

Cybersecurity Follow-up Audit

Across Entities

© Commonwealth of Australia 2017

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-231-0 (Print)

ISBN 978-1-76033-232-7 (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:

Senior Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:

communication@anao.gov.au.



Canberra ACT
15 March 2017

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit across entities, titled *Cybersecurity Follow-up Audit*. The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, 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>

Audit Team

William Na
Lisa Elkner
Gayantha Mendis
Elenore Karpfen
David Gray

Contents

Summary and recommendations.....	7
Background	7
Supporting findings.....	10
Recommendations.....	11
Summary of entities' responses	11
Audit Findings.....	15
1. Background	17
Introduction	17
Previous audits and JCPAA review.....	18
Audit approach	18
2. Entities' compliance with the government mandatory requirements.....	20
Are entities compliant with the Top Four mitigation strategies?.....	20
Did the entities appropriately assess and report against compliance with the Top Four mitigation strategies?.....	25
3. Entities' cyber resilience	27
Are entities cyber resilient?	28
Are entities' effectively prioritising cyber resilience?	34
Appendices	37
Appendix 1 Entity response	39
Appendix 2 Recommendations from previous audits	50
Appendix 3 Compliance grading scheme	52

Summary and recommendations

Background

1. In June 2014, ANAO Audit Report No. 50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems* was tabled in Parliament. The report examined seven Australian Government entities¹ implementation of the mandatory strategies in the *Australian Government Information Security Manual* (Top Four mitigation strategies). The Top Four mitigation strategies are: application whitelisting, patching applications, patching operating systems and minimising administrative privileges.² The audit found that none of the seven entities were compliant with the Top Four mitigation strategies and none were expected to achieve compliance by the Australian Government's target date of 30 June 2014.

2. The Joint Committee of Public Accounts and Audit held a public hearing to examine Report No. 50 on 24 October 2014. Three of the seven audited entities—the Australian Taxation Office, the Department of Human Services, and the then Australian Customs and Border Protection Service³—appeared before the hearing to explain their plans and timetables to achieve compliance with the Top Four mitigation strategies. Each of the three entities gave assurance to the Joint Committee of Public Accounts and Audit that compliance with the Top Four mitigation strategies would be achieved during 2016.

3. These three major Australian Government entities are significant users of technology:

- the Department of Human Services relies on its information and communications technology (ICT) systems to process \$172 billion in payments annually;
- through its electronic lodgement systems Australian Taxation Office collects over \$440 billion in gross tax revenue annually; and
- the Department of Immigration and Border Protection electronically processes around seven million visas annually and inspects and examines around two million air and sea cargo imports and exports.

4. All three entities collect, store and use data, including national security data and personally identifiable information that can be used to identify, contact, or locate an individual such as date of birth, bank account details, driver's licence number, tax file number and biometric data.⁴

5. Not operating in a cyber resilient environment puts entities' data and business processes at risk, with potentially significant consequences for Australian citizens and other clients and stakeholders.

1 The seven entities were: Australian Bureau of Statistics, Australian Customs and Border Protection Service, Australian Financial Security Authority, Australian Taxation Office, Department of Foreign Affairs and Trade, Department of Human Services and IP Australia.

2 The Australian Signals Directorate advises that if government entities implemented these top four of 35 strategies, it would prevent 85 percent of targeted cyber intrusions.

3 From 1 July 2015, the Australian Customs and Border Protection Service and the Department of Immigration and Border Protection were merged into a single entity.

4 Biometric data includes for example facial and voice recognition and fingerprint scans.

Audit objective and criteria

6. The objective for this audit was to assess whether the Australian Taxation Office, the Department of Human Services, and the Department of Immigration and Border Protection are compliant with the Top Four mitigation strategies in the *Australian Government Information Security Manual*. The audit also examined entities' cyber resilience, which includes establishing a sound ICT general controls framework⁵ and effectively implementing the Top Four mitigation strategies.

7. To form a conclusion against the audit objective, the ANAO adopted the following high level assessment criteria:

- do the entities comply with the Top Four mitigation strategies; and
- are entities cyber resilient?

Conclusion

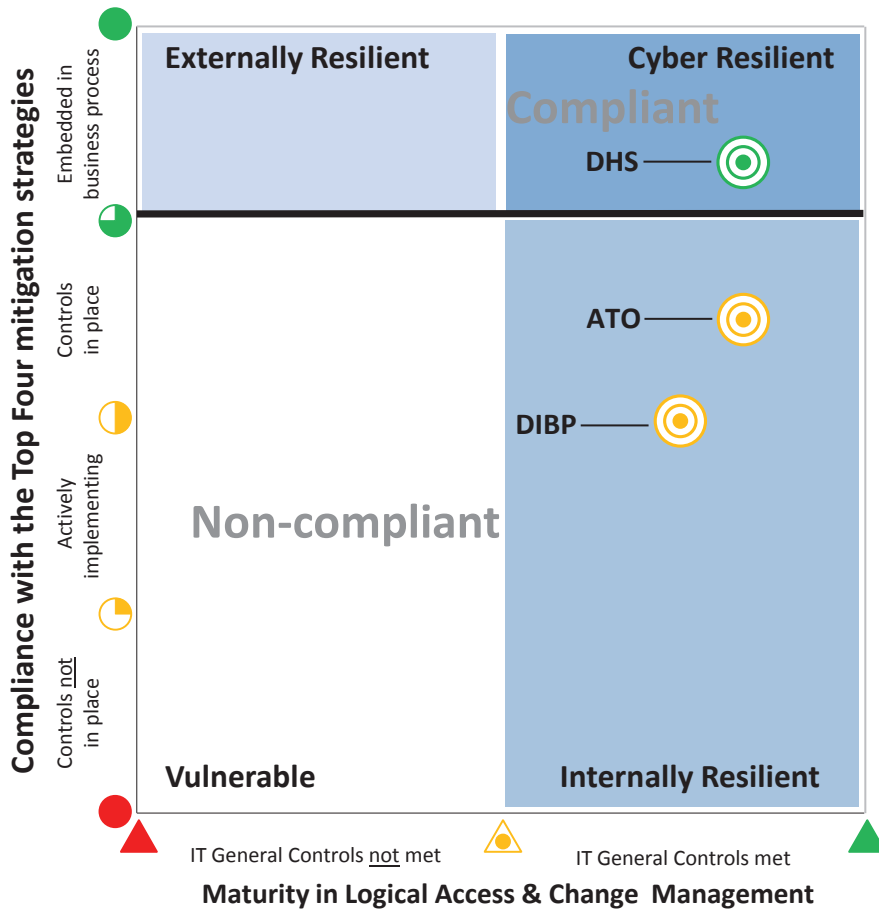
8. The ANAO assessed that of the three entities only the Department of Human Services was compliant with the Top Four mitigation strategies. The Department of Human Services also accurately self-assessed compliance against the Top Four mitigation strategies and met its commitment to the Joint Committee of Public Accounts and Audit of achieving compliance during 2016.

9. Of the three entities, only the Department of Human Services was cyber resilient. 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. To progress to being cyber resilient, the Australian Taxation Office and the Department of Immigration and Border Protection need to improve their governance arrangements and prioritise cybersecurity.

10. Figure S.1 shows each entity's cyber resilience.

5 ICT General Controls are policies and procedures developed to deal with ICT system risks, including controls in relation to ICT governance, ICT infrastructure, security and access to operating systems and databases, user access provisioning, and program change procedures that include test and release to production.

Figure S.1: Entities' cyber resilience^a



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.

Note a: An entity's position on the matrix indicates its overall cyber resilience—in essence how well the entity is protected from external intrusions, internal breaches and unauthorised disclosures of information, and how well it is positioned to address threats.

Source: ANAO.

Supporting findings

Entities' compliance with the mandatory strategies

11. The Top Four mitigation strategies are: application whitelisting; application patching; operating system patching; and minimising privileged user access.

12. Overall, only the Department of Human Services was assessed as having effectively implemented application whitelisting. The Department of Immigration and Border Protection had an application whitelisting strategy but deviated from it. The Australian Taxation Office only developed an application whitelisting strategy during the course of this audit.

13. The Department of Human Services is the only entity that effectively implemented applications and operating systems patching. The Department of Immigration and Border Protection's service provider contract arrangements did not align with the Top Four mitigation strategies. Both the Australian Taxation Office and the Department of Immigration and Border Protection did not effectively use their internal assurance processes to validate service provider's performance self-assessments.

14. All three entities managed privileged user access effectively. However, there was room for improvement in the monitoring of privileged account usage. All three entities were aware of this shortcoming and were working to address it during the course of the audit.

15. All three entities conducted compliance self-assessments against the Top Four mitigation strategies and reported the results in accordance with government requirements. The Australian Taxation Office's and the Department of Immigration and Border Protection's self-assessments both reported compliance against three of the Top Four mitigation strategies. The ANAO assessed that the Australian Taxation Office and the Department of Immigration and Border Protection complied with only two and one of the Top Four mandatory strategies respectively.

Entities' cyber resilience

16. All three entities had improved their cyber resilience—to various degrees—since the 2014 audit.

17. The Department of Human Services had security controls in place to provide protection from external attacks, internal breaches and unauthorised information disclosures. This was achieved by prioritising activities that were required to implement the Top Four mitigation strategies and by strengthening supporting governance arrangements. It is now positioned in the '*cyber resilient*' zone.

18. The Australian Taxation Office and the Department of Immigration and Border Protection had security controls that provided a reasonable level of protection from breaches and unauthorised disclosures of information from internal sources. However, there was insufficient protection against cyber attacks from external sources. As a result, they remain in the '*internally resilient*' zone.

19. Cybersecurity is a strategic priority for the Australian Government. 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.

20. 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.

Recommendations

Recommendation No. 1
Paragraph 2.25 The ANAO recommends that entities periodically assess their cybersecurity activities to provide assurance that: they are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives; and that they can report on them accurately. This applies regardless of whether cybersecurity activities are insourced or outsourced.

Department of Human Services' response: Agreed.

Australian Taxation Office's response: Agreed.

Department of Immigration and Border Protection's response: Agreed.

Recommendation No. 2
Paragraph 3.24 The ANAO recommends that entities improve their governance arrangements, by:

- (a) asserting cybersecurity as a priority within the context of their entity-wide strategic objective;
- (b) ensuring appropriate executive oversight of cybersecurity;
- (c) implementing a collective approach to cybersecurity risk management; and
- (d) conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

Department of Human Services' response: Agreed.

Australian Taxation Office's response: Agreed.

Department of Immigration and Border Protection's response: Agreed.

Summary of entities' responses

21. A summary of entities' responses are below, with the full responses provided at Appendix 1.

Department of Human Services

The Department of Human Services (the department) welcomes this report and considers that the Australian National Audit Office (ANAO) recommendations support effective cybersecurity governance arrangements.

The department is committed to protecting the confidentiality, integrity and availability of its information and assets. We are pleased to note the ANAO found that the department was compliant with the Top Four mandatory cyber strategies and was cyber resilient. Achieving this

compliance and strengthening cybersecurity governance arrangements has been a priority for the department over recent years. As a result, the department can continue to deliver government outcomes while also effectively managing a rapidly escalating and changing cyber threat environment.

Australian Taxation Office

The ATO welcomes this review and agrees with the two recommendations in the report.

The ATO is increasingly taking advantage of new technologies which provide convenient and accessible services for the community. These new and emerging technologies are often accompanied with new and emerging risks.

We consider and manage risks associated with new technology to protect the integrity of the tax and superannuation systems and works across government to strengthen the security of digital services.

The ATO is committed to meeting community expectations for data security and privacy protection and to providing improved services.

The review recognised the ATO's strong general information communications technology controls and we will continue to build upon these and continuously improve our overall cybersecurity governance arrangements.

While there has been improvement in the overall maturity of the security posture of the ATO, the review clearly highlighted further improvements that are required. The ATO has committed additional resource and focus to address deficiencies and reach a greater level of cyber resilience. Immediate improvements have already been put in place with a commitment to reach cyber resilience status in 2017.

Department of Immigration and Border Protection

The Department of Immigration and Border Protection (DIBP) recognises and accepts the risks posed in the cyber domain and acknowledges the importance of compliance with the ISM Top Four mitigation strategies.

The Department has taken a risk based approach to cybersecurity, taking into account our position in the ICT investment cycle. The Department manages this risk through a number of controls.

The Department's Executive Committee is committed to maintain the Department's cybersecurity posture. In responding to this ever present threat, the Department has invested in a number of major programmes. These include: Security; Identity and Access Management; End User Computing Capability and ICT Consolidation these programmes will significantly enhance the Department's current cybersecurity capability and improve the Department's compliance with the Top Four mitigation strategies.

In considering the findings raised in the report, it is important to recognise the previous audit tabled in June 2014, ANAO Audit Report No. 50 2013–14, assessed the former Australian Customs and Border Protection Service (ACBPS). The current audit assessed the Department of Immigration and Border Protection, which operates in a significantly more complex environment, from migration policy, visa and cargo processing to frontline border operations involving the timely movement of people and goods across the border that include civil maritime security operations and border law enforcement activities.

July 2015 saw the dis-establishment of the ACBPS and the creation of the Australian Border Force as part of an integrated immigration and border protection portfolio. From an ICT

perspective this represented an enormous challenge of integrating two very different ICT architectures, ICT operational management processes and cybersecurity maturity.

In comparing DIBP with the agencies, subjected to this audit is important to recognise the relevant position of each agency on the ICT investment curve. This in turn has a direct implication and relationship to the maturity of their respective cybersecurity initiatives. DHS and ATO have invested heavily over the last three to five years in large cybersecurity and ICT investment programmes. DIBP, however, is only in its second year of a number of multi-year programmes.

Audit Findings

1. Background

Introduction

1.1 The Australian Government Information Security Manual outlines 35 strategies to assist government entities mitigate the risk of cyber intrusions to their information and communications technology (ICT) systems.⁶ The Australian Signals Directorate⁷ advised that if government entities implemented the top four of these 35 strategies (Top Four mitigation strategies), it would prevent 85 percent of targeted cyber intrusions.

1.2 The Top Four mitigation strategies are:

- using **application whitelisting**⁸ on desktops and servers to prevent malicious software and unapproved programs from running on a computer;
- applying **application patches**⁹ through sound policies, procedures and practices to help ensure the applications' security;
- applying **security patches** through sound policies, procedures and practices to **operating systems** to mitigate security risks and reduce system vulnerabilities; and
- effectively managing access provisions for **privileged user accounts** across an entity's ICT environment, including the entity's network, applications, databases and operating systems.¹⁰

1.3 In April 2013, the Australian Government Protective Security Policy Framework¹¹ mandated that government entities implement the Top Four mitigation strategies by July 2014.

1.4 In order to effectively implement the Top Four mitigation strategies, an entity must have a sound entity-wide ICT general controls framework. This framework provides an entity with a stable and reliable ICT environment and forms the foundation upon which other processes and controls can be built. ICT general controls include controls over: ICT governance; ICT infrastructure; acquiring and developing applications; logical user access¹² to ICT infrastructure, applications and data; and making changes to ICT systems and applications.

1.5 Together, the effectiveness of the implementation of the Top Four mitigation strategies and the soundness of an entity's ICT general controls framework forms the basis of its cyber resilience.

6 Australian Signals Directorate, *Australian Government Information Security Manual*, <http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf>, [accessed October 2016].

7 The Australian Signals Directorate is an intelligence agency in the Department of Defence.

8 A whitelist is a list of trusted executables. It is a more practical and secure method of securing a system than prescribing a list of bad executables that are to be prevented from running (a blacklist).

9 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.

10 System administrators typically have greater access rights to systems and information than normal users.

11 The Australian Government Protective Security Policy Framework is administered by the Attorney-General's Department. It is available from <<https://www.protectivesecurity.gov.au/Pages/default.aspx>>.

12 Logical access controls are tools and protocols used for identification, authentication, authorisation, and accountability in computer information systems.

Previous audits and JCPAA review

1.6 ANAO Performance Audit Report No. 50 2013–14 *Cyber Attacks: Securing Agencies' ICT Systems* (the first audit), was tabled in June 2014. In this audit, the ANAO examined seven entities'¹³ compliance with the Top Four mitigation strategies and found that none of the seven entities were compliant with these strategies. The ANAO made three recommendations, which were agreed by all agencies (see Appendix 2).

1.7 The Joint Committee of Public Accounts and Audit (JCPAA) reviewed the first audit in October 2014.¹⁴ Three of the seven audited entities—Australian Taxation Office, Department of Human Services and the then Australian Customs and Border Protection Service—appeared before the hearing to explain their plans and timeframes to achieve compliance. Each of the three entities gave assurance to the JCPAA that they would achieve compliance during 2016.

1.8 The JCPAA published its report in March 2015 and recommended that the seven entities achieve full compliance with the Top Four mitigation strategies as soon as possible. The JCPAA also recommended the Auditor-General consider a follow-up audit, as well as undertaking regular audits of Commonwealth entities' compliance with the Top Four mitigation strategies.

1.9 In 2015, the ANAO conducted a second performance audit to examine a further four government entities' compliance with the Top Four mitigation strategies. The four entities were: Australian Federal Police, Australian Transaction Reports and Analysis Centre, Department of Agriculture and Water Resources and the Department of Industry, Innovation and Science. The ANAO Performance Audit Report No. 37 2015–16 *Cyber Resilience* was tabled in May 2016. In this audit the ANAO found that two entities—Australian Transaction Reports and Analysis Centre, Department of Agriculture and Water Resources—were compliant with the Top Four mitigation strategies. The other two agencies were not compliant with these strategies. The ANAO made three recommendations and all entities agreed with all recommendations (see Appendix 2).

Audit approach

1.10 This audit is a follow-up audit of the ANAO Performance Audit Report No. 50 2013–14 that was tabled in June 2014.

1.11 The audit objective was to assess whether three of the seven entities assessed in the first audit had achieved compliance with the Top Four mitigation strategies. The three entities were:

- Australian Taxation Office,
- Department of Human Services; and
- Department of Immigration and Border Protection.¹⁵

13 ANAO Audit Report No.50 2013–14, op. cit., p. 15.

14 Joint Committee of Public Accounts and Audit, The Parliament of the Commonwealth of Australia, *Report 447 EPBC Act, Cyber Security, Mail Screening, ABR and Helicopter Program: Review of Auditor-General Reports Nos 32-54 (2013-14)* (2016).

15 ANAO Audit Report No.50 2013–14, op. cit., p. 15.

1.12 These three major Australian Government entities are significant users of technology:

- the Department of Human Services relies on its ICT systems to process \$172 billion in payments annually;
- through its electronic lodgement systems the Australian Taxation Office collects over \$440 billion tax revenue per year; and
- the Department of Immigration and Border Protection electronically processes around seven million visas annually and inspects and examines over two million air and sea cargo imports and exports.

1.13 All three entities collect, store and use data, including national security data and personally identifiable information that can be used to identify, contact, or locate an individual such as date of birth, bank account details, driver's licence number, tax file number and biometric data.

1.14 To form a conclusion against the audit objective, the ANAO adopted the following high-level criteria:

- do the examined entities comply with the Top Four mitigation strategies? and
- are the examined entities cyber resilient?

1.15 The ANAO reviewed records and interviewed relevant personnel from each entity and conducted assessment and tests of controls that underpin the compliance of the Top Four mitigation strategies for each entity.

1.16 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of approximately \$419 396.

Reporting on audit findings

1.17 The ANAO provided detailed briefings regarding the specific findings of the audit to senior executives, IT Security Advisors, senior managers and officers of ICT operations within each entity. A detailed technical paper outlining specific findings was also provided to each entity.

1.18 The audit team was William Na, Lisa Elkner, Gayantha Mendis, Elenore Karpfen and David Gray.

2. Entities' compliance with the government mandatory requirements

Areas examined

This chapter examines whether the Australian Taxation Office, Department of Human Services, and Department of Immigration and Border Protection are compliant with the Top Four mitigation strategies and met their commitment to the Joint Committee of Public Accounts and Audit of achieving compliance during 2016. It also examines whether the entities appropriately self-assessed and reported the extent of this compliance.

Conclusion

The ANAO assessed that of the three entities only the Department of Human Services was compliant with the Top Four mitigation strategies. The Department of Human Services also accurately self-assessed compliance against the Top Four mitigation strategies and met its commitment to the Joint Committee of Public Accounts and Audit of achieving compliance during 2016.

Area for improvement

The ANAO made one recommendation aimed at strengthening entities' cybersecurity by aligning cybersecurity activities with cybersecurity outcomes.

Are entities compliant with the Top Four mitigation strategies?

The Top Four mitigation strategies are: application whitelisting; application patching; operating system patching; and minimising privileged user access.

Overall, only the Department of Human Services was assessed as having effectively implemented application whitelisting. The Department of Immigration and Border Protection had an application whitelisting strategy but deviated from it. The Australian Taxation Office only developed an application whitelisting strategy during the course of this audit.

The Department of Human Services is the only entity that effectively implemented applications and operating systems patching. The Department of Immigration and Border Protection's service provider contract arrangements did not align with the Top Four mitigation strategies. Both the Australian Taxation Office and the Department of Immigration and Border Protection did not effectively use their internal assurance processes to validate service provider's performance self-assessments

All three entities managed privileged user access effectively. However, there was room for improvement in the monitoring of privileged account usage. All three entities were aware of this shortcoming and were working to address it during the course of the audit.

Entity compliance with the Top Four mitigation strategies

2.1 The Top Four mitigation strategies are:

- application whitelisting;
- application patching;

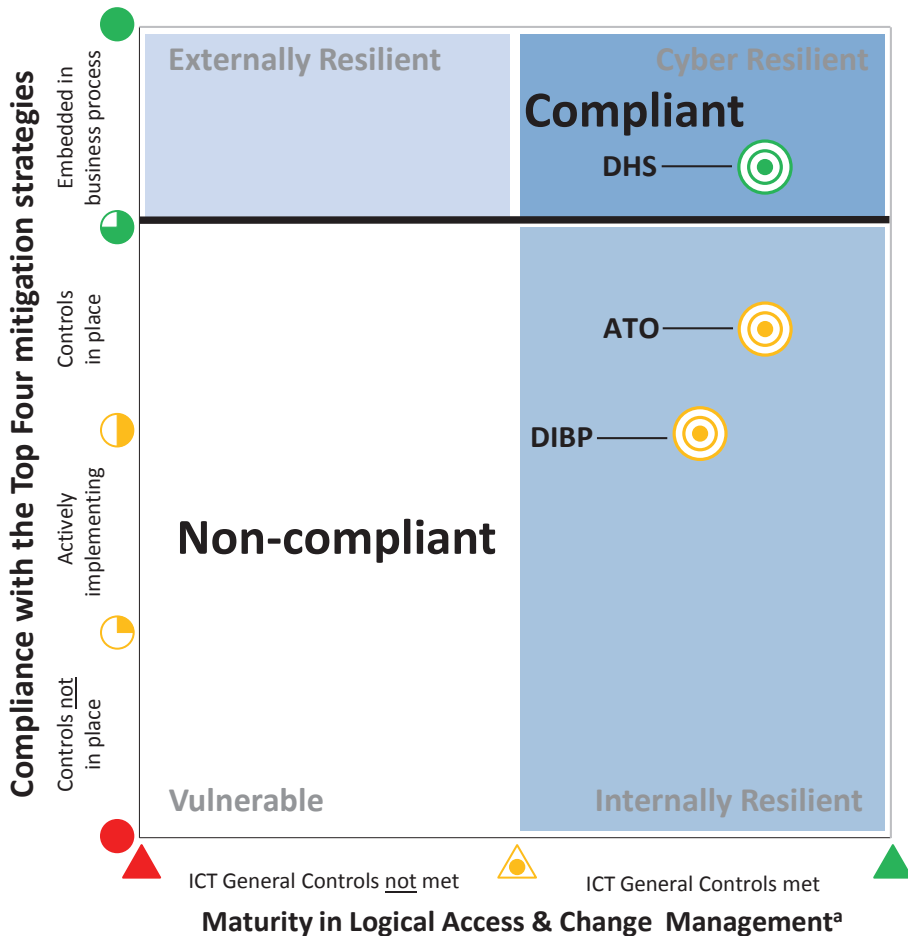
- operating system patching; and
- minimising privileged user access.

2.2 The Department of Human Services (Human Services) complied with the Top Four mitigation strategies. The Australian Taxation Office (ATO) complied with two of four the strategies and the Department of Immigration and Border Protection (Immigration) complied with one of the four strategies.









2.3 The ANAO assessed that the ATO and Immigration also did not meet their commitment to the Joint Committee of Public Accounts and Audit to achieve compliance with the Top Four mitigation strategies during 2016.

2.4 Figure 2.1 depicts the level of compliance with the Top Four mitigation strategies. Appendix 3 contains information relating to the graphical key and criteria used to assess compliance.

Figure 2.1: Entities' overall assessment against the Top Four mitigation strategies



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.

Note a: ICT general controls, as depicted on the horizontal axis, are entity-wide structures, policies, procedures, and standards applied to information systems that support business processes. These provide a stable and reliable foundation upon which other processes and controls can be built. The assessment of ICT general controls is discussed in Chapter 3.













Source: ANAO analysis.

2.5 The ANAO identified the following shortcomings in the entities' implementation of the Top Four mitigation strategies:

- application whitelisting controls did not cover all desktops and servers;
- systems were excluded from regular security patching as required by the entities' security policies;
- deployment of critical security patches were delayed and outside the timeframes recommended by either the government's Information Security Manual and/or the entities' policies; and
- many incidences of outdated software on desktops.¹⁶

2.6 These shortcomings increase the risks of system vulnerabilities being exploited, which can lead to the compromise of the integrity, confidentiality and availability of entities' systems and information holdings. The consequence of a compromised system will impact on the entities' ability to deliver government programs and services. Table 2.1 shows the aggregated assessment grading for the Top Four mitigation strategies.

Table 2.1: Aggregated entity control assessment grading

Control areas assessed	Control assessment score		
Top Four Mitigation Strategies	DHS	ATO	DIBP
Application Whitelisting			
Patching applications			
Patching operating systems			
Minimising administrative privileges			

Source: ANAO analysis.

¹⁶ Software includes, for example, Microsoft Office, Java, Adobe Reader and Flash Player.

Application whitelisting

2.7 Application whitelisting protects ICT systems against unauthorised applications running on them. Its purpose is to protect systems and networks from harmful applications. The Information Security Manual requires entities to implement application whitelisting for both desktops and servers.

2.8 Overall, only Human Services was assessed as having effectively implemented application whitelisting. Both the ATO and Immigration had not effectively implemented application whitelisting on their servers. Only Immigration had not effectively implemented application whitelisting on its desktops. This contravenes the Information Security Manual and the entities' own ICT security policies.

2.9 Immigration had configured its desktop application whitelisting policies to allow over 1400 users to by-pass the whitelisting controls. This allowed users to install and run unauthorised applications on their desktops which increased the security risks for the entity. This configuration was aimed at improving flexibility for end-users; however, it deviated from the entity's own ICT security policy requirements. This entity's cybersecurity branch was aware of these risks and did not implement compensating controls.

2.10 The ATO did not have a coordinated approach to application whitelisting. It allowed service providers to choose their own preferred technology to implement application whitelisting in their responsible areas, with no overarching strategy to guide the process. The lack of strategy resulted in some areas having no application whitelisting coverage. During the course of this audit, the ATO developed an overarching strategy to better coordinate its approach to implementing application whitelisting.

Patching applications and operating systems

2.11 The Information Security Manual requires entities to deploy security patches¹⁷ as soon as possible after being released by the vendor to protect ICT systems from known vulnerabilities. Critical security patches should be deployed within two days.¹⁸ According to the Australian Signals Directorate, applying security patches to applications, operating systems and devices is one of the most effective security practices to address known system vulnerabilities.

2.12 Entities had installed either Microsoft Windows 7 or Windows 10 operating systems on their desktops. Entities used vendor provided tools to support the automatic deployment of security patches to desktops. The automated deployment of security patches was efficient and timely.

2.13 While all entities had automatic patching processes for the Windows environment, entities with a UNIX/Linux environment were yet to automate and streamline patching processes, despite tools being available to do this. In the ATO, the number of UNIX/Linux servers tripled in a year. The ATO had not anticipated this change and had not developed a process for deploying security patches across their servers. The increased number of servers complicated the deployment of

17 Security patch is a fix to a program that eliminates a vulnerability exploited by malicious actors.

18 Australian Signals Directorate 2016, *Australian Government Information Security Manual: Controls* [Internet], Commonwealth of Australia, available from <http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf> [accessed October 2016].

security patches. Proper planning of ICT capabilities and cybersecurity measures would help entities to adapt and respond to the ever changing nature of the cybersecurity landscape and their business requirements.

2.14 The ANAO found many incidences of outdated software on desktops. In one case, Immigration had six versions of the same application installed on its desktops, and most versions were no longer supported by vendors. The Australian Signals Directorate advised that using unsupported software increased security risks and entities must update software to a vendor supported version.¹⁹

2.15 To apply security patches, servers often need to be taken offline. There were many instances where entities chose not to take servers offline in order to maintain service delivery. The ANAO assessed that maintaining high levels of system availability without compromising cybersecurity is possible. Human Services achieved this while maintaining a diverse ICT environment.

2.16 The ATO and Immigration had not deployed security patches to their servers in the timeframes specified by the Information Security Manual. The entities also had not deployed security patches to a large number of servers.

2.17 There were weaknesses in entities' management of ICT contracts. In particular, some of Immigration's ICT contract arrangements did not align with the Information Security Manual's security patching requirements. Both the ATO and Immigration did not effectively use their internal assurance processes to validate the accuracy of service provider self-assessments against contractual obligations. This led to both entities having limited visibility of the true status of security patches across their ICT environments. In one instance, the ATO did not know that a service provider took significantly longer than the contractually specified timeframe to complete patching.

Manage privileged access

2.18 Privileged access can give a user the ability to:

- change key system configurations and control parameters;
- circumvent security measures;
- access sensitive information (such as audit and security); and
- access and modify data, files and accounts used by other users.

2.19 Misuse of privileged access can lead to significant security compromises, such as unauthorised information disclosure and system/process breakdown. The Information Security Manual requires entities to implement effective controls over assigning and using privileged accounts to maintain system and information integrity.

2.20 All entities had policies and procedures in place to enforce key controls over the use of privileged accounts, and include:

- granting and restricting privileged accounts only to appropriate staff;

19 Australian Signals Directorate, op. cit., p. 160.

- minimising the number of privileged accounts;
- preventing privileged accounts from accessing emails and the internet;
- password length and complexity requirements that comply with Top Four mitigation strategies; and
- activity logging and monitoring.

2.21 The process of granting and revoking privileged user accounts is in accordance with the Information Security Manual. However, there was room to improve the monitoring of privileged account usage. The entities were aware of this shortfall and were implementing solutions to address it.

Did the entities appropriately assess and report against compliance with the Top Four mitigation strategies?

All three entities conducted compliance self-assessments against the Top Four mitigation strategies and reported the results in accordance with government requirements. The Australian Taxation Office's and the Department of Immigration and Border Protection's self-assessments both reported compliance against three of the Top Four mitigation strategies. The ANAO assessed that the Australian Taxation Office and the Department of Immigration and Border Protection complied with only two and one of the Top Four mandatory strategies respectively.

2.22 Since 2013 entities are required to undertake an annual self-assessment against the mandatory requirements detailed in the Protective Security Policy Framework. Entities are required to report their compliance to the relevant portfolio Minister, to the Secretary of the Attorney-General's Department and provide a copy to the Auditor-General. The Top Four mitigation strategies are part of the self-assessment criteria.

2.23 For the past two financial years, Human Services self-assessed as compliant with the Top Four mitigation strategies. The ATO and Immigration self-assessed as non-compliant. Through the self-assessment process, the ATO and Immigration both reported compliance against three of the Top Four mitigation strategies. The entities outlined their actions to address the self-identified area of non-compliance.

2.24 The ANAO assessed that the ATO and Immigration were compliant with two and one of the Top Four mitigation strategies respectively. Compliance reporting relies on the accuracy of self-assessed data and the supporting processes to check that data. Stronger monitoring, evaluation and review of Top Four mitigation strategies in particular will help entities to identify areas of non-compliance and better allocate resources to address them.

Recommendation No.1

2.25 The ANAO recommends that entities periodically assess their cybersecurity activities to provide assurance that: they are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives; and that they can report on them accurately. This applies regardless of whether cybersecurity activities are insourced or outsourced.

Department of Human Services' response: *Agreed.*

2.26 *The ANAO has concluded that the department was cyber resilient and accurately self-assessed its compliance against the Top Four mandatory strategies. Continuous monitoring of cyber activities in place at the time of the audit has been strengthened by the establishment of a team dedicated to compliance activities. The outcomes of these activities are routinely reported to the Executive through numerous governance boards.*

Australian Taxation Office's response: *Agreed.*

2.27 *As the ATO continues to enhance our systems to provide better services for the Australian community, we are focused on maintaining the security and integrity of our data and information. Understanding new threats and protecting our systems from any potential vulnerabilities is a priority.*

2.28 *Following advice from external scrutineers, the ATO has merged its Information Security and IT Security capabilities to form one integrated Information and IT Security functional unit. We have also appointed an SES Band 2 as the Chief Security Officer (CSO).*

2.29 *The CSO and the integrated security unit have been charged with taking a multifaceted approach to cyber security; including regular information technology risk and threat assessments, strategy and policy (including a revised whitelisting strategy), system certification reviews, monitoring and compliance regime.*

2.30 *In addition the CSO will ensure that findings and recommendations relating to cyber security from scrutineers (such as the subject audit) are followed up and implemented how and when necessary.*

2.31 *The ATO is working to reflect the newly released 'essential eight', cybersecurity controls which incorporate the 'Top 4' covered in this Audit.*

Department of Immigration and Border Protection's response: *Agreed.*

2.32 *The Department agrees with this recommendation and will assess its cybersecurity activities on an annual basis.*

3. Entities' cyber resilience

Areas examined

The ANAO examined factors affecting the entities' ability to achieve cyber resilience.

Conclusion

Of the three entities, only the Department of Human Services was cyber resilient. 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. To progress to being cyber resilient, the Australian Taxation Office and the Department of Immigration and Border Protection need to improve their governance arrangements and prioritise cybersecurity.

Area for improvement

There is one recommendation aimed at improving entities' governance arrangements and cyber resilience.

Cyber resilience

3.1 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. To become cyber resilient, an entity must first establish a sound ICT general controls framework. ICT general controls provide a stable and reliable foundation upon which other processes and controls can be built. An entity must also effectively implement the Top Four mitigation strategies. Together, these form the basis of the entity's cyber resilience. In essence, how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and unauthorised information disclosures, and how well it is positioned to address cyber threats.

ICT general controls

3.2 ICT general controls are entity-wide structures, policies, procedures, and standards applied to information systems that support business processes.²⁰ Effective implementation of ICT general controls provides a level of assurance that an entity's systems are protected from security threats.²¹ Two elements of the ICT general controls framework—logical access control and change management—are crucial as they relate directly to security management.²²

3.3 Table 3.1 shows the aggregated assessment grading for the two ICT general controls for each entity.

20 ANAO Audit Report No. 15 2015-16 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2015*, p. 24.

21 ANAO Audit Report No. 37 2015-16 *Cyber Resilience*, p. 28.

22 *ibid.*

Table 3.1: Aggregated ICT general controls assessment grading

Control areas assessed	Control assessment score		
	DHS	ATO	DIBP
ICT general controls			
ICT change management	▲	▲	▲
Logical access controls	▲	▲	▲

Source: ANAO analysis.

3.4 All entities have a sound ICT general controls framework in place. Changes to systems required endorsements from responsible parties and must go through testing before being implemented in the production environments.

3.5 All entities' logical user access controls were assessed as effective. All entities had controls in place to enforce the 'least privilege principle' over privileged users. The least privilege principle is to assign users with the minimal required system access rights that are necessary to support them performing their defined job duties.

Are entities cyber resilient?

All three entities had improved their cyber resilience—to various degrees—since the 2014 audit.

The Department of Human Services had security controls in place to provide protection from external attacks, internal breaches and unauthorised information disclosures. This was achieved by prioritising activities that were required to address the Top Four mitigation strategies and by strengthening supporting governance arrangements. It is now positioned in the '*cyber resilient*' zone.

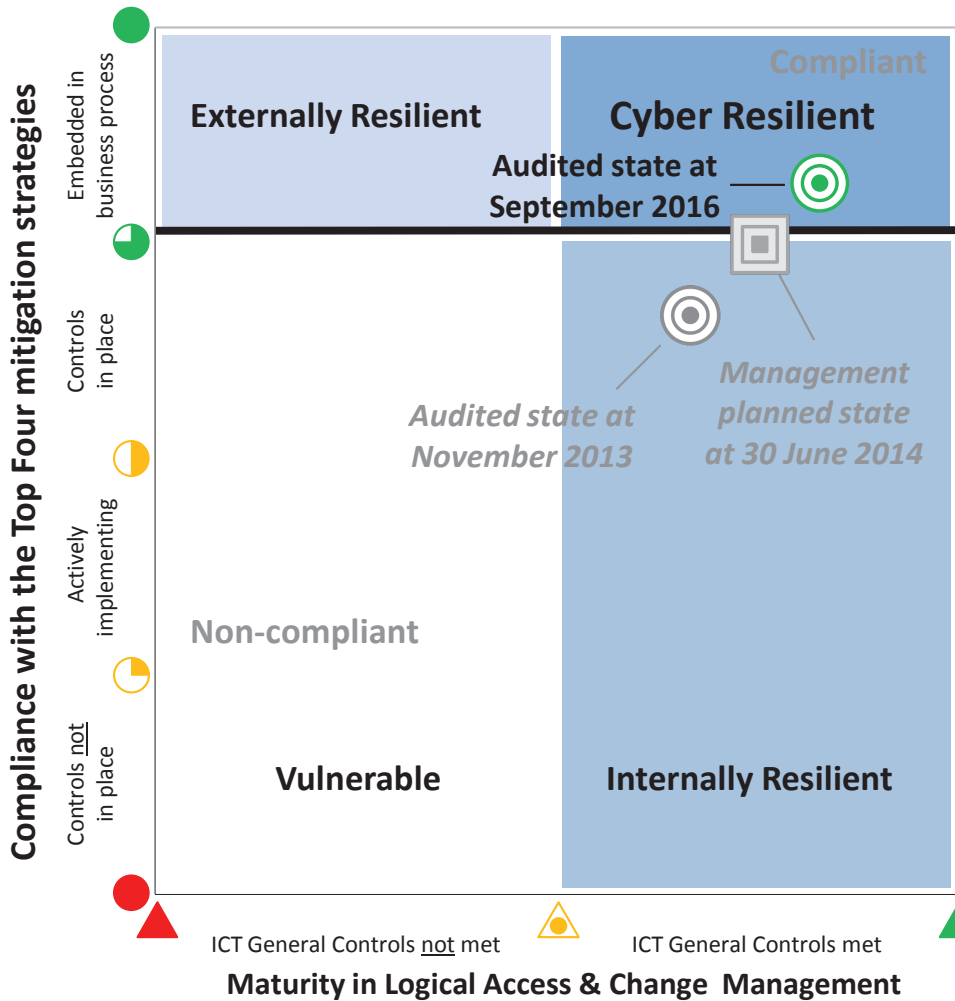
The Australian Taxation Office and the Department of Immigration and Border Protection had security controls that provided a reasonable level of protection from breaches and unauthorised disclosures of information from internal sources. However, there was insufficient protection against cyber attacks from external sources. As a result, they remain in the '*internally resilient*' zone.

3.6 In the first audit (2014), the ANAO examined each selected entities' projects to implement the Top Four mitigation strategies. The ANAO assessed the likelihood of compliance by 30 June 2014 and concluded that all entities would remain in the '*internally resilient*' zone.

3.7 Since the 2014 audit, entities have improved their cyber resilience to various degrees. The ANAO found all entities largely maintained the strength of their ICT general controls frameworks. Despite all entities working towards '*cyber resilience*', only Human Services had achieved it.

3.8 Figure 3.1 shows the change to Human Services' cyber resilience from November 2013 to September 2016.

Figure 3.1: Department of Human Services' cyber resilience

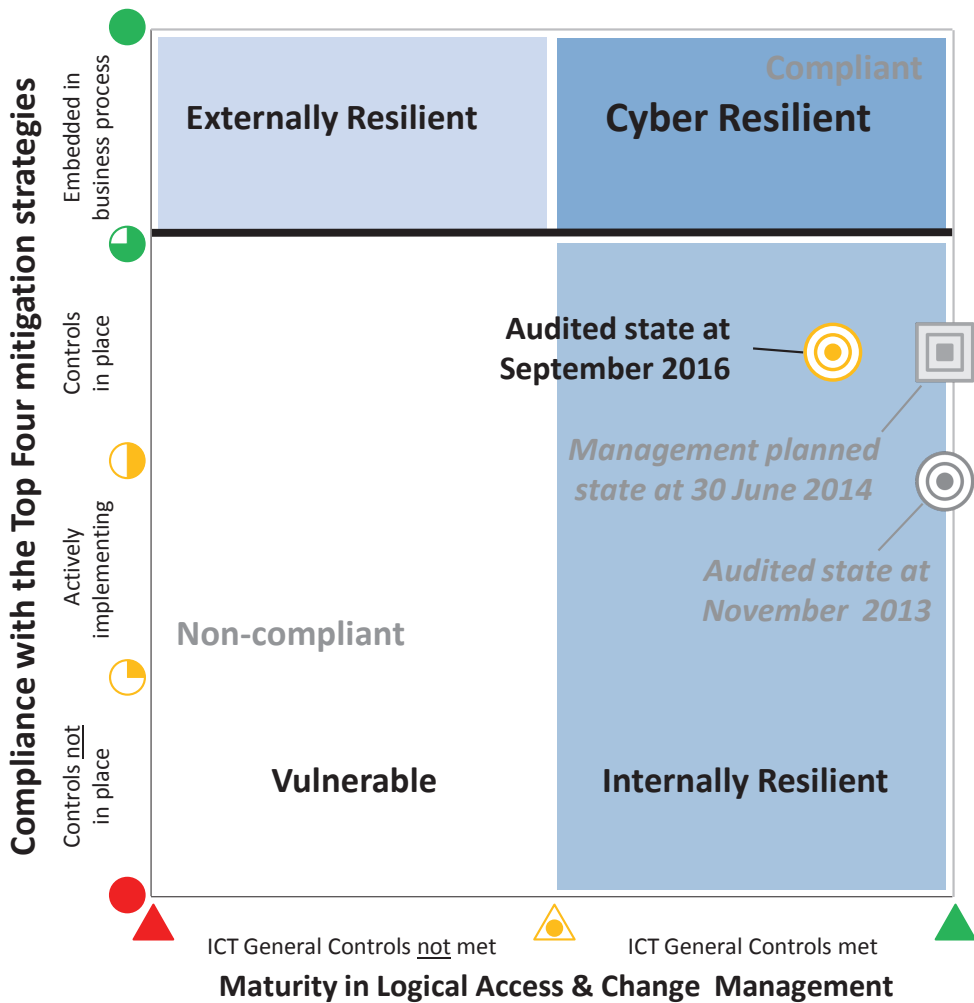


Source: ANAO analysis.

3.9 Human Services is now positioned in the 'cyber resilient' zone. It strengthened its ICT general controls framework and implemented the Top Four mitigation strategies, providing protection from external attacks and internal breaches and unauthorised information disclosures. Human Services achieved this outcome while maintaining a large number of legacy systems that support the Child Support Agency and the Department of Veterans' Affairs and payments for Medicare and Centrelink personal benefits. The ANAO also noted that Human Services maintained high levels of system availability without compromising its ICT security.

3.10 Figure 3.2 shows the change to the ATO's cyber resilience from November 2013 to September 2016.

Figure 3.2: Australian Taxation Office’s cyber resilience

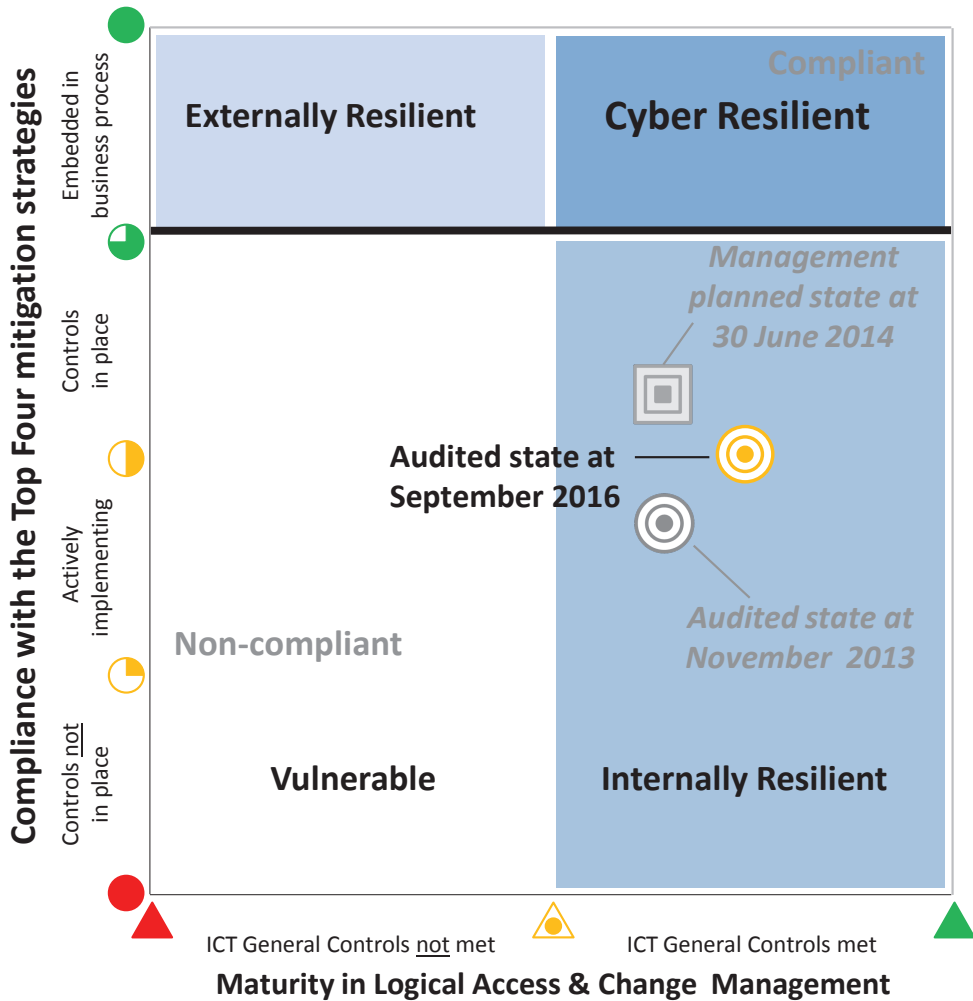


Source: ANAO analysis.

3.11 The ATO improved its cybersecurity position by making progress towards implementing the Top Four mitigation strategies. The ATO maintained a high level of protection from breaches and unauthorised information disclosures from internal sources, despite a slight decline in its ICT general controls framework during this period. The ATO was still vulnerable to external attacks and remained in the 'internally resilient' zone.

3.12 Figure 3.3 shows the change to Immigration’s cyber resilience from November 2013 to September 2016.

Figure 3.3: Department of Immigration and Border Protection's cyber resilience



Source: ANAO analysis.

3.13 Immigration made a small improvement in its cybersecurity position, remaining in the middle of the 'internally resilient' zone. It strengthened its ICT general controls framework and made limited progress towards implementing the Top Four mitigation strategies. Overall, Immigration had a reasonable level of protection from breaches and unauthorised information disclosures from internal sources, but remained vulnerable to external attacks.

Overall comparisons between 2014 and 2016

3.14 In the first audit, the ANAO found that entities had security controls in place to provide a reasonable level of protection from breaches and unauthorised information disclosures from internal sources. However, there was insufficient protection against cyber attacks from external sources. All entities were therefore in the 'internally resilient' zone. All entities were aware of the

shortfalls to implement the Top Four mitigation strategies, and all had plans and worked towards achieving compliance. They accepted the audit findings and endorsed the three recommendations proposed by the ANAO (see Appendix 2).

3.15 Since the first audit in 2014, all three entities have undergone strategic business changes, such as machinery of government changes or upgrading and transforming core ICT systems that support government service delivery. These changes are common in the public sector landscape and entities must maintain business continuity, including ensuring the integrity and availability of their systems, data and information.²³

3.16 A comparison of the summary findings from the first audit and this audit are outlined in Table 3.2 below.

Table 3.2: Comparison between 2014 and 2016 cybersecurity postures

Key areas affecting entities' cyber resilience	Audit observation in 2014	Audit observation in 2016
Senior management awareness	Entities' senior managers lacked awareness of the entities' cybersecurity posture.	Entities' senior managers had a better understanding of the entities overall cybersecurity posture.
Progress towards implementing the Top Four mitigation strategies	Limited initiatives were in place to implement the Top Four mitigation strategies.	There were shortfalls in the implementation of initiatives for the Top Four mitigation strategies.
Implementing new ICT security initiatives	Security controls had been deployed, but these controls were at various states of effectiveness.	Security controls continued to be at various states of effectiveness.
Cybersecurity governance framework	Entities' had established internal information security frameworks.	In practice, entities were not always following the policies and procedures of their internal information security frameworks.
ICT general controls framework	Entities had controls in place to effectively: <ul style="list-style-type: none"> • manage changes to ICT assets; and • manage logical user access provisioning. 	Entities continue to effectively maintain ICT general controls.

Source: ANAO Audit Report No. 50 2013–14 *Cyber Attacks: Securing Agencies' ICT Systems* and ANAO Analysis.

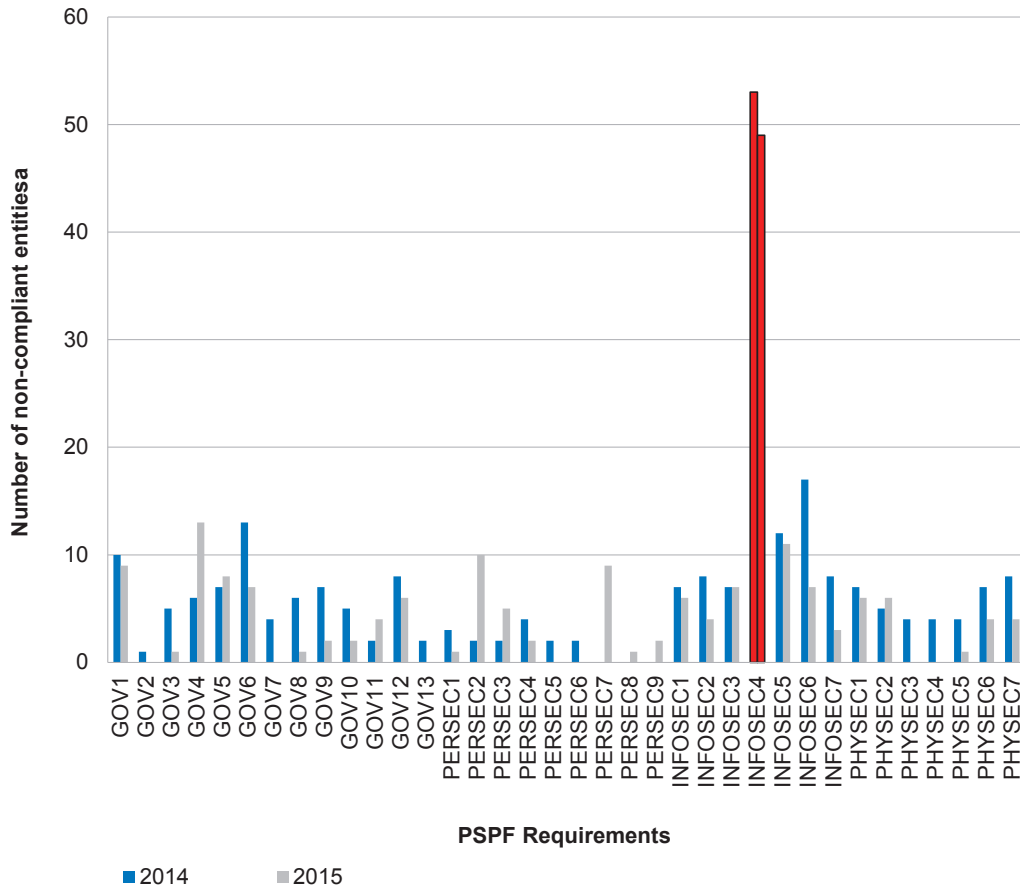
Whole of government comparison

3.17 As discussed in Chapter 2, all government entities are required to undertake an annual self-assessment against the 36 requirements of the Protective Security Policy Framework (PSPF). These 36 requirements are divided into four categories: Governance, Personnel Security, Information Security and Physical Security. The Top Four mitigation strategies are included in the

23 ANAO Audit Report No. 3 of 2016-17 *Machinery of Government Changes*, p. 44.

Information Security category labelled INFOSEC 4.^{24, 25} Figure 3.4 shows INFOSEC 4 has the highest rate of self-assessed non-compliance among the 36 requirements.

Figure 3.4: Compliance comparison by mandatory requirement 2014 and 2015



Note a: A total of 104 entities conducted an annual PSPF compliance self-assessment.

Source: Attorney-General's Department, Protective Security Policy Framework 2014–15 Compliance Report.

3.18 The consolidated results of the self-assessments across government entities are consistent with the findings of the ANAO's three cybersecurity audits. The ANAO has assessed a total of 11 entities and found that only three entities were compliant with the Top Four mitigation

24 INFOSEC 4 "... includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual." The Australian Government Protective Security Policy Framework, op. cit., p. 14.

25 The ISM states that "... To satisfy INFOSEC 4, agencies are required to implement the Top 4 Strategies ..." Australian Signals Directorate, op. cit., p. 118.

strategies.^{26,27} All entities examined were aware of their obligation to be compliant with the Top Four mitigation strategies.

Are entities' effectively prioritising cyber resilience?

Cybersecurity is a strategic priority for the Australian government. 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 core 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.

3.19 Cybersecurity is a strategic priority for the Australian government. As noted in the Prime Minister's Foreword in *Australia's Cyber Security Strategy*:

Australia and Australians are targets for malicious actors—including serious and organised criminal syndicates and foreign adversaries ... The scale and reach of malicious cyber activity ... is unprecedented. The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving.²⁸

3.20 In responding to cyber threats, the Australian Government mandated the Top Four mitigation strategies in April 2013. This mandate is part of the government's initiatives to build cyber resilience for government entities. However, many entities were slow to respond to the government policy requirements.

3.21 The ANAO assessed that there is no impediment to entities establishing a sound ICT general controls framework and effectively implementing the Top Four mitigation strategies. During the series of cybersecurity audits, the ANAO assessed three entities as cyber resilient. These entities chose to prioritise cybersecurity and achieved cyber resilience as a result.

3.22 The ANAO observed that senior executives from cyber resilient entities considered cybersecurity as part of their core business delivery. They were committed to continuously improving their entities' cyber resilience. Entities' senior executives treated cybersecurity as both a business risk and a strategic opportunity, rather than just as an operational matter. There were effective governance arrangements in place to support prioritising cybersecurity and managing cybersecurity risks while still focusing on delivering core business outcomes. These included²⁹:

- informing key stakeholders³⁰ of the consequences of an unsecure ICT environment and not being compliant with the Top Four mitigation strategies;
- sharing the responsibility of cybersecurity risks between stakeholders;

26 ANAO Audit Report No. 50 2014-15 *Cyber Attack: Secure Agencies' ICT Systems*.

27 ANAO Audit Report No. 37 2015-16 *Cyber Resilience*.

28 Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy* [Internet], Commonwealth of Australia, available from <<https://cybersecuritystrategy.dpmc.gov.au/>>, [accessed November 2016].

29 Australian National Audit Office, *Better Practice Guide, Public Sector Governance: Strengthening Performance Through Good Governance*, June 2014, Canberra.

30 Key stakeholders include executives, security teams, ICT operations teams, business owners and contract management teams.

- clearly defining accountabilities for cybersecurity; and
- involving key stakeholders when making investment decisions about cybersecurity initiatives.

3.23 To progress towards cyber resilience entities need to improve their governance arrangements and prioritise cybersecurity. Effective governance would help entities to implement robust cybersecurity controls and sustain a cyber resilient posture. Entities that operate in a cyber resilient environment are better positioned to protect their core business processes from cybersecurity risks. They are also able to better maintain the public's confidence in the government's ability to deliver its programs and services. A key step towards achieving cyber resilience is a stronger focus by government entities on cybersecurity.

Recommendation No.2

3.24 The ANAO recommends that entities improve their governance arrangements, by:

- asserting cybersecurity as a priority within the context of their entity-wide strategic objective;
- ensuring appropriate executive oversight of cybersecurity;
- implementing a collective approach to cybersecurity risk management; and
- conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

Department of Human Services' response: *Agreed.*

3.25 *The department's management of its cyber operations is aligned with the ANAO's recommendation for improving governance arrangements and cyber resilience. The report notes that the department has achieved cyber resilience by prioritising cyber security and strengthening supporting governance arrangements.*

3.26 *The establishment of a dedicated Cyber Security Operations Centre clearly demonstrates the department's strong commitment to cyber security as an entity wide strategic objective. Cyber security is a standing agenda item at executive level governance committees and boards to ensure appropriate visibility, transparency and understanding of current threats, mitigations risks and impacts.*

Australian Taxation Office's response: *Agreed.*

3.27 *The ATO places high priority on cybersecurity and recognises that confidence in security and safety of data and systems is paramount to offering services to the Australian community.*

3.28 *The ATO has reflected this in the current Corporate Plan.*

3.29 *The ATO has strong executive oversight of cybersecurity through our Security Committee.*

3.30 *The ATO has overhauled its governance arrangements with our third party suppliers to strengthen our compliance to cyber controls. In addition, the 'essential eight' cybersecurity controls will form part of the regular reporting requirements to the Security Committee and newly formed Risk Management Committee going forward.*

Department of Immigration and Border Protection's response: Agreed.

3.31 *The Department agrees with this recommendation and has commenced actions to improve its governance arrangements for cybersecurity.*

3.32 *To improve executive oversight of cybersecurity, the Chief Information Security Officer (CISO) role has been elevated to the First Assistant Secretary Integrity, Security and Assurance position.*

3.33 *A review of cyber security executive oversight and governance is also planned for the Department's 2017–18 strategic assurance programme.*



Grant Hehir
Auditor-General

Canberra ACT
15 March 2017

Appendices

Appendix 1 Entity response

The formal responses received by ANAO following circulation of the draft report from the Department of Human Services; Australian Taxation Office; and the Department of Immigration and Border Protection have been reproduced on the following pages.



Australian Government
Department of Human Services

Kathryn Campbell CSC
Secretary

Ref: EC17-000262

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

Dear Mr Hehir

Thank you for your letter of 24 January 2017, providing the Department of Human Services (the department) with the opportunity to comment on the Australian National Audit Office's (ANAO) proposed report on *Cybersecurity Follow-Up Audit*.

The department agrees with the ANAO's recommendations and is pleased to note that the ANAO found the department to be cyber resilient. I am also pleased to advise that the department has commissioned a Cyber Security Operations Centre to maintain and further improve its cyber security arrangements.

Attachment A to this letter details the overall response to the proposed report and to each of the recommendations.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Kathryn Campbell'.

Kathryn Campbell
17 February 2017

PO Box 7788, Canberra Business Centre ACT 2610 • Telephone (02) 6223 4411 • Facsimile (02) 6223 4489
Internet www.humanservices.gov.au

Attachment A

Response to the proposed audit report on “*Cybersecurity Follow-up Audit*”:

Summary of response for inclusion in ‘Summary’ section of report

The Department of Human Services (the department) welcomes this report and considers that the Australian National Audit Office (ANAO) recommendations support effective cyber security governance arrangements.

The department is committed to protecting the confidentiality, integrity and availability of its information and assets. We are pleased to note the ANAO found that the department was compliant with the Top Four mandatory cyber strategies and was cyber resilient. Achieving this compliance and strengthening cyber security governance arrangements has been a priority for the department over recent years. As a result, the department can continue to deliver government outcomes while also effectively managing a rapidly escalating and changing cyber threat environment.

Response to Recommendations

Recommendation No.1

The ANAO recommends that entities periodically assess their cyber security activities to provide assurance that: they are accurately aligned with the outcomes of the Top Four mitigation strategies and entities’ own ICT security objectives; and that they can report on them accurately. This applies regardless of whether cybersecurity activities are insourced or outsourced.

The department’s response: Agree

The ANAO has concluded that the department was cyber resilient and accurately self-assessed its compliance against the Top Four mandatory strategies. Continuous monitoring of cyber security activities in place at the time of the audit has been strengthened by the establishment of a team dedicated to compliance activities. The outcomes of these activities are routinely reported to the Executive through numerous governance boards.

Recommendation No.2

The ANAO recommends that entities improve their governance arrangements, by:

- (a) asserting cybersecurity as a priority within the context of their entity-wide strategic objective;
- (b) ensuring appropriate executive oversight of cybersecurity;
- (c) implementing a collective approach to cybersecurity risk management; and
- (d) conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

The department's response: Agree

The department's management of its cyber operations is aligned with the ANAO's recommendation for improving governance arrangements and cyber resilience. The report notes that the department has achieved cyber resilience by prioritising cyber security and strengthening supporting governance arrangements.

The establishment of a dedicated Cyber Security Operations Centre clearly demonstrates the department's strong commitment to cyber security as an entity wide strategic objective. Cyber security is a standing agenda item at executive level governance committees and boards to ensure appropriate visibility, transparency and understanding of current threats, mitigations risks and impacts.



Australian Government
Australian Taxation Office

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

Dear Ms Kelly

**AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE FOLLOW-UP AUDIT
- CYBERSECURITY**

Thank you for your letter dated 24 January 2017 and for the opportunity to provide comments on the Cybersecurity Follow-up Audit.

The ATO agrees with the two recommendations as presented in the section 19 report.

Attached is the ATO response to recommendations (Annexure 1) and summary of our comments to be included in the report (Annexure 2).

I would like to thank the Australian National Audit Office audit team for the cooperative and professional manner they have adopted in working with us on this matter. I look forward to continuing the good working relationship developed in this performance audit.

If you require further information on this matter, please contact Steve McCauley, Assistant Commissioner, IT Security on 02 6216 1611 or 0416 242 620.

Yours sincerely

A handwritten signature in black ink, appearing to read 'R. Katf'.

Ramez Katf
Chief Information Officer
Australian Taxation Office

Date: 20 February 2017

Annexure 1

Summary of ATO's response

The ATO welcomes this review and agrees with the two recommendations in the report.

The ATO is increasingly taking advantage of new technologies which provide convenient and accessible services for the community. These new and emerging technologies are often accompanied with new and emerging risks.

We consider and manage risks associated with new technology to protect the integrity of the tax and superannuation systems and works across government to strengthen the security of digital services.

The ATO is committed to meeting community expectations for data security and privacy protection and to providing improved services.

The review recognised the ATO's strong general information communications technology controls and we will continue to build upon these and continuously improve our overall cybersecurity governance arrangements.

While there has been improvement in the overall maturity of the security posture of the ATO, the review clearly highlighted further improvements that are required. The ATO has committed additional resource and focus to address deficiencies and reach a greater level of cyber resilience. Immediate improvements have already been put in place with a commitment to reach cyber resilience status in 2017.

Annexure 2

Rec	ANAO recommendation	ATO response
1	<p>The ANAO recommends that entities periodically assess their cyber security activities to provide assurance that the activities are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives. This applies regardless of whether cybersecurity activities are insourced or outsourced.</p>	<p>Agreed.</p> <p>As the ATO continues to enhance our systems to provide better services for the Australian community, we are focused on maintaining the security and integrity of our data and information. Understanding new threats and protecting our systems from any potential vulnerabilities is a priority.</p> <p>Following advice from external scrutineers, the ATO has merged its Information Security and IT Security capabilities to form one integrated Information and IT Security functional unit. We have also appointed an SES Band 2 as the Chief Security Officer (CSO).</p> <p>The CSO and the integrated security unit have been charged with taking a multifaceted approach to cyber security; including regular information technology risk and threat assessments, strategy and policy (including a revised whitelisting strategy), system certification reviews, monitoring and compliance regime.</p> <p>In addition the CSO will ensure that findings and recommendations relating to cyber security from scrutineers (such as the subject audit) are followed up and implemented how and when necessary.</p> <p>The ATO is working to reflect the newly released 'essential eight', cybersecurity controls which incorporate the 'Top 4' covered in this Audit.</p>
2	<p>The ANAO recommends that entities improve their governance arrangements by:</p> <ol style="list-style-type: none"> a. Asserting cybersecurity as a priority within the context of their entity-wide strategic objective; b. Ensuring appropriate executive oversight of cyber security; c. Implementing a collective approach to cybersecurity risk management; and d. Conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness. 	<p>Agreed.</p> <p>The ATO places high priority on cyber security and recognises that confidence in security and safety of data and systems is paramount to offering services to the Australian community.</p> <p>The ATO has reflected this in the current Corporate Plan.</p> <p>The ATO has strong executive oversight of cybersecurity through our Security Committee.</p> <p>The ATO has overhauled its governance arrangements with our third party suppliers to strengthen our compliance to cyber controls. In addition, the 'essential eight' cyber security controls will form part of the regular reporting requirements to the Security Committee and newly formed Risk Management Committee going forward.</p>



Michelle Kelly
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
19 National Circuit
Barton ACT 2600

Dear Ms Kelly

Proposed report on Cybersecurity Follow-up Audit

Thank you for the opportunity to review and comment on your proposed report to Parliament on the designated agencies and our own compliance with the Australian Signals Directorate (ASD) Top Four mitigation strategies and the overall level of cyber resilience.

I would like to express my appreciation for the way your team conducted the field phase and their willingness to consult with my leadership team and technical staff on matters you observed during your work.

The Department agrees with the findings of the report and supports the recommendations.

However, in considering the findings raised in the report, it is important to recognise the previous audit tabled in June 2014, ANAO Audit Report No. 50 2013-14, Cyber Attacks: Securing Agencies' ICT Systems assessed the former Australian Customs and Border Protection Service (ACBPS). The current audit assessed the Department of Immigration and Border Protection, which operates in a significantly more complex environment, from migration policy, visa and cargo processing to frontline border operations involving the timely movement of people and goods across the border that include civil maritime security operations and border law enforcement activities.

July 2015 saw the disestablishment of the ACBPS and the creation of the Australian Border Force as part of an integrated immigration and border protection portfolio. From an ICT perspective this presented an enormous challenge of integrating two very different ICT architectures, ICT operational management processes and cybersecurity maturity. Combined the two agencies have over 900 applications, of which 569 are unique, and of 279 business critical, approximately 70% are bespoke. These applications are supported by over \$250 million of ICT infrastructure that is located in 84 regional locations around Australia and 51 offshore posts. The integrated portfolio had multiple external service providers including two telecommunications and two mainframe processing providers, which have now been transitioned to single providers.

In comparing DIBP with the other agencies subject to this audit, it is important to recognise the relevant position of each agency on the ICT investment curve. This in turn has a direct implication and relationship to the maturity of their respective cyber security initiatives. DHS and ATO have invested heavily over the last three to five years in large cybersecurity and ICT investment programmes. DIBP, however, is only in its second year of a number of multi-year programmes - Security; Identity and Access Management; End User Computing Capability and

- 2 -

ICT Consolidation that will significantly enhance the Department's current cybersecurity capability.

The Security Programme includes a dedicated project focused on delivering and maintaining compliance with the ISM Top Four mitigation strategies. This financial year the project will deliver:

- Improved and effective application whitelisting across all desktops by July 2017
- Improved cybersecurity compliance and vulnerability reporting to the Department's Executive.

The Identity and Access Management (IAM) Programme incorporates significant improvements in the overall management of privileged accounts including a proof of concept for the introduction of multifactor authentication for privileged accounts to be completed this financial year.

The End User Computing Consolidation (EUCC) Programme due to be completed by June 2020 will introduce the single departmental end user ICT environment BorderNet (this includes a single desktop, printing service, email and file systems). It is complimentary with the IAM and Security programmes as it will deliver more robust ICT security controls including improved user account management, application whitelisting and security auditing are built into BorderNet. The EUCC programme has already commenced rolling out the new desktop which includes application whitelisting.

The move to a single Departmental ICT environment, that will include the rationalisation of the Department's large application and infrastructure environment is also progressing and is due to be completed by 2020. The cost of these integration initiatives have been absorbed by the internal Departmental budget.

The Department recognises that cybersecurity is a critical issue for government agencies and with the amalgamation of the two major government border agencies to form the new Department and the Australian Border Force there is added emphasis on cybersecurity issues.

The Department's responses to the recommendations and our summary response are at Attachment A.

If you would like to further discuss our response to the audit report, please contact Mr Stephen Hayward (Chief Audit Executive) on 02 6264 1427.

Yours sincerely



Jenet Connell
Chief Operating Officer
Deputy Secretary Corporate

20 February 2017



Maria Fernandez
Deputy Secretary Intelligence and Capability

20 February 2017

Attachment A - DIBP Response to ANAO Report

Summary response

The Department of Immigration and Border Protection (DIBP) recognises and accepts the risks posed in the cyber domain and acknowledges the importance of compliance with the ISM Top Four mitigation strategies.

The Department has taken a risk based approach to cybersecurity, taking into account our position in the ICT investment cycle. The Department manages this risk through a number of controls.

The Department's Executive Committee is committed to maintain the Department's cybersecurity posture. In responding to this ever present threat, the Department has invested in a number of major programmes. These include: Security; Identity and Access Management; End User Computing Capability and ICT Consolidation these programmes will significantly enhance the Department's current cybersecurity capability and improve the Department's compliance with the Top Four mitigation strategies.

In considering the findings raised in the report, it is important to recognise the previous audit tabled in June 2014, ANAO Audit Report No. 50 2013-14, assessed the former Australian Customs and Border Protection Service (ACBPS). The current audit assessed the Department of Immigration and Border Protection, which operates in a significantly more complex environment, from migration policy, visa and cargo processing to frontline border operations involving the timely movement of people and goods across the border that include civil maritime security operations and border law enforcement activities.

July 2015 saw the dis-establishment of the ACBPS and the creation of the Australian Border Force as part of an integrated immigration and border protection portfolio. From an ICT perspective this presented an enormous challenge of integrating two very different ICT architectures, ICT operational management processes and cybersecurity maturity.

In comparing DIBP with the agencies, subject to this audit it is important to recognise the relevant position of each agency on the ICT investment curve. This in turn has a direct implication and relationship to the maturity of their respective cybersecurity initiatives. DHS and ATO have invested heavily over the last three to five years in large cybersecurity and ICT investment programmes. DIBP, however, is only in its second year of a number of multi-year programmes.

Responses to Recommendations

Recommendation No. 1:

The ANAO recommends that entities periodically assess their cybersecurity activities to provide assurance that the activities are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives. This applies regardless of whether cybersecurity activities are insourced or outsourced.

The Department agrees with this recommendation and will assess its cyber security activities on an annual basis.

- 4 -

Recommendation No. 2:

The ANAO recommends that entities improve their governance arrangements, by,

- a) Asserting cybersecurity as a priority within the context of their entity-wide strategic objective;*
- b) Ensuring appropriate executive oversight of cybersecurity;*
- c) Implementing a collective approach to cybersecurity risk management; and*
- d) Conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.*

The Department agrees with this recommendation and has commenced actions to improve its governance arrangements for cybersecurity.

To improve executive oversight of cybersecurity, the Chief Information Security Officer (CISO) role has been elevated to the First Assistant Secretary Integrity, Security and Assurance position.

A review of cyber security executive oversight and governance is also planned for the Department's 2017-18 strategic assurance programme.

Appendix 2 Recommendations from previous audits

Box 1: The recommendations of the previous audits and the JCPAA review

Audit Report No. 50 2013–14 Cyber Attacks: Securing Agencies' ICT Systems

ANAO Recommendation No. 1

To achieve full compliance with the mandatory ISM strategies and related controls, the ANAO recommends that agencies:

- (a) complete activities in train to implement the top four ISM controls across their ICT environments; and
- (b) define pathways to further strengthen application whitelisting, security patching for applications and operating systems, and the management of privileged accounts.

Response from selected agencies: Agreed

ANAO Recommendation No. 2

To reduce the risk of cyber attacks to information stored on agency databases, the ANAO recommends that agencies strengthen logical access controls for privileged user accounts to the database by eliminating shared accounts, recording audit logs and monitoring account activities.

Response from selected agencies: Agreed

ANAO Recommendation No. 3

To strengthen their ICT security posture, the ANAO recommends that agencies:

- (a) conduct annual threat assessments across the ICT systems, having regard to the Top 35 Mitigations Strategies—as proposed by the Australian Signals Directorate; and
- (b) implement periodic assessment and review by the agency security executive of the overall ICT security posture.

Response from selected agencies: Agreed

Audit Report No. 37 2015–16 Cyber Resilience

ANAO Recommendation No. 1

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

Response from selected entities: Agreed.

ANAO Recommendation No. 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.

Response from selected entities: Agreed.

ANAO Recommendation No. 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.

Response from selected entities: Agreed.

Appendix 3 Compliance grading scheme

1. In order to assess compliance consistently across the three entities, the ANAO applied a set of assessment criteria and developed a graphical key; a reporting convention similar to a 'traffic light' report. The keys are represented as either a Harvey Ball or cone. The key is outlined in Table A.1.

Table A.1: Key to grading scheme for assessing compliance with the Top Four mitigation strategies and ICT general controls

Grading scheme for mandatory ISM strategies	Grading scheme for ICT general controls
 Controls not in place and no dispensation authorised by the Accountable Authority.	 Control objectives not met.
 Controls not in place but a dispensation is authorised by the Accountable Authority.	 Identified controls not in place but compensating controls in place and observed.
 Controls not in place but entity is actively implementing, with a minimum of design deliverables in evidence.	 Control objectives met.
 Control 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 September 2016.

Source: ANAO.

2. The selected entities were assessed on their:

- compliance with the Top Four mitigation strategies and related controls; and
- maturity to effectively manage logical access and change management as part of normal business processes (ICT general controls).

3. The ANAO's summary findings for each of the selected entities are reported in the context of a matrix, shown in Figure 2.1, which indicates entities' overall level of protection against internal and external threats as a consequence of steps taken to implement the Top Four mitigation strategies and ICT general controls. The matrix, which is referred to as the *Entity Cyber Resilience*, indicates where entities are positioned in terms of cyber resilience zones: *vulnerable zone*; *externally resilience zone*; *internally resilience zone*, and *cyber resilience zone*.

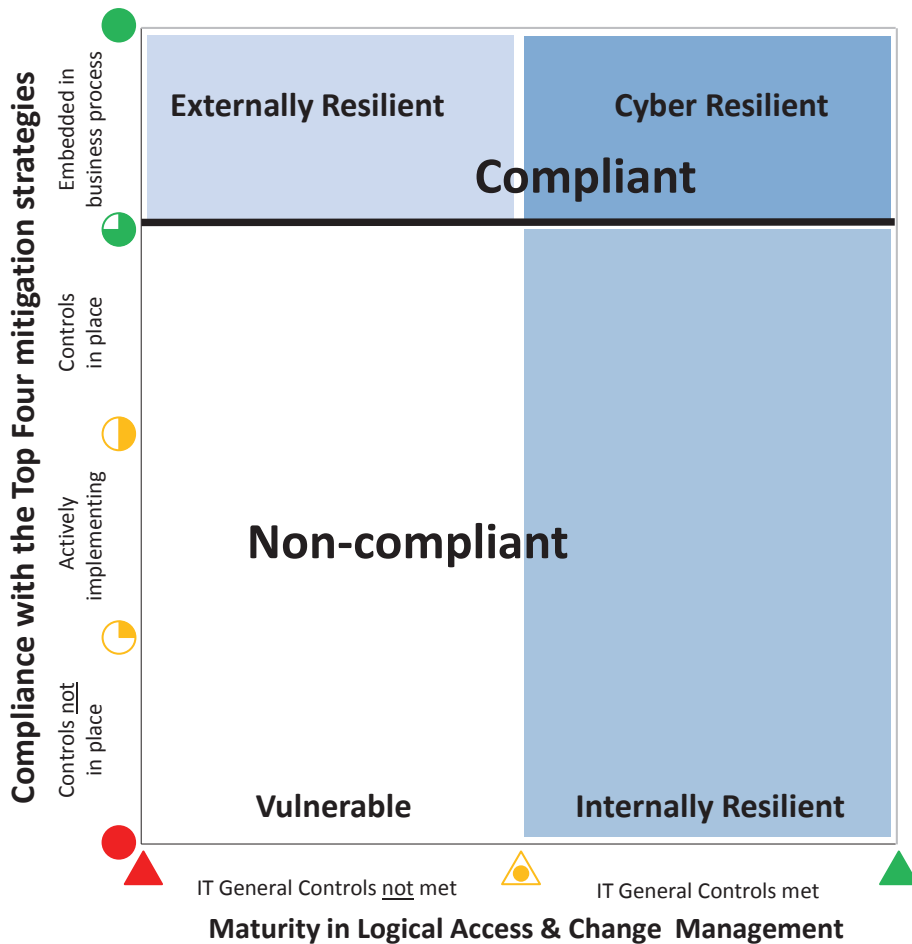
4. The zones are explained further in Table A.2 and illustrated in Figure A. 1. An entity's position indicates its overall cyber resilience—in essence how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

Table A.2: Definitions of the Cyber Resilient 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 both external attacks and internal breaches and disclosures of information.

Source: ANAO.

Figure A. 1: Entity cybersecurity posture matrix



Source: ANAO.

