high-level criteria:
 - entity-level implementation of the 'Top Four' strategies mandated in the ISM; and
 - overall ICT security posture.

Conclusion

6. All entities made efforts to achieve compliance with the mandated strategies in the ISM. Two of the four selected entities achieved compliance—AUSTRAC and the Department of Agriculture and Water Resources. Two entities did not achieve compliance—Australian Federal Police and the Department of Industry, Innovation and Science.
7. The ANAO has made three recommendations aimed at achieving compliance with mandated strategies in the ISM. The recommendations are likely to apply to other Australian Government entities not specifically examined in this audit.

1 Four entities under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) were included in the audit. The entities were the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC), the Department of Agriculture and Water Resources, and the Department of Industry, Innovation and Science. The entities were selected based on the character and sensitivity of the information collected, stored and reported by the entity.

ICT security posture matrix

8. The ANAO’s summary findings for each of the selected entities are reported in the form of a matrix. This matrix indicates entities’ overall compliance with mandated strategies in the ISM and the underpinning IT general controls.² An entity’s position on the matrix indicates its overall ICT security posture—in essence how well the entity is protected from external intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

9. The matrix indicates where entities are positioned in terms of Cyber Resilience zones: *vulnerable zone*; *externally resilient zone*; *internally resilient zone*, and *cyber resilient zone*. The zones are explained further in Table S.1 and illustrated in Figure S.1.

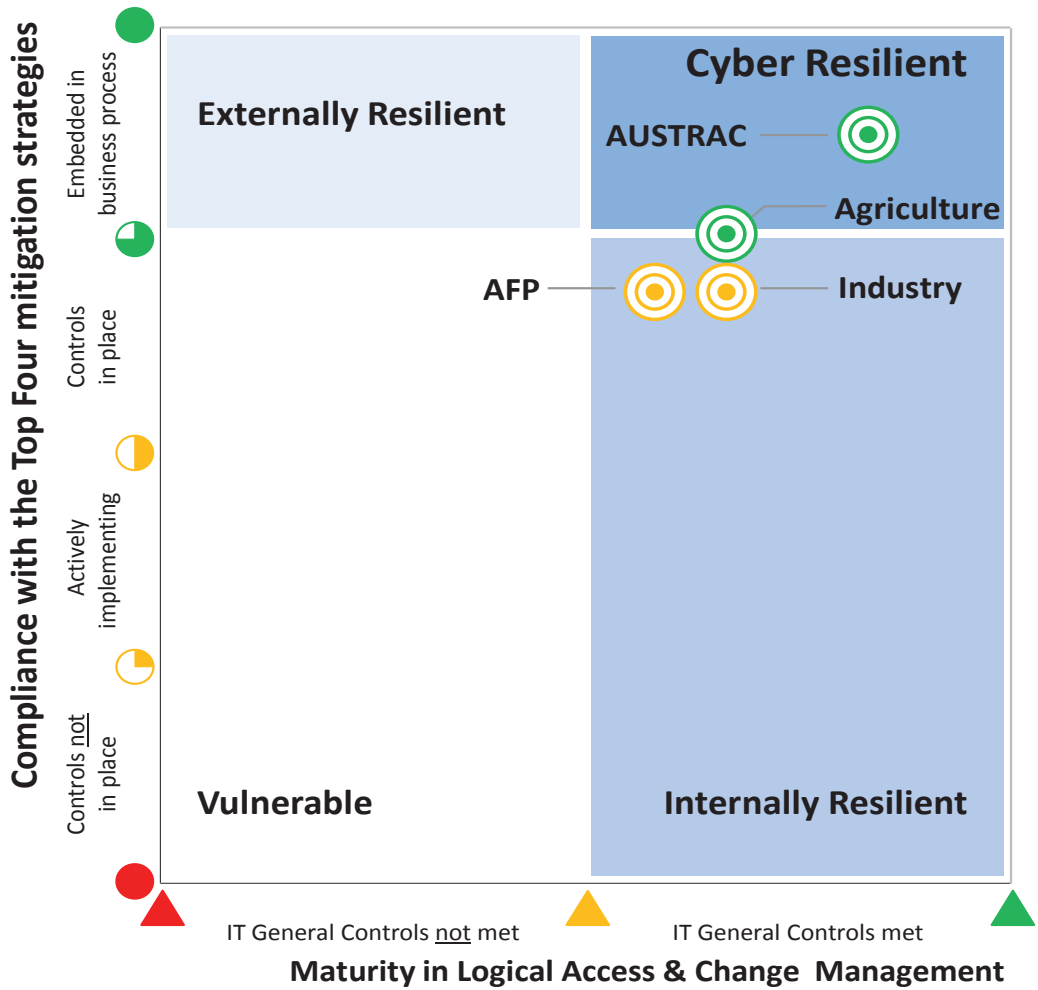
Table S.1: Definition of the Cyber Resilience zones

Zone scheme	Definition of the Cyber Resilience zones
Vulnerable Zone	High-level of exposure and opportunity for external attacks and internal breaches and disclosures of information.
Externally Resilient Zone	A level of protection from attacks and intrusions from external sources but vulnerabilities remain to breaches and disclosures from internal sources.
Internally Resilient Zone	A level of protection from breaches and disclosures of information from internal sources but vulnerabilities remain to attacks from external sources.
Cyber Resilient Zone	High-level of protection from external attacks and internal breaches and disclosures of information.

Source: ANAO.

2 As defined by ISACA—the international association that set guidelines and frameworks for IT Auditors—IT General Controls are policies and procedures developed to deal with risks, including controls in relation to ICT governance, ICT infrastructure, security and access to operating systems and databases, and program change and testing procedures.

Figure S.1: Entity ICT security posture



GRADING SCHEME:

- Control not in place and no dispensation authorised by the Accountable Authority.
 - ◐ Control not in place but a dispensation is authorised by the Accountable Authority.
 - ◑ Control not in place but entity is actively implementing, with a minimum of design deliverables in evidence.
 - ◒ Control in place and meeting control objectives.
 - Control in place and maintenance is part of business processes, including monitoring and taking corrective action as required.
- ▲ Control objective not met.
 - ▲ Identified controls not in place but compensating controls in place and observed.
 - ▲ Control objective is met.

Source: ANAO.

Recommendations

Recommendation No.1 Entities establish processes to monitor patch levels across their enterprise ICT systems.

Para 2.16

Response from selected entities: *Agreed.*

Recommendation No.2 That entities:

Para 2.26

- (a) conduct periodic assessments on the effectiveness of IT security controls across their enterprise ICT systems;
- (b) decide on the optimal and/or desired ICT security posture; and
- (c) define strategies to achieve and maintain the desired ICT security posture.

Response from selected entities: *Agreed.*

Recommendation No.3 That entities:

Para 2.39

- (a) capture and store audit logs for privileged user accounts; and
- (b) actively monitor privileged user accounts for unauthorised access and inappropriate behaviour, preferably with the support of a security information and event management (SIEM) tool.

Response from selected entities: *Agreed.*

Summary of entities' responses

Australian Federal Police (AFP)

The AFP agrees that the report is an accurate assessment of the agency's compliance state as at July 2015.

The AFP supports the recommendations of the report, noting that the audit has identified some areas for improvement. The AFP has established programs of work to implement the recommendations.

Australian Transaction Reports and Analysis Centre (AUSTRAC)

AUSTRAC has reviewed this report and supports all findings. We will continue to optimise cyber security capability, processes, and systems in line with ANAO recommendations, ASD advice, and the agency's approach to risk. The audit identified some areas for improvement and work is underway to address those.

AUSTRAC acknowledges the ongoing effort by all staff in contributing to an organisational culture of resilience and high performance that is fundamental in delivering our outcomes. The audit findings also reflect the long term commitment of our ICT teams to securing our systems.

Department of Agriculture and Water Resources

The department has had a programme of investment over the past four years to improve its security posture. Our most recent investment is an implementation of the Security Information and Event Management System (SIEM) that will support detection of possible trusted insider

threats particularly through monitoring privileged user accesses. The department will continue to focus on our ability to identify ICT risk in the area of privileged user access.

The department takes great pride in being compliant with the top 4 mitigation strategies and continues to review and improve in all 35 mitigation strategies and each of the underlying controls.

Department of Industry, Innovation and Science

The Department of Industry, Innovation and Science acknowledges the Australian National Audit Office's (ANAO) report on *Cyber Resilience*, and accepts the audit's findings that the department was not fully compliant, at the time of the audit, with the mandated strategies in the ISM.

Although the report highlights the department, at the time of the audit, was not fully compliant, since the audit was completed steps have been taken to address the identified shortcomings. Those steps were undertaken as part of an existing work programme.

Audit Findings

1. Background

Introduction

1.1 For some years, the Australian Government has established both an overarching protective security policy framework, and promulgated specific ICT risk mitigation strategies and related controls. In 2013, the Government mandated elements of the framework in response to the rapid escalation, intensity and sophistication of cyber crime and other cyber security threats.³

1.2 In June 2014, the Australian National Audit Office tabled in Parliament ANAO Audit Report No.50 2013-14, *Cyber Attacks: Securing Agencies' ICT Systems*. The report examined implementation of the mandatory strategies in the ISM across seven Australian Government entities.

1.3 The ANAO made three recommendations aimed at achieving compliance with mandated strategies in the ISM. The recommendations were likely to apply to other Australian Government entities not specifically examined in that audit.

Mitigation strategies

1.4 The Attorney-General's Department (AGD) is responsible for administering the Australian Government's protective security policy. This policy promotes ways to secure the delivery of Government business. AGD's *Protective Security Policy Framework (PSPF)*⁴ outlines the core requirements for the effective use of protective security. The PSPF assists entities to:

- identify their levels of security risk tolerance;
- develop an appropriate security culture; and
- achieve the mandatory protective security requirements expected by the Government.

1.5 The PSPF is supported by the *Australian Government Information Security Manual (ISM)*⁵, which is released by Australian Signals Directorate (ASD).⁶ The ISM is the standard governing the security of government ICT systems. The ISM is intended to assist entities to apply a risk-based approach to protecting their information and systems.

1.6 In 2010, ASD developed a list of 35 strategies to assist Australian Government entities achieve the desired level of control over their systems and mitigate the risk of cyber intrusions. ASD has advised that if implemented, the top four mitigation strategies would prevent at least 85 per cent of the targeted cyber intrusions to an entity's ICT systems. This list of strategies is revised annually based on the most recent analysis of incidents.

3 Attorney-General's Department, *Australian Government Cyber Security Strategy*, Canberra, 2009, p. vii.

4 The PSPF was first released in June 2010, with several subsequent amendments. In April 2013, the PSPF was updated to include four mandatory strategies and related controls to mitigate targeted cyber intrusions.

5 The ISM complements the PSPF, and is part of the Australian Government's strategy to enhance its information security capability.

6 The Australian Signals Directorate, located within the Department of Defence, is Australia's national authority for signals intelligence and ICT security. In accordance with the *Information Security Act 2001*, ASD provides material, advice and other assistance to Commonwealth and state authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means. The Directorate was re-named the Australian Signals Directorate in 2013.

1.7 The current top four mitigation strategies are:

- **application whitelisting:** designed to protect against unauthorised and malicious programs executing on a computer. This strategy aims to ensure that only specifically selected programs can be executed⁷;
- **patching applications:** applying patches to applications and devices to ensure the security of systems⁸;
- **patching operating systems:** deploying critical security patching to operating systems to mitigate risk vulnerabilities; and
- **minimising administrative privileges:** restricting administrative privileges provides an environment that is more stable, predictable, and easier to administer and support as fewer users can make changes to their operating environment.^{9,10}

1.8 Effective implementation of the mandated strategies assists entities to control their ICT systems. And provides a higher level of assurance that systems will support business services.

1.9 An amendment to the PSPF issued in April 2013 mandated the top four mitigation strategies. It set a target date of July 2014 for implementation.

Shortcomings in implementing mandated strategies

1.10 The Joint Committee of Public Accounts and Audit (JCPAA) held a public hearing to examine Report No.50 on 24 October 2014. The Committee was concerned that the seven entities audited were not compliant with the 'Top Four' strategies in the ISM. And that none of the entities were expected to achieve compliance by the mandated target date of 30 June 2014.

1.11 In light of concerns about entities' shortcomings to achieve compliance, the JCPAA asked the Auditor-General to extend the coverage of the audit to include other entities. In response to the JCPAA, two related performance audits are scheduled:

- a follow-up audit to re-assess the entities examined in Report No.50. The report is scheduled to be tabled in Parliament in late 2016; and
- assess another four selected entities' compliance with Australian Government requirements. This report covers the additional four selected entities.

7 Defence Signals Directorate, *Application whitelisting explained* [Internet], 2012, available from <http://www.dsd.gov.au/publications/csocprotect/application_whitelisting.htm> [accessed 23 May 2013]. Defining a list of trusted executables—a whitelist—is a more practical and secure method of securing a system than prescribing a list of bad executables to be prevented from running—a blacklist.

8 Defence Signals Directorate, *Assessing security vulnerabilities and patches* [Internet], 2012, available from <http://www.dsd.gov.au/publications/csocprotect/assessing_security_vulnerabilities_and_patches.htm> [accessed 23 May 2013]. A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data; this includes fixing security vulnerabilities.

9 Defence Signals Directorate, *Minimising administrative privileges explained*, 2012, available from <http://www.dsd.gov.au/publications/csocprotect/minimising_admin_privileges.htm> [accessed 23 May 2013]. System administrators typically have greater access rights to systems and information than normal users.

10 CERT Australia advises business to use the Top Four mitigation strategies. CERT Australia is the national computer emergency response team within AGD, which works with major Australian businesses to provide cyber security advice and support to critical infrastructure and other systems of national interest. See Attorney-General's Department, CERT Australia, *Cyber Crime & Security Survey Report 2013*, p. 20.

Selected entities in this audit

1.12 Four entities under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) were included in the audit:

- Australian Federal Police (AFP)¹¹;
- Australian Transaction Reports and Analysis Centre (AUSTRAC)¹²;
- Department of Agriculture and Water Resources¹³; and
- Department of Industry, Innovation and Science.¹⁴

1.13 The entities were selected based on the character and sensitivity of the information collected, stored and reported by the entity. Table 1.1 outlines the type of information held by each entity.

Table 1.1: Key information collected, stored and used by the selected entities

Australian Government entity	Economic and/or commercial information	Policy and/or regulatory information	National security information	Program and service delivery	Personal information
Australian Federal Police			✓	✓	✓
Australian Transaction Reports and Analysis Centre	✓	✓	✓		✓
Department of Agriculture and Water Resources	✓	✓		✓	✓
Department of Industry, Innovation and Science	✓	✓		✓	✓

Source: ANAO analysis.

Audit approach

1.14 The audit objective was to assess selected entities' compliance with the four mandatory ICT security strategies and related controls in the *Australian Government Information Security Manual* (ISM).

1.15 To form a conclusion against the audit objectives, the audit examined:

- entity-level implementation of the 'Top Four' strategies mandated in the ISM¹⁵; and
- overall ICT security posture.^{16 17}

11 AFP is a prescribed entity in the Attorney-General's Portfolio.

12 AUSTRAC is a prescribed entity in the Attorney-General's Portfolio—it is Australia's anti-money laundering and counter-terrorism financing regulator, and specialist financial intelligence unit.

13 The Department of Agriculture and Water Resources is a Department of State.

14 The Department of Industry, Innovation and Science is a Department of State.

15 Table A.1 in Appendix 3 outlines the criterion and compliance statements used to assess whether the entities were fully implementing the mandatory mitigation strategies and related controls.

16 Table A.2 in Appendix 3 outlines the criterion and compliance statements used to assess whether the entities were fully implementing the IT general controls across their systems.

1.16 The methodology employed for the audit involved:

- interviewing key ICT security personnel, namely the Chief Information Security Officer (CISO), the Information Technology Security Advisor (ITSA), and a selection of officers with the role of Information Technology Security Managers (ITSMs) and Information Technology Security Officers (ITSOs);
- reviewing the work of internal audit to assess compliance with the ISM;
- examining user access controls that support standard and administrative privileged accounts; and
- examining change management processes that support the authorisation for patching and testing of applications and operating systems.

1.17 An audit methodology was prepared to examine key business and information management systems in preference of assessing other application systems. Test controls were prepared that were non-vendor specific. This approach was adopted to ensure a consistent assessment, grading and reporting was in place across the selected entities.¹⁸

1.18 To support the development of test protocols against the mandatory strategies in the ISM, the audit referenced international policy and practices that informed the PSPF, ISM and the *Top 35 strategies to mitigate targeted cyber intrusions*. Reports referenced, but not limited to, include: National Security Agency's *Critical controls for effective cyber defense*¹⁹ and the National Institute of Standards and Technology's *Security and privacy controls for federal information systems and organisations*.²⁰

1.19 The audit fieldwork was conducted between May and October 2015.

1.20 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of approximately \$643 600.

Reporting on audit findings

1.21 In this audit, the ANAO departed from its usual practice of identifying entities on individual issues due to the risk of disclosing sensitive information about entity ICT security. Security weaknesses are addressed at an aggregate level. A summary assessment of each entity's performance against the audit objective is provided in Figure 2.2.

17 These are logical access and change management controls. Logical access controls prevent unauthorised access to ICT resources (including files, data and applications) and the associated administrative procedures. Change management controls ensure that standardised methods and procedures support the formal request for a change to ICT systems.

18 The following applications were assessed. For business applications: Microsoft Office, Java, and Abode Reader. For Financial Information Management Systems (FMIS): SAP or E5. For Human Resource Information Management System (HRMIS): SAP, PeopleSoft or Aurion.

19 In 2008, the Office of the Secretary of Defense (US) asked the National Security Agency (NSA) for help in prioritizing the myriad of security controls that were available for cybersecurity. Led by the NSA, a public-private consortium was established with representation from over 50 organisations that led to the definition of the 'Twenty Critical Controls'. By 2011, Australia, the UK and Canada had adopted the critical controls as a framework against targeted cyber intrusions.

20 NIST Special Publication 800-39 revision 4 provides guidance on managing information security risk.

2. Have entities achieved compliance with Australian Government requirements?

Areas examined

This chapter examines the selected entities' compliance with the four mandatory *Australian Government Information Security Manual* (ISM) strategies and related controls that protect ICT systems.

Conclusion

Two of the selected entities are located in the *Cyber Resilient* zone—and achieved compliance with the *Protective Security Policy Framework* (PSPF) and ISM. These entities had security controls in place to provide a high-level of protection from external attacks and internal breaches and disclosure of information.

The other two selected entities are located in the *Internally Resilient* zone—and did not achieve compliance. These entities had security controls in place to provide a level of protection from breaches and unauthorised disclosures of information from internal sources. There was insufficient protection against cyber attacks from external sources.

Areas for improvement

The ANAO made three recommendations aimed at achieving compliance with mandated strategies in the ISM.

Are mandatory information security strategies effectively deployed?

The mandatory strategies in the ISM are deployed across each of the entity's ICT environments but at various states of effectiveness. For two of the four entities, further initiatives are required to achieve compliance with the ISM.

Entity compliance

2.1 Under the PSPF, entities must satisfy INFOSEC 4. INFOSEC 4 is a key PSPF requirement which states that entities must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently.

2.2 Based on the PSPF and ISM requirements, the ANAO anticipated that entities would have the following security controls in place across their systems:

- application whitelisting deployed on desktops and servers;
- policy and procedures for the security patching of applications and operating systems, supported by a change management process that supports the authorisation of patching and testing; and
- effective management of standard and administrative privileged accounts, underpinned by ICT security controls for logical access across the systems' layers—network, application, database and operating systems.

Application whitelisting deployed on desktops and servers

2.3 Application whitelisting is a control which protects against unauthorised applications executing on a system.²¹ Table 2.1 provides a summary assessment of entity compliance with the seven controls that support application whitelisting.

Table 2.1: Summary assessment of entities' compliance with application whitelisting controls across the desktop and servers

Control [ISM control number]	No. of entities per grade				
Application Whitelisting					
Agencies must implement application whitelisting as part of the SOE for both workstations and servers. [ISM 0843]					4
Grade for Desktop					
Grade for Servers	2		1	1	
Agencies must prevent a user from running arbitrary executables. [ISM 0844]	1				3
Agencies must restrict a user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties. [ISM 0845]	1				3
Agencies must ensure that a user cannot disable the application whitelisting mechanism. [ISM 0846]					4
Agencies must ensure that application whitelisting does not replace antivirus and other Internet security software already in place for a system. [ISM 0847]					4
Agencies must ensure that system administrators are not exempt from application whitelisting policy. [ISM 0848]					4
Agencies must ensure that the default policy is to deny the execution of software. [ISM 0849]					4
KEY:	Control <u>not</u> in place and <u>no</u> dispensation authorised by the Accountable Authority				
	Control <u>not</u> in place but a dispensation is authorised by the Accountable Authority				
	Control <u>not</u> in place but entity is actively implementing, with a minimum of design deliverables in evidence				
	Control in place and meeting control objectives				
	Control in place and maintenance is part of business processes including monitoring and taking corrective action as required				

Source: ANAO analysis.

21 According to ASD, application whitelisting can be an effective mechanism to prevent the compromise of systems resulting from the exploitation of vulnerabilities in an application or from the execution of malicious code. Defining a list of trusted applications—a whitelist—is a more practical and secure method of securing a system than prescribing a list of bad applications to be prevented from running—a blacklist.

2.4 All entities had implemented application whitelisting on their desktop systems. Three types of application whitelisting tools were in use by the entities subject to audit: *Symantec Endpoint Protection*; *McAfee Application Control for Desktops*; and *Microsoft AppLocker*. Application whitelisting rules—a set of protocols to identify executable files—were found to be a combination of path-based and hash-based rules. Path-based rules were widely in use for application control for both local and network locations. However, there is evidence hash-based rules are more frequently applied for more recently authorised applications to the policy.

2.5 Only two entities had implemented application whitelisting on their enterprise servers. Where entities did not have application whitelisting deployed on servers, there were initiatives underway to deploy a security information and event management (SIEM) tool. The deployment of SIEM is a mitigating security control for application whitelisting but does not replace the security protection afforded by a whitelisting policy and/or application control.

2.6 Whitelisting rules were found not to be periodically assessed to ensure unused applications were removed from the authorised list of departmental applications.

2.7 One entity had implemented a ‘step’ in the change management process to highlight a likely update to the whitelisting rules. This step better informs and supports the coordinated change release. New change requests were required to record a likely amendment to whitelisting rules. This alert—in the form of a check box—would seek authorisation to:

- deploy a new application;
- update an existing application; or
- remove an application from the network.

Policies and procedures for security patching of applications and operating systems

2.8 Security patching²² involves the periodic deployment of software releases designed to fix problems with existing software. According to Australian Signals Directorate (ASD), security patching to applications, operating systems and devices is one of the most effective security practices to protect the security of ICT systems.

2.9 ASD provides guidance on assessing announced vulnerabilities and patches to determine the risk they pose, and guidelines for patch deployment. According to ASD, a responsive and effective security patch management strategy relies on a lifecycle of:

- assessing security vulnerabilities and patches;
- vulnerability–patch risk assessment;
- patch deployment timeframes; and
- patch testing.²³

22 A patch is a piece of computer code that is inserted into an existing program to fix problems or to improve usability and performance.

23 Australian Signals Directorate, *Assessing Security Vulnerabilities and Patches* [Internet], 2013, available from <http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm> [accessed 2 March 2015].

2.10 Entities made efforts to adhere to their patch management policy. Practices were in place to deploy vendor-recommended updates for business and corporate applications in an efficient and timely manner.

2.11 There are several tools available which are capable of providing patches to applications and operating systems, as well as monitoring and auditing their patch levels. All four selected entities used Microsoft’s *System Centre Configuration Manager (SCCM)*. SCCM is built upon the framework of the *Windows Server Update Services (WSUS)*. Unlike WSUS, SCCM is capable of managing a geographically dispersed fleet of computing assets, and if configured correctly, can manage both Microsoft and third-party applications.²⁴

2.12 Table 2.2 provide a summary assessment of the selected entities’ compliance with the five controls that support the patching of applications; and with the five controls that support the patching of operating systems at the desktop and servers.

Table 2.2: Summary assessment of entities’ compliance with controls to patch applications, and patch desktop and server operating systems

Control [ISM control number]	No. of entities per grade				
Patching Applications					
Agencies must apply all security patches as soon as possible. [ISM 0940]				4	
Agencies must have a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities. [ISM 1143]				3	1
Agencies must apply all critical security patches within two days. [ISM 1144]	1		2	1	
Agencies must install the latest version of applications as soon as possible. [ISM 1348]			1	2	1
Agencies must install the latest version of applications within two days if the upgrade addresses a critical security vulnerability. [ISM 1349]	1		3		
KEY:	Control <u>not</u> in place and <u>no</u> dispensation authorised by the Accountable Authority				
	Control <u>not</u> in place but a dispensation is authorised by the Accountable Authority				
		Control <u>not</u> in place but entity is actively implementing, with a minimum of design deliverables in evidence			
			Control in place and meeting control objectives		
				Control in place and maintenance is part of business processes including monitoring and taking corrective action as required	

24 Vendors use different means of communicating vulnerability severity, and will respond by releasing security fixes with either a security patch, or with a new version of the application. WSUS only manages security notification and fixes for Microsoft products; however, SCCM is configurable to manage security fixes for most third-party applications.

Have entities achieved compliance with Australian Government requirements?

Control [ISM control number]		No. of entities per grade				
Patching Operating Systems						
Agencies must apply all security patches as soon as possible. [ISM 0940]	Grade for Desktop				2	2
	Grade for Servers			2	1	1
Agencies must have a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities. [ISM 1143]	Grade for Desktop				3	1
	Grade for Servers			1	2	1
Agencies must apply all critical security patches within two days. [ISM 1144]	Grade for Desktop	1		2	1	
	Grade for Servers	3			1	
Agencies must install the latest version of operating systems as soon as possible. [ISM 1348]	Grade for Desktop				3	1
	Grade for Servers			2		2
Where known vulnerabilities cannot be patched, or security patches are not available, agencies must implement one or more controls to: resolve the vulnerability; prevent exploitation of the vulnerability; contain the exploit; or detect intrusions. [ISM 0941]	Grade for Desktop				2	2
	Grade for Servers			1	1	2
KEY:		Control <u>not</u> in place and <u>no</u> dispensation authorised by the Accountable Authority				
		Control <u>not</u> in place but a dispensation is authorised by the Accountable Authority				
		Control <u>not</u> in place but entity is actively implementing, with a minimum of design deliverables in evidence				
		Control in place and meeting control objectives				
		Control in place and maintenance is part of business processes including monitoring and taking corrective action as required				

Source: ANAO analysis.

2.13 For the period of October 2014 to April 2015, Microsoft had released several critical and important security patches for their applications and operating systems. For the entities subject to audit, the patch deployment result is below the industry standard of 95 per cent of network devices. By way of example, one critical security patch was successfully deployed across only 58 per cent of the desktops of one entity’s ICT network. The entity in question was not aware of the low patch levels, and did not have procedures in place to monitor and audit the effectiveness of the deployed patches.

2.14 Updates to the latest version of applications were *ad hoc*, with many applications deployed three or more months after vendor release. In some cases, more than two versions of a given application were deployed across the network.

2.15 Monitoring patch levels across the network are an important practice. Adopting this practice as part of the normal business process may provide better assurance that applications and operating systems are effectively patched, and will support to maintain the desired ICT security posture for the government entity.

Recommendation No.1

2.16 Entities establish processes to monitor patch levels across their enterprise ICT systems.

AFP's response: *Agreed.*

2.17 *The AFP has implemented a number of programs of work to address this recommendation with a planned implementation date of 1 July 2016.*

AUSTRAC's response: *Agreed.*

The Department of Agriculture and Water Resources response: *Agreed.*

2.18 *All patches applied to the department's ICT environments are implemented through appropriate, formal and internally managed and controlled Change Management processes to ensure an auditable level of accountability and approval.*

2.19 *The majority of the department's patches are handled by the department's primary outsourced ICT Services Provider, Hewlett Packard Enterprises (HPE). The department has processes and tools in place to ensure the HPE applied patches are consistent with our change management processes.*

The Department of Industry, Innovation and Science response: *Agreed.*

Management of standard and administrative privileged accounts

2.20 Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributing factor leading to reduced logical security. Administrative privileges are the highest level of permission, granted only to trusted personnel to enable them to configure, manage and monitor an ICT system. Ensuring that privileged accounts do not have a channel from within the entity to the Internet—such as email and web browsing capability—minimises opportunities for these accounts to be compromised. Furthermore, mechanisms to monitor privileged account activities and log user security events provide greater accountability and an audit trail.²⁵

2.21 Table 2.3 provides a summary assessment of the selected entities' compliance with the ISM control to minimise administrative privileges.

25 Chapter 4 of the *Interim Phase of the Audits of the Financial Statements of Major General Government Sector Entities* presents the results of the ANAO's assessment of selected elements of the IT control environments that underpin the processing of financial information used in the preparation of entities' financial statements. A focus of this chapter is IT security management arrangements to safeguarding the security and confidentiality of financial information. Key controls assessed include: general user and privileged user access management; network security; security governance; and security monitoring and reporting. Available at <<http://www.anao.gov.au/Publications/Audit-Reports/2014-2015/Interim-Phase-of-the-Audits-of-the-Financial-Statements-of-Major-General-Government-Sector-Entities>>

Table 2.3: Summary assessment of entities' compliance with controls for privileged access accounts

Control [ISM control number]	No. of entities per grade				
Minimising Administrative Privileges Agencies must: <ul style="list-style-type: none"> ensure that the use of privileged accounts is controlled and auditable ensure that system administrators are assigned a separate account for the performance of their administration tasks keep privileged accounts to a minimum allow the use of privileged accounts for administrative work only regularly audit the passphrases of privileged accounts to check they meet length or complexity requirements regularly audit the passphrases of privileged accounts to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts) regularly review privileges allocated to privileged user accounts. [ISM 0849] 					
KEY: Control <u>not</u> in place and <u>no</u> dispensation authorised by the Accountable Authority Control <u>not</u> in place but a dispensation is authorised by the Accountable Authority Control <u>not</u> in place but entity is actively implementing, with a minimum of design deliverables in evidence Control in place and meeting control objectives Control in place and maintenance is part of business processes including monitoring and taking corrective action as required				3	1

Source: ANAO analysis.

2.22 For the entities subject to audit, each had policies and procedures in place to control and manage the use of privileged user accounts, and included:

- granting and limiting privileged accounts only to staff with a business need, and authorised by the business owner of the data and/or ICT system;
- both standard and privileged accounts are created for privileged users, thereby segregating access to only authorised systems based on business needs;
- email accounts are not available to privileged accounts; however, there were instances where Administrative Users were granted email accounts to complete their duties; and
- security controls at the network layer is in place to prevent access to the Internet; and
- passphrases for privileged user accounts comply with the ISM.

2.23 For two of the selected entities, access to the network by privileged user required multifactor authentication, using a RSA token. As a further security control, system administrators do not have direct access to the key systems in the network; instead they are required to log on to an intermediary computer—a 'jump box'—to elevate their access rights to server administrator

privilege in order to carry out maintenance work. Further, remote logon is prevented for network administrator accounts.

2.24 The process of granting and revoking privileged user accounts is performed in accordance with entities' policy. There is a lack of activity monitoring for unauthorised access and inappropriate behaviour of privileged users. This is a systemic control weakness that raises questions as to how effectively entities can identify, respond to, or investigate unauthorised access to privileged user accounts, or inappropriate activities by privileged users. Three of the four entities were taking steps to review their process of actively monitoring accounts.

2.25 Two of the selected entities had security control weakness for one or more of their enterprise information management systems, and include:

- *infrequent reviews of user access to the information systems.* By way of example, several staff retained access rights to the system when business use was no longer required;
- *the enforcement of segregation of duties for several accounts.* By way of example, five superusers in an application system also held privileged user access, thereby allowing these staff to administer system user access, and create and amend the employee master data; and
- *cessation procedures for accounts.* By way of example, six terminated APS staff had privileged user access to a system despite staff terminations taking place over 30 days earlier.

Recommendation No.2

2.26 That entities:

- (a) conduct periodic assessments on the effectiveness of IT security controls across their enterprise ICT systems;
- (b) decide on the optimal and/or desired ICT security posture; and
- (c) define strategies to achieve and maintain the desired ICT security posture.

AFP's response: *Agreed.*

2.27 *The AFP, via its Security Committee, regularly reviews its ICT security posture. The desired posture is reflected in the setting of the AFP's Cyber Security Alert Level.*

AUSTRAC's response: *Agreed.*

The Department of Agriculture and Water Resources response: *Agreed.*

2.28 *The department undertook a gap analysis covering the 35 strategies to mitigate targeted cyber intrusions identified by the Australian Security Directorate in May 2015 and is currently implementing the remainder of those recommendations from that analysis as well as commencing its biennial review of the 35 strategies for this calendar year.*

2.29 *The department will continue to invest in Cyber Security and believes that the plans, outlined below, will position the department firmly in the ANAO's cyber secure quadrant.*

2.30 *Since the audit into Cyber Resilience took place, the department has introduced a number of initiatives including Server Whitelisting and a Security Information and Event Management (SIEM) capability. We believe these capabilities would have moved us towards being 'safely' in the cyber secure quadrant.*

2.31 *The department's plan is to continue to:*

- (a) *Refine its ICT governance and change management procedures and processes;*
- (b) *Maintain the ICT security capabilities it already has in place from the investment of the last four years;*
- (c) *Expand the use of its Security Information and Event Management (SIEM) capability that became operational in late 2015 to accommodate all critical infrastructure and applications;*
- (d) *Progress with its current programme of work that includes introducing an updated Information Security Management Framework, Security Architecture, an Identity and Access Management system and an assessment of our key process capability based on the required standard, ISO/IEC 33020:2015; and*
- (e) *Upon completion of this programme the department will then engage an Independent Risk Assessment Process (IRAP) assessor to determine the effectiveness of the department's critical infrastructure and systems.*

2.32 *To maintain and enhance its position as 'cyber secure' the department will review its position against ASD cyber-security strategies biennially and then continually cycle through the five steps identified in its plans above.*

The Department of Industry, Innovation and Science response: *Agreed.*

2.33 *The department has a rolling program in place to review and update the relevant IT security policies and procedures, including those related to controls used across enterprise ICT systems.*

2.34 *The department's desired ICT security posture has been defined within the relevant ICT security strategic policies.*

IT general controls

2.35 An effective IT general controls²⁶ framework is an essential prerequisite for securing systems against cyber attacks. It creates layers of protection for critical systems elements against internal source threats and establishes a foundation for implementing controls directed against external source threats, including the mandated ISM strategies and related controls. Two elements of an IT general controls framework—logical access control and change management—are crucial as they relate directly to security management.

2.36 Entities had appropriate and effective logical access control and change management processes in place. The entities' performance in this regard is attributable to the level of attention given to those elements over time, including annual assessments by the ANAO in the context of financial statement audits.

2.37 An area for improvement relevant for most of the entities is the process of capturing audit logs and actively monitoring privileged user accounts. There was limited evidence to support an effective review procedure is in place to identify unauthorised access and inappropriate behaviour of privileged users. This is an issue that requires early attention, so as to reduce the risk of internal breaches and unauthorised disclosures of information stored on entity databases and information management systems.

2.38 Entities were aware of these shortfalls and were investigating multiple options. These include:

- instructing line managers and IT Security Advisors to actively monitor control systems for high risk profile events and unauthorised activities; and
- the merits of deploying a security information and event management (SIEM) tool to produce alerts in a near real time basis.

26 According to ISACA, IT general controls (ITGC) are the policies and procedures developed to deal with an entity's identified system risks. They include controls over ICT governance, ICT infrastructure, security and access to operating systems and databases, application acquisition and development, and program change procedures. Effective implementation of IT general controls provides a level of assurance that an entity's systems are protected from ICT security threats.

Recommendation No.3

2.39 That entities:

- (a) capture and store audit logs for privileged user accounts; and
- (b) actively monitor privileged user accounts for unauthorised access and inappropriate behaviour, preferably with the support of a security information and event management (SIEM) tool.

AFP's response: *Agreed.*

2.40 *The AFP has a program of work currently underway to replace its SIEM. Monitoring rules specifically relating to this recommendation have been developed and are currently being tested. The replacement capability is to be implemented in July 2016.*

AUSTRAC's response: *Agreed.*

The Department of Agriculture and Water Resources response: *Agreed.*

2.41 *The department commenced a project to implement a Security Information and Event Management (SIEM) capability in 2015. The SIEM is now operational and is actively capturing and storing activity logs, including privileged user accounts, across our ICT environment. This activity includes actions such as logons/logoffs, modification of other user accounts and account lockouts.*

2.42 *The SIEM alerts security staff in real-time for such activities where detection is critical, such as a privileged access being granted after normal business hours. In addition, the associated logs can be reviewed and analysed by security staff at any time after an alert is raised, for the purposes of investigation.*

2.43 *The department has a program of work in train to progressively ensure each of our critical and bespoke systems provide security related logging data into SIEM for appropriate analysis.*

The Department of Industry, Innovation and Science response: *Agreed.*

2.44 *The department has implemented a process to ensure all privileged user account audit logs across the environment are captured and stored.*

2.45 *The department currently actively monitors privileged user accounts with the use of a SIEM and behaviours analytics tool.*










Are entities Cyber Secure?

Two of the four selected entities were located in the *Cyber Resilient* zone. These entities had security controls in place to provide a high-level of protection from external attacks, internal breaches and unauthorised disclosure of information. These two entities had achieved compliance with the PSPF and ISM. The remaining two entities were not compliant with the ISM and required further initiatives to achieve compliance.

Assessing compliance

2.46 In order to assess compliance consistently across the four selected entities, the ANAO applied a set of assessment criteria and developed a graphical key²⁷; a reporting convention similar to a 'traffic light' report, as outlined in Table 2.4.

Table 2.4: Key to grading scheme for assessing compliance with the mandatory ISM strategies and IT general controls

Grading scheme for mandatory ISM strategies	Grading scheme for IT general controls
 Controls <u>not</u> in place and <u>no</u> dispensation authorised by the Accountable Authority.	 Control objectives <u>not</u> met.
 Controls <u>not</u> in place but a dispensation is authorised by the Accountable Authority.	 Identified controls <u>not</u> in place but compensating controls in place and observed.
 Controls <u>not</u> in place but entity is actively implementing, with a minimum of design deliverables in evidence.	 Control objectives met.
 Controls in place and meeting control objectives.	Entity Compliance Grade
 Control in place and maintenance is part of business processes, including monitoring and taking corrective action as required.	 Audited state at 30 October 2015.

Source: ANAO.

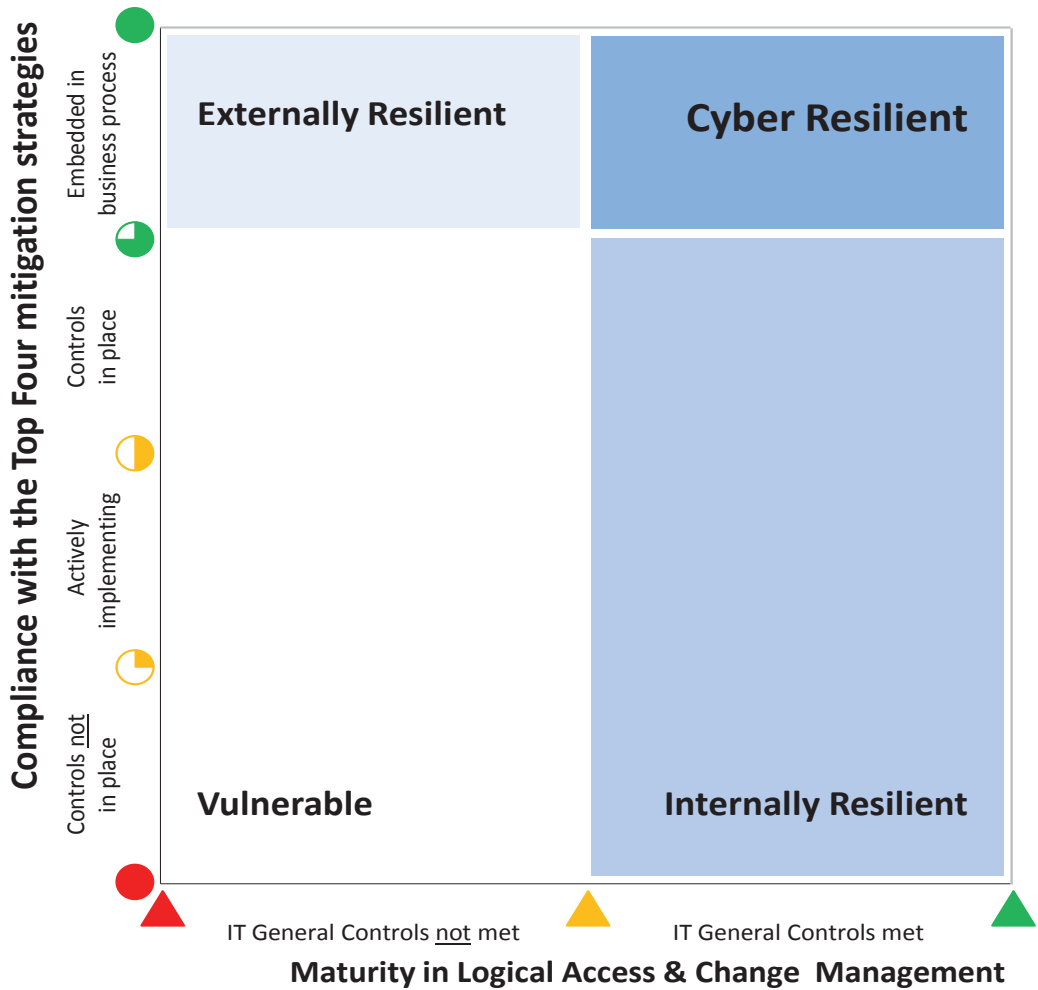
2.47 The selected entities were assessed on their:

- compliance with the top four mitigation strategies and related controls;
- maturity to effectively manage logical access and change management as part of normal business processes (IT general controls); and
- audited compliance state as at 30 October 2015.

2.48 The ANAO's summary findings for each of the selected entities are reported in the form of a matrix, shown in Figure 3.1. This matrix indicates entities' overall compliance with mandated strategies in the ISM and the underpinning IT general controls. It also grades where entities are positioned in terms of *Cyber Resilience* zones: *vulnerable zone*; *externally resilient zone*; *internally resilient zone*, and *cyber resilient zone*.

²⁷ The keys are represented as either a Harvey Ball or cone.

Figure 2.1: ICT security posture matrix



Source: ANAO.

2.49 The zones are explained further in Table 2.5 and illustrated in Figure 3.1. An entity's position indicates its overall ICT security posture—in essence how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and unauthorised disclosures, and how well it is positioned to address threats.

Table 2.5: Definition of the Cyber Resilience zones

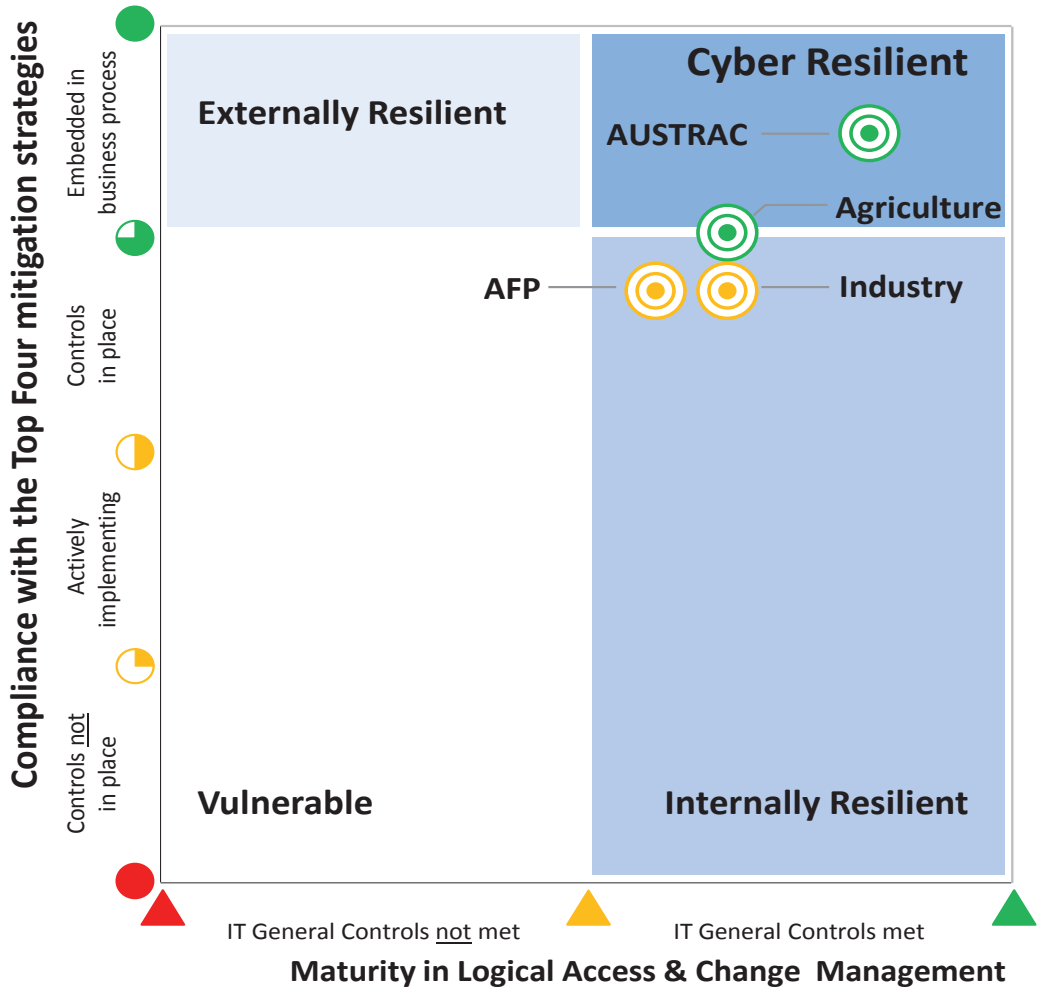
Zone scheme	Location of the Cyber Resilience zones in the matrix
<p>Vulnerable Zone</p> <p>High-level of exposure and opportunity for external attacks and internal breaches and disclosures of information.</p> <ul style="list-style-type: none"> • Top Four ISM strategies and IT general controls are <u>not</u> in place across the ICT systems, or inconsistently implemented across the system. 	
<p>Externally Resilient Zone</p> <p>A level of protection from attacks and intrusions from external sources but vulnerabilities remain to breaches and disclosures from internal sources.</p> <ul style="list-style-type: none"> • Top Four ISM strategies in place across the ICT systems and embedded as part of the normal business process. • IT general controls are <u>not</u> in place, or inconsistently implemented across the system. 	
<p>Internally Resilient Zone</p> <p>A level of protection from breaches and disclosures of information from internal sources but vulnerabilities remain to attacks from external sources.</p> <ul style="list-style-type: none"> • Top Four ISM strategies are <u>not</u> in place across the ICT systems, or inconsistently implemented across the system. • IT general controls for logical access and change management are met by the entity. 	
<p>Cyber Resilient Zone</p> <p>High-level of protection from external attacks and internal breaches and disclosures of information.</p> <ul style="list-style-type: none"> • Top Four ISM strategies in place across the ICT systems and embedded as part of the normal business process. • IT general controls for logical access and change management are met by the entity. 	

Source: ANAO.

Entity ICT security posture—summary assessment

2.50 Figure 2.2 summarises individual and comparative entity compliance with the ISM, as at 30 October 2015.

Figure 2.2: ICT security posture



GRADING SCHEME:

- Control not in place and no dispensation authorised by the Accountable Authority.
- Control not in place but a dispensation is authorised by the Accountable Authority.
- Control not in place but entity is actively implementing, with a minimum of design deliverables in evidence.
- Control in place and meeting control objectives.
- Control in place and maintenance is part of business processes, including monitoring and taking corrective action as required.
- ▲ Control objective not met.
- ▲ Identified controls not in place but compensating controls in place and observed.
- ▲ Control objective is met.

Source: ANAO analysis.

Security threat zones

2.51 Two of the selected entities are located in the *Cyber Resilient* zone. AUSTRAC and the Department of Agriculture and Water Resources achieved compliance with the ISM. These entities had security controls in place to provide a high-level of protection from external attacks and internal breaches and disclosure of information.

2.52 The other two selected entities are located in the *Internally Resilient* zone. Australian Federal Police and the Department of Industry, Innovation and Science did not achieve compliance with the ISM. These entities had security controls in place to provide a level of protection from breaches and unauthorised disclosures of information from internal sources. There was insufficient protection against cyber attacks from external sources. Further initiatives are required from these two entities to achieve compliance with the ISM.

3. Have entities achieved their overall information security posture?

Areas examined

This chapter examines the selected entities' overall ICT security posture, and considers how entities can improve levels of cyber resilience.

Conclusion

Entities that looked beyond the Top Four strategies in the ISM were better placed to manage their enterprise ICT systems from cyber attacks. These entities had revised their business model and ICT governance, and embedded security awareness as part of their enterprise culture.

Area for improvement

The ANAO has suggested that entities assess their ICT security posture against ASD's Top 35 Mitigation Strategies across their enterprise ICT systems so as to adopt an informed ICT security posture appropriate for their circumstances.

What comparisons can be made between audited entities in 2013 and 2015?

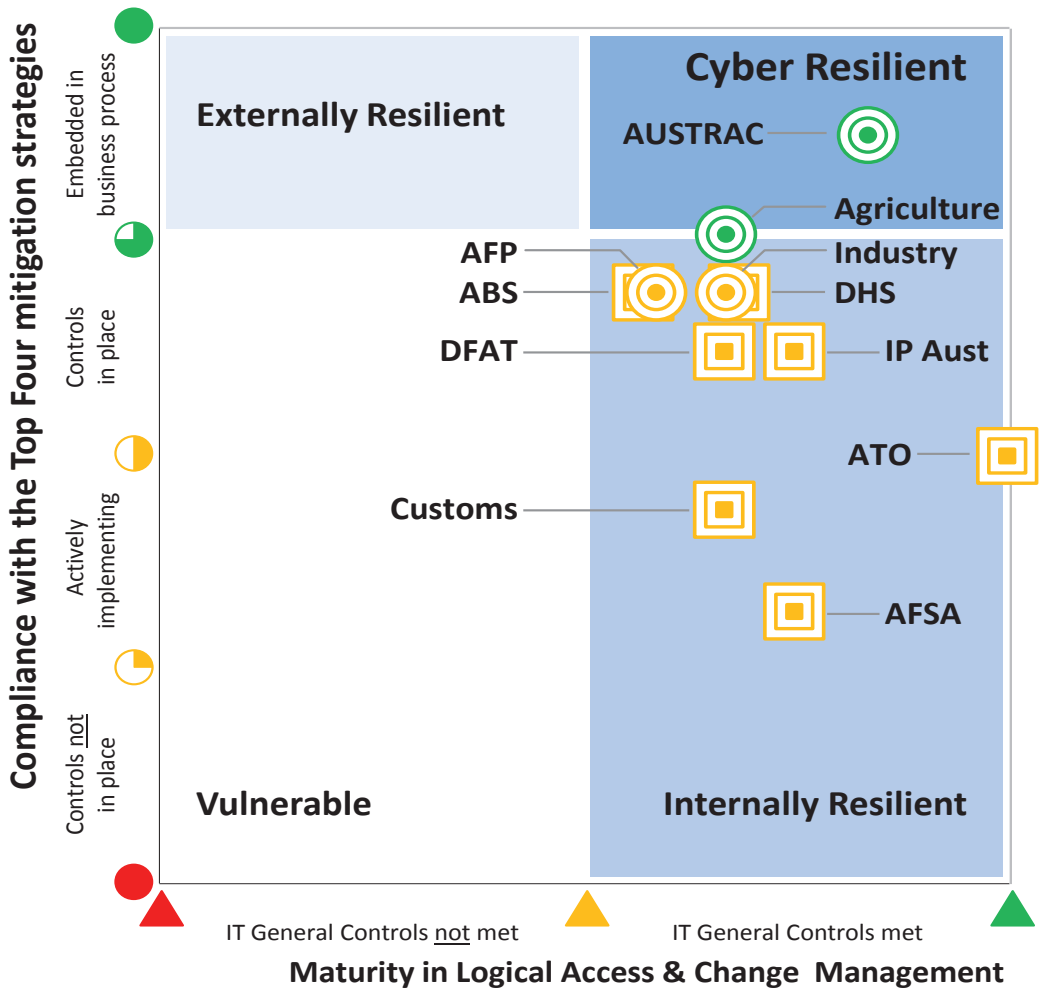
The seven entities in 2013 were aware that their enterprise ICT systems were not compliant, nor would be compliant with the ISM by the Government target date of 30 June 2014. Audit findings corroborated these assertions.

The entities in 2015 had self-reported their compliance with the ISM to the ANAO at the start of audit fieldwork. Only two of the four entities achieved compliance. The non-compliant entities had initiatives underway to achieve compliance, but they did not provide a timeframe when compliance would be achieved across their enterprise ICT systems.

3.1 The rapid escalation, persistence and sophistication of cyber attacks against government are increasingly a matter for executive management attention. Periodic assessment and review of an entity's ICT security posture can provide additional assurance on an entity's resilience to cyber attacks.

3.2 Figure 3.1 summarises the ICT security posture for the seven selected entities as at November 2013 and the four selected entities as at October 2015.

Figure 3.1: Comparing ICT security posture for audited entities in 2013 and 2015



- KEY:
- Entity ICT security posture, as assessed in November 2013
 - Entity ICT security posture, as assessed in October 2015

Source: ANAO analysis.

Summary assessment of entity compliance in 2013

3.3 Audit Report No.50 2013–14 reported that the seven entities had:

- established internal information security frameworks;
- implemented controls to safeguard the enterprise ICT systems from cyber attack; and
- change management processes in place to authorise the patching and testing of applications and operating systems.

3.4 These ICT security measures contributed to the protection of entity' ICT systems but were inadequate to achieve compliance with the mandatory strategies in the ISM. Further, none of the entities were expected to achieve compliance by the Government's target date of mid-2014, notwithstanding their advice regarding further initiatives which, when implemented, would strengthen ICT security controls and protection against cyber attacks.

3.5 The entities' overall ICT security posture was assessed as providing a level of protection from breaches and unauthorised disclosures of information from internal sources. Vulnerabilities remaining across their enterprise ICT systems against attacks from external sources.

3.6 The ANAO assessed the entities' plans to achieve compliance by 30 June 2014. Assessments were conducted for entity activities that were:

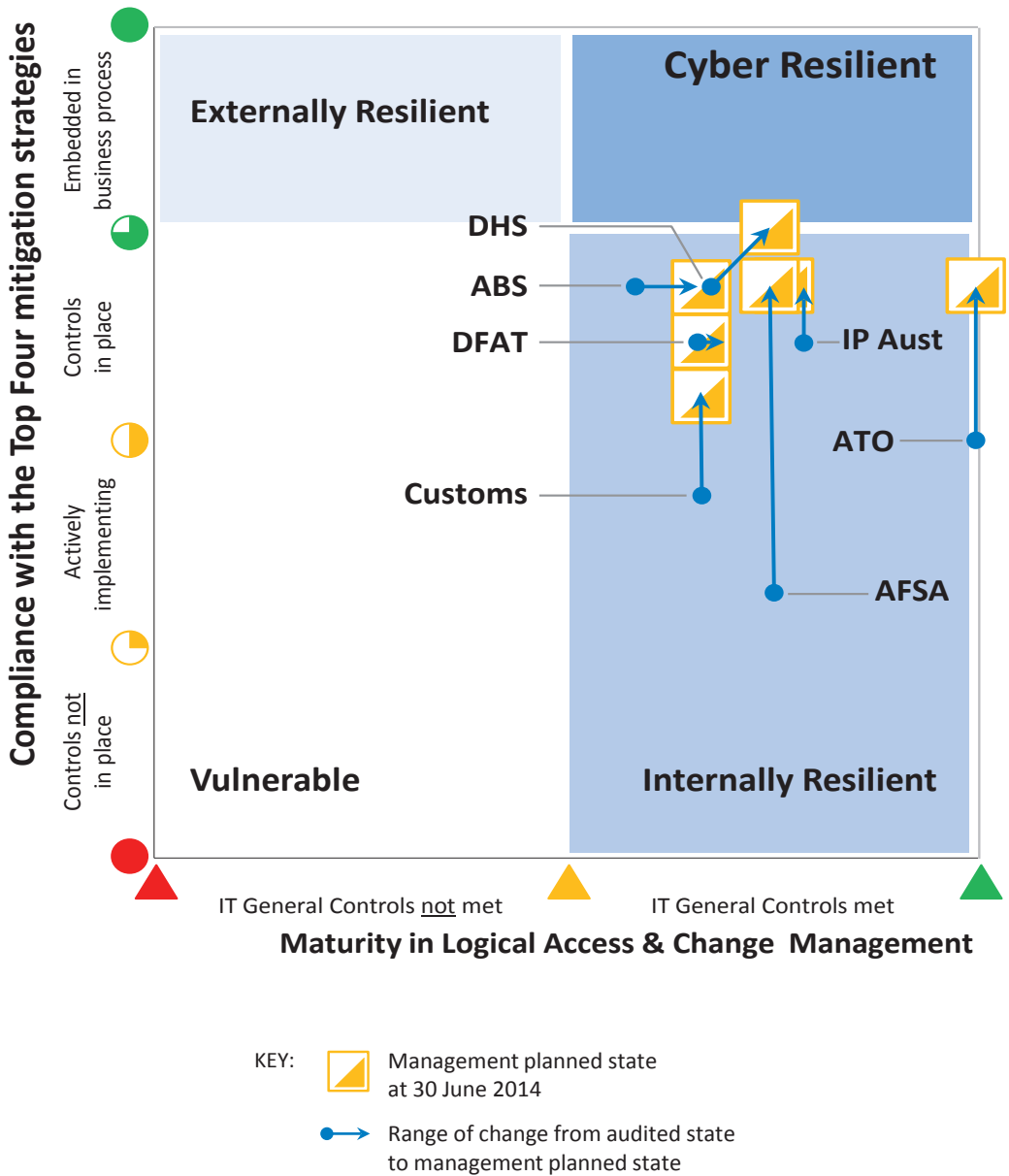
- underway by November 2013;
- had demonstrable design deliverables; and
- were assessed as having a low level of risk regarding deployment by 30 June 2014.

3.7 If effectively implemented, the activities underway would enhance the level of protection across the enterprise ICT systems, and are likely to achieve compliance with the ISM.

3.8 Figure 3.2 illustrates the entities' audited state as at 30 November 2013, and the management planned state by 30 June 2014.²⁸ The seven entities remained in the *Internally Secure* zone and did not achieve compliance by the government target date of mid-2014.

28 Reported in ANAO Audit Report No.50 2013–14 *Cyber Attacks: Securing Agencies' ICT Systems*, p. 56.

Figure 3.2: Entities range of change from audited state to management planned state



Source: ANAO analysis.

Drawing on comparisons

3.9 The entities subject to audit in 2013 and 2015 understood their obligation to achieve compliance with the PSPF and ISM but the effectiveness to implement the mandated strategies varied considerably.

- In 2013, the seven entities were aware of their shortfalls to deploy the mandated strategies, and worked towards achieving compliance by 30 June 2014. These entities accepted the audit findings and endorsed the three recommendations proposed by the ANAO.
- In 2015, the four entities were audited twelve months after the government target date to achieve compliance. These entities had self-reported their compliance with the ISM to the ANAO at the start of audit fieldwork. Only two entities achieved compliance. The non-compliant entities had initiatives underway but they did not provide a timeframe when compliance would be achieved across their enterprise ICT systems.

What are the characteristics of an entity in the Cyber Resilient zone?

Entities assessed as being in the Cyber Resilient zone had revised their business model and ICT governance, and embedded security awareness as part of their enterprise culture.

3.10 Cyber resilience is the ability to continue to provide services while deterring or responding to cyber attacks. To build cyber resilience, entities should first understand their ICT security posture. While there are significant differences between entities—in the services delivered, business needs, staff numbers, breadth of client base and the information managed—a one-size-fits-all approach to combat against cyber attacks is unlikely to be fully effective.

3.11 Entities should understand their specific ICT environment so as to adopt an informed ICT security posture appropriate for their circumstances. In the context of strengthening ICT security posture, there are behaviours and practices that improve an entity's level of cyber resilience. Similarly there are behaviours and practices that could be an impediment to realising the full benefits of further security initiatives. Entities which look beyond the Top Four strategies are better placed to manage threats and intrusions.

3.12 Entities assessed as being in the Cyber Resilient zone were aware of the factors affecting their current security posture. They knew their level of compliance with the PSPF and ISM. These entities had revised their business and management practices, and made a decision to invest in ICT security.

Characteristics of an entity in the Cyber Resilient zone

3.13 Effective entities had a business model and ICT governance that incorporated ICT security into their strategy, planning and delivery of government services. For these entities, ICT systems were no longer considered an enabler to business—it was core to business. These entities understood the risk profile across their enterprise ICT systems. They had taken steps to improve business processes to accommodate the security strengths and weaknesses for each ICT system. For these effective entities, ICT security was a priority.

3.14 The deployment of ICT security measures does not ensure, by default, a strengthened ICT security posture across the enterprise environment. Effective entities adopted a risk-based approach to prioritise security enhancements and to ensure the highest vulnerabilities are addressed first. They designed and deployed security measures at a system-level rather than at a control-level. They were aware of the importance to look beyond the Top Four strategies. They had taken varying steps to implement the remaining 31 controls from ASD's *Top 35 mitigation strategies against cyber intrusions*.

3.15 Leading by example, executives and senior managers in these entities responded to cyber security incidents in a timely manner. They were informed of the cyber trends—the motives, opportunities and emerging technology—that might target and compromise their systems. These leaders and managers understood their roles and responsibilities for the business services and systems they were accountable for. They did not expect ICT technical staff to be solely responsible for resolving ICT security matters.

3.16 Effective entities had key ICT operational staff with a sound understanding of the threats that may affect the enterprise ICT network, applications, databases and operating systems. They were aware of known security flaws affecting their assigned systems. And they deployed mitigating controls in the absence of enterprise-wide security measures.

3.17 Security awareness and initiatives are a shared responsibility within an organisation. Entities that embedded security awareness as part of their culture adopted a mutual obligation approach towards security responsibility and accountability. All staff had a duty to monitor and report on observed cyber attacks. These entities have established ICT security officers²⁹, and provided information security awareness and training to all staff and contractors.

3.18 Table 3.1 provides a checklist of the behaviours and practices that may improve an entity's level of cyber resilience. All entities are encouraged to assess the benefits of implementing these behaviours and practices in light of their own circumstances.

29 Key personnel are the Chief Information Security Officer (CISO), the Information Technology Security Advisor (ITSA), and the Information Technology Security Officers (ITSO).

Table 3.1: Behaviours and practices that may improve the level of cyber resilience

Checklist: Behaviours and practices that may improve the level of cyber resilience	
<input type="checkbox"/>	Establish a business model and ICT governance that incorporates ICT security into the strategy, planning and delivery of services.
<input type="checkbox"/>	Adopt a risk-based approach to prioritise improvements to security and to ensure the highest vulnerabilities are addressed first.
<input type="checkbox"/>	Ensure management understand their roles and responsibilities to enhance security initiatives for the services they are accountable for.
<input type="checkbox"/>	Appoint key ICT operational staff with a sound understanding of the threats and vulnerabilities relating to their specific applications and/or security layers.
<input type="checkbox"/>	Embed security awareness as part of the enterprise culture.

Source: ANAO.



Grant Hehir
Auditor-General

Canberra ACT
5 May 2016

Appendices

Appendix 1 Responses from the selected entities



AFP
AUSTRALIAN FEDERAL POLICE

COMMISSIONER

GPO Box 401, Canberra ACT 2601 Australia
Telephone +61 2 6131 5600 Facsimile +61 2 6132 6600
www.afp.gov.au
ABN 17 864 931 143

CMS 2016/4770

29 April 2016

Mr Grant Hehir
Auditor-General
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601



Dear *Grant*

Thank you for your letter dated 4 April 2016 relating to the proposed Audit Report on Cyber Resilience and for the opportunity to provide comment.

The AFP agrees with the three recommendations contained in the report. Our responses to each of the recommendations are as follows:

Recommendation 1

Agreed. The AFP has implemented a number of programs of work to address this recommendation with a planned implementation date of 1 July 2016.

Recommendation 2

Agreed. The AFP, via its Security Committee, regularly reviews its ICT security posture. The desired posture is reflected in the setting of the AFP's Cyber Security Alert Level.

Recommendation 3

Agreed. The AFP has a program of work currently underway to replace its existing SIEM. Monitoring rules specifically relating to this recommendation have been developed and are currently being tested. The replacement capability is to be implemented in July 2016.

Our summary comments for inclusion in the report are attached.

I would be grateful if you could pass on my thanks to the Australian National Audit Office audit team responsible for undertaking the audit for their professionalism and cooperation during the progress of the audit. The AFP looks forward to continuing the relationship in future audits.

Please contact Mr Robert Jackson, Manager Security, on (02) 6131 5728 or Mr Craig Petrie, Manager ICT Infrastructure, on (02) 6131 5743 if you require further information on the AFP's response.

Yours sincerely

A handwritten signature in black ink, appearing to read 'M. Phelan', with a long horizontal flourish extending to the right.

Michael Phelan APM
Performing the duties of Commissioner

**Australian Transaction Reports
and Analysis Centre**

Zenith Centre, 821 Pacific Highway
Chatswood, Sydney, NSW

Telephone +612 9950 0055



Australian Government

**Australian Transaction Reports
and Analysis Centre**

Correspondence

PO Box 5516
West Chatswood, NSW 1515,
Australia

Facsimile +612 9950 0054

www.austrac.gov.au

29 April 2016

Ms Michelle Kelly
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Ms Kelly

Re: Proposed Audit Report on Cyber Resilience

Thank you for the opportunity to review and provide comment for the draft report on the Australian National Audit Office's (ANAO) performance audit of Cyber Resilience across the sampled agencies.

The Australian Transaction Reports and Analysis Centre (AUSTRAC) supports the findings and agrees with all recommendations. I would like to express my thanks for the thorough and collaborative approach taken by the audit team.

AUSTRAC's responses are attached; our formal summary response to the proposed report (p. 8) is:

Australian Transaction Reports and Analysis Centre (AUSTRAC)

AUSTRAC has reviewed this report and supports all findings. We will continue to optimise cyber security capability, processes, and systems in line with ANAO recommendations, ASD advice, and the agency's approach to risk. The audit identified some areas for improvement and work is underway to address those.

AUSTRAC acknowledges the ongoing effort by all staff in contributing to an organisational culture of resilience and high performance that is fundamental in delivering our outcomes. The audit findings also reflect the long term commitment of our ICT teams to securing our systems.

If you would like to discuss the agency's response, please contact Dr Maria Milosavljevic, National Manager Innovation and Technology, on (02) 6120 2606 or maria.milosavljevic@austrac.gov.au.

Yours sincerely

Paul Jevtovic APM
CHIEF EXECUTIVE OFFICER



Australian Government
Department of Agriculture
and Water Resources

SECRETARY

Ref: EC16-000251

Mr Grant Hehir
Auditor General
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir,

Thank you for your letter of 4 April, 2016 and for the opportunity to respond to the ANAO's Cyber Resilience Report, the department is pleased with the results of the report and welcomes the recommendations to improve its security posture.

As you are aware the department has had a programme of investment over the past four years to improve its security posture. Our most recent investment is an implementation of the Security Information and Event Management System (SIEM) that will support detection of possible "trusted insider" threats particularly through monitoring privileged user accesses. The department will continue to focus on our ability to identify ICT risk in the area of privileged user access.

The department takes great pride in being compliant with the top 4 mitigation strategies and continues to review and improve in all 35 mitigation strategies and each of the underlying controls.

The department's responses to the relevant recommendations are as follows:

Recommendation 1 - "Entities establish processes to monitor patch levels across their enterprise ICT systems."

- All patches applied to the department's ICT environments are implemented through appropriate, formal and internally managed and controlled Change Management processes to ensure an auditable level of accountability and approval.
- The majority of the department's patches are handled by the department's primary outsourced ICT Services Provider, Hewlett Packard Enterprises (HPE). The department has processes and tools in place to ensure the HPE applied patches are consistent with our change management processes.

T +61 2 6272 3933
F +61 2 6272 5161

18 Marcus Clarke Street
Canberra City ACT 2601

GPO Box 858
Canberra ACT 2601

agriculture.gov.au
ABN 24 113 085 695

Recommendation 2 - "That entities:

- a) Conduct periodic assessments on the effectiveness of IT Security controls across their enterprise ICT systems**
- b) Decide on the optimal and/or desired ICT security posture; and**
- c) Define strategies to achieve and maintain the desired ICT security posture"**

- The department undertook a gap analysis covering the 35 strategies to mitigate targeted cyber intrusions identified by the Australian Security Directorate in May 2015 and is currently implementing the remainder of those recommendations from that analysis as well as commencing its biennial review of the 35 strategies for this calendar year;
- The department will continue to invest in Cyber Security and believes that the plans, outlined below, will position the department firmly in the ANAO's "cyber-secure" quadrant.
- Since the audit into Cyber Resilience took place, the department has introduced a number of initiatives including "Server Whitelisting" and a Security Information and Event Management (SIEM) capability. We believe these capabilities would have moved us towards being 'safely' in the cyber secure quadrant.
- The department's plan is to continue to:
 - a) refine its ICT governance and change management procedures and processes;
 - b) maintain the ICT security capabilities it already has in place from the investment of the last four years;
 - c) expand the use of its "Security Information and Event Management (SIEM)" capability that became operational in late 2015 to accommodate all critical infrastructure and applications;
 - d) progress with its current programme of work that includes introducing an updated Information Security Management Framework, Security Architecture, an Identity and Access Management system and an assessment of our key process capability based on the required standard, ISO/IEC 33020:2015; and
 - e) Upon completion of this programme the department will then engage an Independent Risk Assessment Process (IRAP) assessor to determine the effectiveness of the department's critical infrastructure and systems.
- To maintain and enhance its position as "cyber secure" the department will review its position against ASD cyber-security strategies biennially and then continually cycle through the five steps identified in its plans above.

Recommendation 3 - "That entities:

- a) Capture and store audit logs for privileged user accounts; and**
- b) Actively monitor privileged user accounts for unauthorised access and inappropriate behaviour, preferably with the support of a Security Information and Event Management (SIEM) tool";**

- The department commenced a project to implement a "Security Information and Event Management (SIEM)" capability in 2015. The SIEM is now operational and is actively capturing and storing activity logs, including privileged user accounts, across our ICT environment. This activity includes actions such as logons/logoffs, modification of other user accounts and account lockouts.

- The SIEM alerts security staff in real-time for such activities where detection is critical, such as a privileged access being granted after normal business hours. In addition, the associated logs can be reviewed and analysed by security staff at any time after an alert is raised, for the purposes of investigation.
- The department has a program of work in train to progressively ensure each of our critical and bespoke systems provide security related logging data into SIEM for appropriate analysis.



Yours sincerely

Daryl Quinlivan

29 April 2016



Australian Government
**Department of Industry,
Innovation and Science**

Secretary

Ms Michelle Kelly
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Ms Kelly

Proposed Audit report on *Cyber Resilience*

Thank you for your letter dated 4 April 2016 seeking comment from the department on the proposed audit report on *Cyber Resilience*. In accordance with section 19 of the *Auditor-General Act 1997*, please find enclosed the department's response to the report.

I acknowledge the findings in the report noting that the department has made efforts to achieve compliance with the mandated strategies in the ISM.

I agree with the three recommendations noted in the audit report for achieving compliance. Each recommendation has been addressed at [Attachment A](#).

A summary response for inclusion on the body of the report is at [Attachment B](#)

Thank you for the opportunity to comment on the proposed report.

Yours sincerely

A handwritten signature in black ink, appearing to read 'G. A. Beauchamp', written in a cursive style.

Glenys Beauchamp

26 April 2016

Appendix 2 Glossary

Change management	A process undertaken to minimise the likelihood of disruption and unapproved changes and data errors.
ICT system (or IT system)	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
IT general controls	Policies and procedures developed to deal with identified ICT system risks, including controls over ICT governance, ICT infrastructure, security and access to operating systems and databases, and program change procedures.
Logical access controls	ICT measures used to control access to ICT systems and their information—including user identifications and authenticators such as passwords.
Threat	A source of harm that is deliberate or has intent to do harm.
Vulnerability (in ICT systems)	A flaw, bug or misconfiguration that can be exploited to gain unauthorised access to a network or information.

Appendix 3 Audit criteria and compliance statement

Table A.1: Audit criterion one, and compliance statements

Criterion One: The mandatory ISM controls that support the top four mitigation strategies have been implemented
<p>Application whitelisting</p> <ul style="list-style-type: none">• implement application whitelisting as part of the standard operating system at both the desktop and for servers;• prevent the running of an arbitrary executables not listed in the application whitelisting policy;• permit the running of only predefined sets of executables in accordance to the application whitelisting policy;• prevent users from disabling application whitelisting capability;• complement, and not supplement, antivirus and other Internet security software with application whitelisting;• ensure system administrators are not exempt from application whitelisting policy; and• ensure that the default policy is to deny the running of software. <p>Patching applications and operating systems</p> <ul style="list-style-type: none">• deploy security patches as soon as possible;• have in place a patch management strategy to address security vulnerabilities;• apply critical security patches within two days;• install the latest version of applications and operating systems as soon as possible;• install the latest version of applications within two days if the upgrade addresses a known critical security vulnerability; and• implement 'alternate' controls where known vulnerabilities cannot be patched, or security patches are not available. <p>Minimising domain and local administrative privileges</p> <ul style="list-style-type: none">• ensure that the default policy is to deny the running of software.• ensure privileged accounts are controlled and auditable;• ensure system administrators are assigned separate accounts— segregated from their (general) user accounts—and for administrative duties only;• keep the number of privileged accounts to a minimum;• regularly audit the passphrases of privileged accounts for: length or complexity; and not being reused over time or for multiple accounts; and• regularly review the privileges allocated to privileged user accounts.

Source: Australian Signals Directorate, *Australian Government Information Security Manual*, April 2013, p. 116.

Table A.2: Audit criterion two, and compliance statements

Criterion Two: Effective logical access and change management process to authorise the implementation of critical security patching for application and operating systems are being used
<ul style="list-style-type: none">• only authorised changes are made to systems, programs and data;• authorised changes are correctly reflected in the system and do not adversely impact on other systems and processes;• changes necessary to the proper operation of the systems or programs are made in a timely manner;• emergency changes are controlled; and• changes are successfully implemented or rolled back.

Source: ANAO.

