The Auditor-General
Audit Report No.50 2013–14
Performance Audit

Cyber Attacks: Securing Agencies' ICT Systems

Across Agencies

Australian National Audit Office

© Commonwealth of Australia 2014

ISSN 1036–7632
ISBN 0 642 81490 2 (Print)
ISBN 0 642 81491 0 (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:
publications@anao.gov.au.

Australian National
Audit Office

Canberra ACT
24 June 2014

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit across agencies titled *Cyber Attacks: Securing Agencies' ICT Systems.* 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

Ian McPhee
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:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7505
Fax: (02) 6203 7519
Email: publications@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:

http://www.anao.gov.au

Audit Team

Alex Doyle
Elenore Karpfen
William Na
Gayantha Mendis
IT Audit Branch
David Gray

Contents

Abbreviations 8
Glossary 9
Summary and Recommendations 11
Summary 12
Introduction 12
Audit objectives, criteria and scope 16
Overall conclusion 17
Key findings 19
Summary of agencies' responses 25
Recommendations 29
Audit Findings 31
1. Background and Context 33
Introduction 33
The protective security framework 35
Audit coverage 40
Selected agencies in this audit 41
Audit objectives, criteria and approach 42
Structure of the report 45
2. Agency Compliance 46
Introduction 46
Assessing compliance 47
Agency compliance grades – summary assessment 50
Agencies' planned improvement activities 54
Conclusion 57
3. Implementing Mandatory Strategies and Related Controls 60
Introduction 60
Deploying Application Whitelisting 61
Patching Applications 68
Patching Operating Systems 73
Restrict Administrative Privileges 77
Conclusion 81
4. IT General Controls 83
Introduction 83
Managing logical access controls 83
Change management process 94
Conclusion 99

5. Strengthening Agencies' ICT Security Posture 101
Introduction 101
Strengthening cyber resilience 102
Conclusion 106

Appendices 109

Appendix 1: Agency responses to the proposed report 110
Appendix 2: Audit criteria and compliance statements 120
Index 122
Series Titles 125
Better Practice Guides 131

Tables

Table S.1: Key information collected, stored and used by the selected agencies 15
Table S.2: Definition of the ICT security zones 19
Table 1.1: Key information collected, stored and used by the selected agencies 42
Table 2.1: Key to grading scheme for assessing compliance with the mandatory ISM strategies and related controls, and for the IT general controls 47
Table 2.2: Definition of the ICT security zones 49
Table 3.1 Summary of the controls agencies must implement on all systems that receive email or Internet content 61
Table 3.2: Summary assessment of agencies' compliance with application whitelisting controls across the desktop and servers 63
Table 3.3: Summary assessment of agencies' compliance with controls to patch applications 70
Table 3.4: Summary assessment of agencies' compliance with controls to patch desktop and server operating systems 74
Table 3.5: Summary assessment of agencies' compliance with controls for privileged access accounts 78
Table 4.1: Summary assessment of agencies' compliance with logical access control requirements at the network security layer 85
Table 4.2: Summary assessment of agencies' compliance with logical access control requirements at the applications security layer 88
Table 4.3: Summary assessment of agencies' compliance with logical access control requirements at the database security layer 91
Table 4.4: Summary assessment of agencies' compliance with logical access control requirements at the operating systems security layer 93

Table 4.5: Summary assessment of agencies' compliance with change management process requirements 96
Table A.1. Audit criterion one, and compliance statements 120
Table A.2 Audit criteria two and three, and compliance statements..... 121

Figures

Figure S.1: Agency Compliance Grade: summary assessment of agencies' compliance with top four mandatory strategies and related controls, and overall ICT security posture 20
Figure 2.1: Reporting on level of security obtained by implementing the mandatory ISM strategies and IT general controls 48
Figure 2.2: Agency Compliance Grade: summary assessment of agencies' compliance with top four mandatory strategies and related controls, and overall ICT security posture 51
Figure 2.3: Agencies' observed compliance grade and planned state..... 56
Figure 5.1: Better Practice Example: Conduct cyber health checks 105

Abbreviations

ABS	Australian Bureau of Statistics
ACSC	Australian Cyber Security Centre
AFSA	Australian Financial Security Authority
AGD	Attorney-General's Department
ASD	Australian Signals Directorate *previously Defence Signals Directorate (DSD)*
ATO	Australian Taxation Office
CISO	Chief Information Security Officer
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Human Services
FMA Act	*Financial Management and Accountability Act 1997*
ICT	Information and Communications Technology
ISM	Australian Government Information Security Manual
ITSA	Information Technology Security Advisor
ITSM	Information Technology Security Manager
ITSO	Information Technology Security Officer
JCPAA	Joint Committee of Public Accounts and Audit
PSPF	Australian Government Protective Security Policy Framework
NBN	National Broadband Network

Glossary

Agency (or Australian Government agency)	As used in the PSPF, includes all Australian Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the *Public Service Act 1999*, the *Financial Management and Accountability Act 1997* or the *Commonwealth Authorities and Companies Act 1997*.
Agency head	As used in the PSPF, the head of any Australian Government department, authority, agency or body.
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.

Summary and Recommendations

Summary

Introduction

1. Governments, businesses and individuals increasingly rely on information and communications technology (ICT) in their day-to-day activities, with rapid advances continuing to be made in how people and organisations communicate, interact and transact business through ICT and the Internet. In the government sector, ICT is used to deliver services, store and process information, and enable communications, with a consequent need to protect the privacy, security and integrity of information maintained on government systems.

2. Cyber crime is an international problem, and it is estimated that in 2012, 5.4 million Australians fell victim to such crimes, with an estimated cost to the economy of $1.65 billion.[1,2] In the government sector, the Australian Signals Directorate (ASD)[3] has estimated that between January and December 2012, there were over 1790 security incidents against Australian Government agencies. Of these, 685 were considered serious enough to warrant a Cyber Security Operations Centre response.[4]

3. The protection of Australian Government systems and information from unauthorised access and use is a key responsibility of agencies, having regard to their business operations and specific risks. In the context of a national government, those risks can range from threats to national security through to the disclosure of sensitive personal information. Unauthorised access through electronic means, also known as cyber intrusions, can result from the actions of outside individuals or organisations. Individuals operating

---

1 National cyber security expenditure was approximately $480 million in 2011–12, representing approximately 13.9 per cent of Australian Government Homeland and Border security expenditure. See Department of the Prime Minister and Cabinet, *Strong and Secure: A strategy for Australia's National Security*, 2013, p. 15.

2 The most recent Australian survey on cyber risks to business indicates that some 56 per cent of organisations identified cyber security incidents on their networks in 2013, compared to 22 per cent in 2012, an increase of 34 per cent. See Attorney-General's Department, CERT Australia, *Cyber Crime & Security Survey Report 2013*, p. 5.

3 Until 2013, ASD was known as the Defence Signals Directorate (DSD). To avoid confusion, it will be referred to as ASD throughout this audit report.

4 The Centre, established in ASD, has two main roles: to provide government with a better understanding of sophisticated cyber threats against Australian interests; and to coordinate and assist operational responses to cyber events of national importance across government and systems of national importance.

from within government may also misuse information which they are authorised to access, or may inappropriately access and use government information holdings.[5]

4. 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, to inform the ICT security posture[6] of agencies. 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.

Mitigation strategies

5. The Attorney-General's Department (AGD) is responsible for administering the Australian Government's protective security policy, which has as its objective to promote the most effective and efficient ways to secure the continued delivery of Government business. AGD's *Protective Security Policy Framework* (PSPF)[7] outlines the core requirements for the effective use of protective security as a business enabler. To facilitate government working confidently and securely, the PSPF assists agencies to: identify their levels of security risk tolerance; develop an appropriate security culture; and achieve the mandatory protective security requirements expected by the Government.

6. The PSPF is supported by the *Australian Government Information Security Manual* (ISM)[8], which is released by ASD, and is the standard governing the security of government ICT systems.

7. 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 fully implemented,

---

5 The scale and sophistication of cyber attacks against government and private sector systems has increased significantly, with ASIO highlighting in 2012–13 the threats posed to national security and economic competitiveness by cyber activity, espionage through electronic means, and the unauthorised use of sensitive material by trusted employees. See Australian Security Intelligence Organisation, *ASIO Report to Parliament 2012–2013* [Internet], available from <http://www.asio.gov.au> [accessed on 4 November 2013].

6 In essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

7 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.

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

the top four mitigation strategies would prevent at least 85 per cent of the targeted cyber intrusions to an agency's ICT systems. This list of strategies is revised annually based on the most recent analysis of incidents.

8. 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 executed[9];
- patching applications: applying patches to applications and devices to ensure the security of systems[10];
- patching operating systems: deploying critical security patching to operating systems to mitigate extreme 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.[11,12]

9. An amendment to the PSPF issued in April 2013, had the effect of: mandating the top four mitigation strategies with immediate effect; and setting a target date of July 2014 for full implementation of the top four strategies. Effective implementation of the mandated strategies assists agencies in achieving control over their ICT systems, providing a higher level of assurance that systems will continue to support the day-to-day business services of the agency.

---

9 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.

10 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.

11 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.

12 Similarly, 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 agencies in this audit

10. Seven agencies were selected by the ANAO to be included in this performance audit:

- Australian Bureau of Statistics (ABS);
- Australian Customs and Border Protection Service (Customs);
- Australian Financial Security Authority (AFSA);
- Australian Taxation Office (ATO);
- Department of Foreign Affairs and Trade (DFAT);
- Department of Human Services (DHS); and
- IP Australia.

11. These agencies were selected based on the character and sensitivity of the information primarily managed by the agency, as summarised in Table S.1.

Table S.1: Key information collected, stored and used by the selected agencies

Australian Government agency	Economic information	Policy and regulatory information	National security information	Program and service delivery	Personal information
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				✓	✓
IP Australia		✓		✓	

Source: ANAO analysis.

Audit objectives, criteria and scope

12. The audit objective was to assess selected agencies' compliance with the four mandatory ICT security strategies and related controls in the *Australian Government Information Security Manual* (ISM). The audit also considered the overall ICT security posture of the selected agencies, based on their implementation of the four mandated mitigation strategies and IT general controls.

13. The ANAO examined agency-level implementation of the 'Top Four' mitigation strategies and related controls mandated in the ISM. In addition, the audit assessed whether the selected agencies had accurately stated their compliance against the ISM controls in their self-assessment reports to the Attorney-General's Department, against the protective security governance guidelines on compliance reporting.[13]

14. The audit also considered the selected agencies' overall ICT security posture, having regard to agencies' implementation of IT general controls[14] and the top four mitigation strategies and related controls. The audit did not consider the PSPF mandatory requirements relating to physical security. A recent ANAO performance audit examined the application of physical security requirements by three Australian Government agencies.[15]

15. In this audit, the ANAO departed from its usual practice of identifying agencies on individual issues due to the risk of disclosing sensitive information about agency ICT systems. In addition, security weaknesses are only addressed at an aggregate level. However, a summary assessment of each agency's performance against the audit objective is provided in Figure S.1.

16. The audit is part of a program of cross-agency performance audits which have examined processes supporting the delivery of services by Government agencies. Since 2000 the ANAO has undertaken 12 cross-agency

---

13 The guidelines contain the underlying principles and outline the responsibilities that agencies are required to follow when measuring their compliance against the PSPF mandatory requirements. See Attorney-General's Department, *Protective security governance guidelines–Compliance reporting* [Internet], 2012, available from <http://www.protectivesecurity.gov.au/governance/audit-reviews-and-reporting/Pages/Supporting-guidelines-for-audit-reviews-and-reporting.aspx> [accessed 17 June 2013].

14 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.

15 ANAO Audit Report No.49 2013–14, *The Management of Physical Security.*

audits on protective security arrangements. In each of these audit reports the ANAO has encouraged all Government agencies to assess the benefits of the recommendations in light of their own circumstances and practices.

Overall conclusion

17. Modern information and communications technology (ICT) and the Internet are increasingly relied upon by Australian Government agencies as business enablers, to the mutual benefit of government and the community. Benefits include improved access to government services and more cost-effective administration.

18. In this context, the protection of ICT systems and information is a key responsibility of government agencies, and includes: the prevention of unauthorised access by outsiders seeking to exploit the Internet; and by insiders seeking to misuse their trusted status. Unauthorised access and misuse of government information is an international issue which can affect, amongst other things, national security, the economy, personal privacy, and the integrity of data holdings. The Australian Government has established a protective security framework and identified ICT-specific risk mitigation strategies and related controls which provide a basis for agencies' management of risks to their ICT systems and information. Four key mitigation strategies—intended to control access to ICT systems and apply timely security upgrades—were mandated by the Australian Government in January 2013, and agencies are expected to achieve full compliance with those strategies by July 2014.

19. The agencies subject to audit had established internal information security frameworks, implemented controls designed to safeguard the enterprise ICT environment from external cyber attack, and had stipulated change management processes to authorise the implementation of security patches for applications and operating systems. While these arrangements contributed to the protection of agency information, the selected agencies had not yet achieved full compliance with the top four mitigation strategies mandated by the Australian Government in 2013; a requirement reflecting heightened government expectations in response to the risk of cyber attack. Further, none of the selected agencies are expected to achieve full 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.

20. Based on their stage of implementation of the top four mitigation strategies and IT general controls, the selected agencies' overall ICT security posture was assessed as providing a reasonable level of protection from breaches and disclosures of information from internal sources, with vulnerabilities remaining against attacks from external sources to agency ICT systems. In essence, agency processes and practices have not been sufficiently responsive to the ever-present and ever-changing risks that government systems are exposed to.

21. In the context of working towards compliance with the mandated requirements, it is important that agencies develop a timetable and process to guide implementation in the following key areas:

- deploy the top four mandated ISM controls across the entire ICT environment, to comply fully with Australian Government requirements;
- adhere to a security patch management strategy and deploy security patches in a timely manner, commensurate with assessed risk and using the Australian Signals Directorate's deployment timeframes for vulnerability and patch risk rating;
- restrict privileged user access accounts based on the level of sensitivity of the information; and strengthen access controls to capture and monitor the audit logs for unauthorised access to privileged accounts, and inappropriate activities by privileged users; and
- promote security awareness and accountability within the agency, recognising that security is a shared responsibility.

22. The growth in cyber attacks indicates that an agency's ICT security posture—in essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats—is increasingly a matter for senior management attention, including agencies' boards of management. Periodic assessment and review of an agency's overall ICT security posture by the agency security executive can provide additional assurance on an agency's resilience to cyber attacks.

23. The ANAO has made three recommendations aimed at improving the selected agencies' approaches to the protection and security of information which they manage. The recommendations are likely to have applicability to other Australian Government agencies.

Key findings

24. The selected agencies 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); observed compliance state as at 30 November 2013; and reported planned compliance state by 30 June 2014.

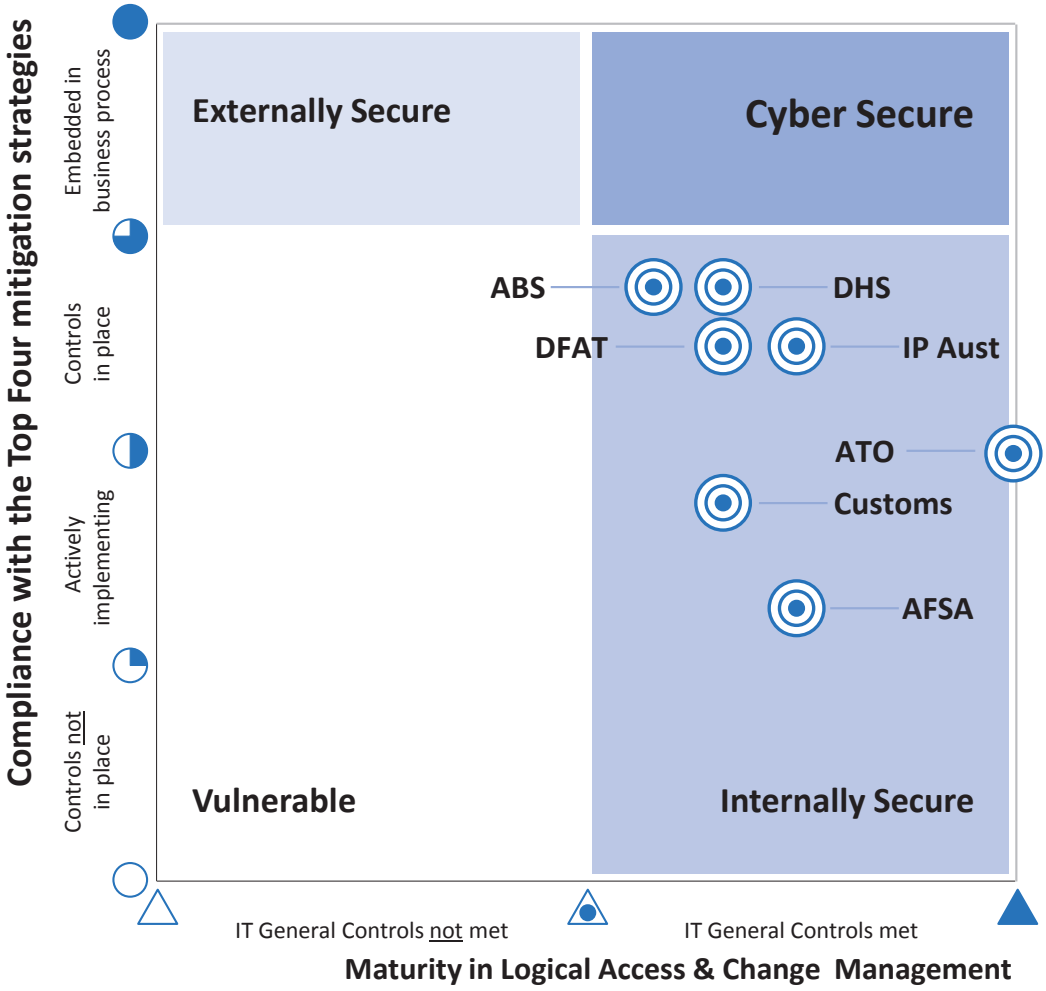
25. The ANAO's summary findings for each of the selected agencies are reported in the context of a matrix, which indicates agencies' overall level of protection against internal and external threats as a consequence of the steps taken to implement the top four strategies and IT general controls. The matrix, which is referred to as the *Agency Compliance Grade,* indicates where agencies are positioned in terms of ICT security zones: *vulnerable* zone; *externally* secure zone; *internally* secure zone, and *cyber secure* zone. The zones are explained further in Table S.2 and illustrated in Figure S.1. An agency's position indicates its overall ICT security posture—in essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

Table S.2: Definition of the ICT security zones

Zone scheme	Definition of the ICT security zones
Vulnerable Zone	High-level of exposure and opportunity for external attacks and internal breaches and disclosures of information
Externally Secure Zone	Reasonable level of protection from attacks and intrusions from external sources—but vulnerabilities remain to breaches and disclosures from internal sources
Internally Secure Zone	Reasonable level of protection from breaches and disclosures of information from internal sources—but vulnerabilities remain to attacks from external sources
Cyber Secure Zone	High-level of protection from external attacks and internal breaches and disclosures of information

Source: ANAO.

Figure S.1: Agency Compliance Grade: summary assessment of agencies' compliance with top four mandatory strategies and related controls, and overall ICT security posture



GRADING SCHEME:

- Controls not in place and no dispensation authorised by the Agency Head
- Controls not in place but a dispensation is authorised by the Agency Head
- Controls not in place but agency is actively implementing, with a minimum of design deliverables in evidence
- Controls in place across 80% or more of the agency
- Controls in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required
- Control objectives not met
- Identified controls not in place but compensating controls in place and observed
- Control objectives met
- Observed state at 30 Nov 2013

Source: ANAO. See Figure 2.3 for the agencies' planned state by 30 June 2014.

Note: IT General Controls are policies and procedures developed to deal with identified ICT system risks, including controls in relation to ICT governance, ICT infrastructure, security and access to operating systems and databases, and program change procedures.

26. In summary, each of the selected agencies was located in the *Internally Secure Zone*. The agencies had security controls in place to provide a reasonable level of protection from breaches and disclosures of information from internal sources. However, this is not sufficient protection against cyber attacks from external sources. To comply fully with the PSPF, agencies should also have a reasonable level of protection from external threats. The preferred state is for an agency to be located in the *Cyber Secure Zone*—where both ISM and IT general controls are effectively in place across the agency's enterprise systems, providing a high level of protection against all threats.

27. The selected agencies had not yet achieved full compliance with the PSPF and ISM, although each has advised of improvement activities underway.[16] Agencies further advised that factors affecting their current security posture and level of compliance with the four mandated strategies included: competing operational priorities[17]; resource restraints; and accessing specialist skills. In the context of working towards compliance with the mandated requirements, it is important that agencies develop a timetable and process to guide implementation.

Application whitelisting deployed on desktops and servers

28. Application whitelisting is a control which protects against unauthorised applications executing on a system. The ANAO observed that the deployment of application whitelisting across agency desktops was a priority activity for all agencies. Three of the seven agencies had implemented application whitelisting across the desktops, while one agency was also actively implementing application whitelisting across its servers.

29. The ANAO examined the application whitelisting rules used by each of the agencies—a set of protocols to identify executable files—and found that in most cases only simple rules were adopted.[18] The ANAO raised concerns when it observed, in the case of two agencies, that their application whitelisting was set to 'audit only mode', which simply logged events that application whitelisting would have blocked, had it been enabled. Both agencies immediately rectified this shortcoming. Of further concern, in the case of four

16 Figure 2.3 illustrates the selected agencies' observed compliance state at 30 November 2013, and the planned compliance state by 30 June 2014.

17 For example, ICT resources must be allocated to deliver a range of business outcomes.

18 Specifically, simple certificate and folder based rules were adopted.

agencies, was that the default policy was not set to deny the execution of software, potentially enabling staff without administration rights to load software on agency systems.

Policies and procedures for security patching of applications and operating systems

30. Security patching involves the periodic deployment of software releases designed to fix problems with existing software. The ANAO observed that while all agencies had implemented a patch management strategy, procedure or instruction that aligned with their change management procedures, these approaches were inadequate to cover the patching or upgrade of desktop and corporate applications to address known security vulnerabilities. More attention was given by agencies to the timely deployment of security patches to operating systems at the desktop and servers. All agencies had mitigating controls to prevent attacks or resolve issues to their systems where known vulnerabilities could not be patched.

31. In all cases, agencies were non-compliant with the requirements to apply critical security patches within two days from the release of the patches, and only two agencies had demonstrable patching practices enabling them to respond to vendors' routine or *ad hoc* patch releases, such as Microsoft's monthly security patch release. While there may be practical challenges to overcome in applying security patches within mandated timeframes, agencies will experience additional risk exposures the longer they delay implementation.

Management of standard and administrative privileged accounts

32. Administrative privileges are the highest level of permission, granted only to trusted personnel to enable them to configure, manage and monitor an ICT system. The ANAO reviewed agencies' group policies for account access, with attention given to the management of privileged accounts. For all agencies: administrative users held separate accounts to perform system administrative duties; were denied email accounts and Internet access; and privileged accounts were controlled and auditable. However, five of the selected agencies had shortcomings in processes used to capture and maintain audit logs for privileged user accounts, and there were also inconsistent practices across agencies in the administration of group policies.

33. Further, the ANAO's assessment of agency policies to capture and maintain audit logs for privileged user accounts, found that in most cases the policy was not enforced. This is a systemic control weakness that raises questions as to how effectively agencies can identify, respond to, or investigate unauthorised access to privileged user accounts, or inappropriate activities by privileged users.

IT general controls

34. The ANAO examined key components of the selected agencies' IT general controls, relating to logical security access and change management. The ANAO observed that the selected agencies, in general, had appropriate and effective access control and change management processes in place. An area for improvement that is relevant for most of the agencies is the access control requirements to the database layer.[19] While other layers of control compensate to varying degrees for weaknesses in this regard, this is an issue that requires early attention.

Agencies' planned improvement activities

35. The need for continuous disclosure and improvement are features of the Australian Government's protective security framework, with the PSPF requiring agencies to:

> Undertake an annual security assessment against the mandatory requirements detailed in the PSPF, and report their compliance with the mandatory requirements to the relevant portfolio Minister.[20]

36. Australian Government agencies are required to use the PSPF compliance reporting process to inform their portfolio Minister(s) and the Attorney-General—who is responsible for national protective security policy and privacy—of progress against mandatory PSPF requirements, and any rationale for non-compliance. The ASD's top four mitigation strategies were mandated with effect from 2013, and must therefore be reported on by agencies. The first of the agencies' self-assessment compliance reports to include an assessment against the mandatory requirements were due in September 2013. However, this did not mean that agencies were expected to

19 The database layer is where official information resides on an IT system.

20 In accordance with the guidance set out in the PSPF, this reporting should be incorporated with the compliance reporting against other PSPF requirements and should be sent to: the relevant portfolio Minister; the Secretary of the Attorney-General's Department; and the Auditor-General for Australia.

have successfully implemented the mandatory requirements by this time, and an 18 month implementation period was set.

37. The ANAO examined the self-assessment compliance reports, as submitted by each of the selected agencies. In all cases, agencies reported non-compliance for one or more of the mandatory requirements.

38. All agencies advised the ANAO of plans to implement further initiatives to strengthen security controls with a view to improving compliance with the PSPF and ISM. The ANAO assessed the selected agencies' plans to achieve compliance by 30 June 2014. Assessments were conducted for agency 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.

39. Each of the selected agencies has activities underway that if effectively and fully implemented, would strengthen ISM controls and enhance the level of protection of information and systems, by 30 June 2014. For six of the agencies, the strengthening of one or more of the ISM controls would improve their agency compliance grade. Notwithstanding the agency activities planned for implementation by 30 June 2014, and in the absence of further agency initiatives, all of the selected agencies are likely to remain in the *Internally Secure Zone* and not achieve full compliance with the mandatory ISM controls by 30 June 2014, the date specified by the Australian Government.

40. Where agencies are unable to comply fully with mandatory Government requirements within a specified timeframe, it is important that they develop a clear timetable and process to establish a path to compliance and guide implementation.

Strengthening agencies' ICT security posture

41. In the context of an evolving cyber threat environment, agencies must have cyber resilience, to enable them to continue providing services while also deterring and responding to external cyber attacks. A sound understanding of an agency's ICT security posture can provide senior management with assurance that effective security measures are implemented to reduce the risk posed by cyber attacks. While ICT operational staff retain day-to-day responsibility for setting and enforcing security policy and procedures across systems, governance arrangements commensurate with the threat, and informed by risk analysis, can provide additional assurance.

42. Security awareness and initiatives are a shared responsibility within an organisation. Well prepared agencies adopted a mutual obligation approach towards security awareness, responsibility and accountability; where key staff had a duty to monitor and report on observed cyber behaviour. Leading by example, senior managers in these agencies responded to cyber security incidents in a timely manner (reactive), and were informed of cyber trends—the motives, opportunities and emerging technology—that might target and compromise agency systems (proactive). To achieve this outcome, the relevant executives understood their roles and responsibilities to enhance security initiatives for the services they were accountable for, and tended not to expect ICT technical staff to be solely responsible for resolving ICT security matters.

43. Further, agencies which look beyond the four mandated strategies are better placed to manage threats and intrusions. Each of the selected agencies had taken varying steps to implement the remaining 31 controls from the *Top 35 mitigation strategies against cyber intrusions* promulgated by ASD.

Summary of agencies' responses

44. Agencies' summary responses to the audit report are provided below. Agency responses to each recommendation are included in the body of the report, directly following each recommendation. Formal responses from the agencies are included at Appendix 1.

Selected agencies' responses

Australian Bureau of Statistics

45. The ABS agrees that the report is an accurate assessment of the agency's compliance state as of 30 November 2013 and the agency's planned state for 30 June 2014.

46. The ABS supports the recommendations of the report and notes that the agency is well placed in terms of its compliance with the top four ISM controls.

47. The audit has identified some areas for improvement and the agency has established programs of work to implement these recommendations. Where full compliance has not been possible due to technical constraints imposed by a small number of legacy systems, mitigations have been put in place to reduce the risks associated with the use of these.

Australian Customs and Border Protection Service

48. The ACBPS believes your audit methodology and the resulting findings are fair and accurate based on the point-in-time of the field phase. The Service has and will continue to benefit from your contribution to our program of work and we look forward to the opportunity to engaging with your team and the other audit agencies to leverage each other's advancements.

49. The ACBPS is enhancing its security culture to address the growing cyber threat. Underpinned by clear policy, supported by security aware leadership the security team has a mandate to achieve compliance with the Australian Signals Directorate Top 35.

Australian Financial Security Authority

50. The Australian Financial Security Authority (AFSA) accepts the proposed report on *Cyber Attacks: Securing Agencies' ICT Systems,* and agrees with the Australian National Audit Office's assessment of agency systems. AFSA will continue in our efforts to achieve full compliance with the top four ASD strategies against potential cyber attacks.

51. AFSA acknowledges the importance of developing and implementing strategies and policies to strengthen the agency security posture. AFSA will continue to develop these strategies and policies in an informed manner so that we may achieve the optimal level of control over our systems to mitigate the risk of cyber attacks.

52. AFSA agrees with the recommendations contained in the report, and appreciates the recognition from the Australian National Audit Office relating to the works completed.

Australian Taxation Office

53. The Australian Taxation Office (ATO) welcomes the proposed audit report on *Cyber Attacks: Securing Agencies' ICT Systems,* and agrees with the Australian National Audit Office's overall assessment. The ATO remains committed to achieving full compliance with the top four mandated strategies against potential cyber-attacks.

54. The ATO will continue to develop and implement strong and robust strategies and policies to continually strengthen the security of ICT systems and achieve the desired level of control over our systems to mitigate the risk of cyber intrusions. The ATO agrees with the three recommendations contained

in the report. Overall, the ATO appreciates the recognition given for the work undertaken to date.

The Department of Foreign Affairs and Trade

55. The Department of Foreign Affairs and Trade (DFAT) has reviewed the proposed report on *Cyber Attacks: Securing Agencies' ICT Systems*, dated 12th May 2014. DFAT agrees with the Australian National Audit Office's key findings and is working towards capability improvements that will increase the level of protection from external attacks and internal breaches and disclosure of information.

56. DFAT will continue to improve compliance with the top four mitigation strategies and related mandatory controls to mitigate risks associated with cyber-attacks. Existing processes and security systems will be strengthened to protect the security of Australian Government information and systems. DFAT agrees with the three recommendations in the report and the value of the work performed in identifying areas for improvement.

The Department of Human Services

57. The Department of Human Services (the department) welcomes this report, and considers that the implementation of its recommendations will enhance our current work practices and our already strong compliance status.

58. The department takes its commitment to securing our organisation against cyber security attacks very seriously. The department will continue to strengthen the posture of compliance with the top four mandatory strategies, related controls and overall ICT security.

IP Australia

59. IP Australia welcomes this report and considers that implementation of the recommendations will enhance the security of its ICT systems. IP Australia agrees with the recommendations in the report and has in place a plan to further strengthen its capability in all these areas. An action plan to address compliance with the Top 4 Strategies is already underway and these recommendations will be added to that plan.

60. IP Australia has reviewed and is actively working to improve its security posture within a timeframe and resource envelope that can be managed based on its cost recovery model of operation. A risk based approach has been used to prioritise improvements to security and to ensure the highest vulnerabilities are addressed first. With its increase in online services, the

increasing threat environment, and the increase in compliance requirements, IP Australia has increased ICT Security resources and initiatives to improve its overall security posture.

Other agency responses

61. A copy of the proposed audit report was also provided to the Attorney-General's Department (AGD) and the Australian Signals Directorate (ASD) for any comments they wished to make. The AGD provided informal comment in the drafting of this report. ASD's response is set out below.

Australian Signals Directorate

62. The Australian Signals Directorate (ASD) endorses the three recommendations of the Australian National Audit Office cross-agency audit report on Cyber Attacks: Securing Agencies' ICT Systems. This audit report is important for the selected agencies and others to improve their ICT security.

63. Based on ASD's technical and operational experience in cyber security, the Top 4 remain the most effective way to mitigate targeted cyber intrusions when implemented as a package. No single strategy can prevent a targeted cyber intrusion, and ASD encourages all government agencies to continue to make inroads into the application of the Top 4. Once organisations have effectively implemented the Top 4 mitigation strategies, ASD recommends additional mitigation strategies be selected from the remaining 31 to address security gaps until an acceptable level of residual risk is reached.

Recommendations

The recommendations are based on findings from fieldwork at the selected agencies, and are likely to be relevant to other agencies. Therefore, all agencies are encouraged to assess the benefits of implementing these recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by practices already in place.

Recommendation No. 1

Paragraph 2.34

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

(b) complete activities in train to implement the top four ISM controls across their ICT environments; and

(c) 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*

Recommendation No. 2

Paragraph 4.63

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*

Recommendation No. 3

Paragraph 5.23

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 Findings

1. Background and Context

This chapter provides background information about the audit, including an overview of the Australian Government's framework for protecting its information and communications technology (ICT) assets against unauthorised and improper access and use.

Introduction

1.1 Governments, businesses and individuals increasingly rely on information and communications technology (ICT) in their day-to-day activities, with rapid advances continuing to be made in how people and organisations communicate, interact and transact business through ICT and the Internet. In the government sector, ICT is used to deliver services, store and process information, and enable communications, with a consequent need to protect the privacy, security and integrity of information maintained on government systems.

1.2 The *Australian Public Service Information and Communications Technology Strategy*[21] sets out the Government's direction for the use of ICT into the future. The Strategy builds on an expectation that government interaction with people, business and the community will occur seamlessly as part of everyday life. It outlines how agencies will continue to use ICT to drive better service delivery, improve government operations, drive productivity, and engage with people, the community and business. The Strategy statement is:

> The Australian Public Service will use ICT to increase public sector and national productivity by enabling the delivery of better government services for the Australian people, communities and business, improving the efficiency of APS operations and supporting open engagement to better inform decisions.[22]

1.3 Advances in ICT and their accessibility to individuals, organised syndicates and sovereign states, mean that Australian ICT networks are facing an unprecedented level of intrusion activities. Targeted cyber intrusions are

21 Led by the Australian Government Information Management Office (AGIMO) within the Department of Finance.

22 *Australian Public Service Information and Communications Technology Strategy 2012–2015*, p. 5.

the highest threat to government ICT systems, according to the *Australian Government Cyber Security Strategy*[23], with evidence that:

> In 2011–12, there were more than 400 cyber incidents against government systems requiring a significant response by the Cyber Security Operations Centre.
>
> In 2012, 5.4 million Australians were victims of cyber crime with an estimated cost to the economy of $1.65 billion.[24]

1.4 The rapid escalation, persistence and sophistication of cyber attacks against government, business and the wider community has been widely reported. In the past two years, there were several public disclosures of cyber intrusions to high profile Australian government entities, banks and corporations. The Australian Bureau of Statistics (ABS) has been the target of a series of sustained online attacks aimed at gathering access to market-sensitive information before its public release[25], and the media has also reported on cyber intrusions targeting the Reserve Bank of Australia, the Department of Finance, and the NBN Co.[26]

1.5 The fundamental concern is that the threats facing business and government are increasing at a rate faster than the deployment of defences in response.[27] The motives and capability of relevant 'actors'—be they individual hackers, crime syndicates, or sovereign states—varies, but research undertaken by IBM and Gartner indicates that actors are increasingly using advanced technologies to conduct targeted cyber attacks.[28]

1.6 External attacks on ICT systems are part of an international trend. Globally, organisations in the government sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 72.2 emails blocked as malicious in 2012, compared with 1 in 41.1 for 2011; while targeted cyber attacks increased from 77 per day in 2010 to 116 per day in 2013.[29]

---

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

24 J Gillard, (Prime Minister), 'Australian Cyber Security Centre', media release, Parliament, Canberra, 24 January 2013.

25 The ABS has been the subject of numerous attacks over the past four years, including at least 11 incidents over seven months during 2012. C Joye, 'Cyber attacks hit statistics bureau', *The Australian Financial Review,* 26 April 2013, p. 1.

26 J Kerin, 'Smith to raise cyber menace in US talks', *The Australia Financial Review*, 20 May 2013, p. 10.

27 McPhee, *Cyber Security: Country Paper–Australia,* Proceedings of the 14th Annual Global Working Group Meeting of Auditors-General, Tokyo, Japan, 2013.

28 ibid., p. 2.

29 Symantec, *Internet Security Threat Report*, 2013, p. 14.

1.7 The Attorney-General's Department has summarised the Australian Government's concerns as follows:

> With the rapid escalation in the intensity and sophistication of cyber crime and other cyber security threats, it is imperative that government, business and the community are aware of the severity of cyber security risks, and commit to work together to protect what has become a vital component of our economy and society.[30]

1.8 The protection of Australian Government systems and information from unauthorised access and use is a key responsibility of agencies, having regard to their business operations and specific risks. In the context of a national government, those risks can range from threats to national security through to the disclosure of sensitive personal information. Unauthorised access through electronic means, also known as cyber intrusions, can result from the actions of outside individuals or organisations. Individuals operating from within government may also misuse information which they are authorised to access, or may inappropriately access and use government information holdings.

1.9 Since 2010, the Australian Government has established both an overarching protective security policy framework, and promulgated specific ICT risk mitigation strategies and related controls to inform the ICT security posture of agencies. 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.

The protective security framework

1.10 The Attorney-General's Department (AGD) is responsible for administering the Australian Government's protective security policy, which has as its objective to promote the most effective and efficient ways to secure the continued delivery of Government business. AGD's *Protective Security Policy Framework* (PSPF)[31] outlines the core requirements for the effective use of

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

31 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.

protective security as a business enabler. To facilitate government working confidently and securely, the PSPF assists agencies[32] to:

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

1.11 The PSPF applies across personnel, information and physical security, and sets out governance arrangements relating to how an agency uses protective security to ensure it meets the relevant policy, protocols and guidelines. The PSPF is intended to contribute to overall government performance through the secure delivery of goods, services or programs, as well as ensuring the confidentiality, integrity and availability[33] of its people, information and assets.

1.12 The PSPF is supported by the *Australian Government Information Security Manual* (ISM)[34], which is released by Australian Signals Directorate (ASD)[35], and is the standard governing the security of government ICT systems. The ISM is intended to assist agencies in applying a risk-based approach to protecting their information and systems. According to ASD:

> Advances in ICT are allowing for greater accessibility, mobility, convenience, efficiency and productivity across almost all aspects of Australian life. Australia's national security, economic prosperity and social wellbeing now depend on ICT, and the Internet in particular. The security of sensitive government and commercial information, the security of our digital

---

32 As a policy of the Australian Government, agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act) must apply the Protective Security Policy to the extent that their enabling legislation allows. See the *Protective Security Policy Framework,* p. 9.

33 The *Protective Security Policy Framework* defines: *confidentiality* to ensure that information is accessible only to those authorised to have access; *integrity* to ensure the safeguarding, accuracy and completeness of information and processing methods; and *availability* to ensure that authorized users have access to information and associated assets when required.

34 The Australian Signals Directorate (ASD) produces the ISM, which is the standard governing the security of government ICT systems. The ISM complements the PSPF, and is an important part of the Australian Government's strategy to enhance its information security capability.

35 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. Defence Signals Directorate, *Australian Government Information Security Manual*, *Controls,* 2013, p. 2. The Directorate was re-named the Australian Signals Directorate in 2013.

infrastructure, and public and international confidence in Australia as a safe place to do business online are critical to our future.[36]

1.13 According to ASD, while there are other (international) standards and guidelines designed to protect information systems, the advice provided in the ISM is specifically based on activity observed by ASD on Australian government networks.[37]

1.14 ASD advises agencies to make informed, risk-based decisions specific to their unique environments, circumstances and risk-appetite—encouraging agencies to employ mitigation strategies identified and detailed in the ISM, and supported by a set of detailed controls[38] that can be applied to an agency's information and systems.

1.15 There are two categories of compliance associated with the controls in the ISM—'must' and 'should'. These compliance requirements are determined according to the degree of security risk an agency will be accepting by not implementing the associated ISM controls. The ASD has advised agencies that non-compliance with:

(a) 'must' controls is likely to represent a high security risk to agency information and systems—therefore the agency head *is required to consider* the justification for non-compliance and accept the associated security risk; and

(b) 'should' controls is likely to represent a medium-to-low security risk to agency information and systems—therefore the agency head or delegate *can consider* the justification for non-compliance and accept the associated security risk.[39]

1.16 While the majority of ISM controls can be risk managed within an agency, the compliance requirements provide an indication of the appropriate level where any residual security risk must be accepted by the agency for a given control. Whether an agency is compliant or non-compliant against the ISM, the accountability and responsibility for implementing and managing

36 ibid., *Executive Companion 2012*, p. 2.

37 ibid., p. 14.

38 A control is defined in the ISM as procedures with associated compliance requirements for mitigating security risks to an agency's information and systems. Ibid., *Controls*, 2013, p. 4.

39 ibid., p. 15.

security risks associated with the agency's information and systems resides with the agency head.

1.17 Agency head responsibilities were highlighted in the April 2013 amendment to the PSPF, which now requires agencies to submit annual reports to the Attorney-General on their compliance with the ISM. Further, the PSPF mandated, from January 2013, the top four mitigation strategies discussed at paragraph 1.19. The requirement to implement mandated strategies had immediate effect, and agencies were expected to be fully compliant by 30 June 2014. The information security directive (INFOSEC 4) states:

> Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the *Australian Government Information Security Manual*.[40]

Preventing cyber intrusions to systems

1.18 Since February 2010, ASD has also published a list of strategies to mitigate targeted cyber intrusions. The list is revised annually based on ASD's most recent analysis of incidents reported across Australian agencies, and currently includes 35 strategies—with a particular focus on the top four mitigation strategies. According to ASD:

> While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 strategies [from the list] remains very high. At least 85% of the intrusions that ASD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.[41]

---

40 Attorney-General's Department, *Protective Security Policy Framework, Operational security management* [Internet], available from <http://www.protectivesecurity.gov.au/informationsecurity/Pages/default.aspx> [accessed 22 May 2013]

41 Defence Signals Directorate, *Strategies to Mitigate Targeted Cyber Intrusion* [Internet], 2012, available from <http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm>[accessed 27 February 2013].

1.19 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 executed[42];
- patching applications: applying patches to applications and devices to ensure the security of systems[43];
- patching operating systems: deploying critical security patching to operating systems to mitigate extreme 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.[44]

1.20 As discussed, an amendment to the PSPF issued in April 2013, had the effect of: mandating the top four mitigation strategies; and setting a target date of July 2014 for full implementation of the top four strategies. Effective implementation of the mandated strategies assists agencies in achieving control over their ICT systems, providing a higher level of assurance that systems will continue to support the day-to-day business services of the agency.

---

42 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.

43 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.

44 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.

Other developments

1.21 The then Prime Minister announced the Government's plans for an Australian Cyber Security Centre (ACSC)[45] in January 2013, in response to heightened cyber threats against Australian Government agencies' information and systems, at home and overseas. In support of *Australia's National Security Strategy*, the Centre is intended to assess and respond in a more agile way to cyber issues identified as key risks to Australia's security.

1.22 The *2013 Defence White Paper*, released on 3 May 2013, states that cyber security continues to be a serious and pressing national security challenge[46] and is a strategic focus of defence strategy for the next 20 years.

Audit coverage

1.23 The audit is part of a program of cross-agency performance audits which have examined processes supporting the delivery of services by Government agencies. Since 2000 the ANAO has undertaken 12 cross-agency audits on protective security arrangements. In each of these audit reports the ANAO has encouraged all Government agencies to assess the benefits of the recommendations in light of their own circumstances and practices.

1.24 The ANAO's most recent performance audits of Australian Government agencies' protective security arrangements are:

- ANAO Audit Report No.33 2010–11, *The Protection and Security of Electronic Information Held by Australian Government Agencies*, tabled in March 2011. This audit focused on the effectiveness of Australian Government agencies' management and implementation of measures to protect and secure their electronic information in accordance with Australian Government protective security requirements. The ANAO made four recommendations, which were agreed by the four selected agencies.

---

45 ACSC will bring together cyber security capabilities from across the national security community in one facility. Co-located in the Centre will be the Australian Signals Directorate Cyber Security Branch, the Attorney-General's Department's Computer Emergency Response Team Australia, the Australian Security Intelligence Organisation's Cyber Espionage Branch, elements from the Australian Federal Police's High-Tech Crime Operations capability, and analysts from the Australian Crime Commission. Prime Minister of Australia, Press Office, *Australian Cyber Security Centre* [Internet], available from <http://www.pm.gov.au/press-office/australian-cyber-security-centre> [accessed 12 June 2013].

46 Department of Defence, *2013 Defence White Paper*, Canberra, 2013, s. 2.82, p. 20.

- ANAO Audit Report No.18 2011–12, *Information and Communications Technology Security: Management of Portable Storage Devices*, tabled in December 2011. This audit focused on the effectiveness of the management of risks arising from the use of portable storage devices in selected Australian Government agencies. The ANAO made five recommendations, which were agreed by the three selected agencies.

1.25 The ANAO's annual financial statement audits for FMA Act agencies may assess the controls listed in the ISM as part of the IT general controls[47] review, as reported in the interim phase and final *Financial Statement Audit Report*, and may have informed findings in the current audit relating to an agency. However, the ANAO has not previously conducted a compliance audit against all or parts of the controls listed in the ISM.

Selected agencies in this audit

1.26 Seven agencies were selected by the ANAO to be included in this performance audit:

- Australian Bureau of Statistics (ABS)[48];
- Australian Customs and Border Protection Service (Customs)[49];
- Australian Financial Security Authority (AFSA)[50];
- Australian Taxation Office (ATO)[51];
- Department of Foreign Affairs and Trade (DFAT)[52];
- Department of Human Services (DHS)[53]; and
- IP Australia.[54]

---

47 The *Australian Auditing Standards* (ASAs) define IT general controls (ITGC) as policies and procedures that relate to many applications and support the effective functioning of application controls.
Institute of Chartered Accountants Australia, *Auditing, Assurance and Ethics Handbook 2014,* John Wiley & Sons Australia, Queensland, 2014, A. 104, p. 324.

48 ABS is a prescribed agency in the Treasury Portfolio.

49 Customs is a prescribed agency in the Immigration and Border Protection Portfolio.

50 AFSA is a prescribed agency in the Attorney-General's Portfolio—it administers and regulates the personal insolvency system, trustee services and the administration of the Personal Property Securities Register (PPSR) and proceeds of crime.

51 ATO is a prescribed agency in the Treasury Portfolio.

52 DFAT is a Department of State.

53 DHS is a Department of State.

1.27 These agencies were selected based on the character and sensitivity of the information primarily managed by the agency. Table 1.1 outlines the type of information held by each agency in the following categories: economic, policy and regulatory, national security, program and service delivery, and personal information.[55]

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

Australian Government agency	Economic information	Policy and regulatory information	National security information	Program and service delivery	Personal information
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				✓	✓
IP Australia		✓		✓	

Source: ANAO analysis.

Audit objectives, criteria and approach

Objectives

1.28 The audit objective was to assess selected agencies' compliance with the four mandatory ICT security strategies and related controls in the *Australian Government Information Security Manual* (ISM). The audit also considered the overall ICT security posture of the selected agencies, based on their

54 IP Australia is a prescribed agency in the Industry Portfolio—it administers intellectual property (IP) rights and legislation relating to patents, trademarks, designs and plant breeder's rights.

55 The *Privacy Act 1988* regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information.

implementation of the four mandated mitigation strategies and IT general controls.

Criteria

1.29 The ANAO examined agency-level implementation of the 'Top Four' mitigation strategies and related controls mandated in the ISM. The audit also assessed whether the selected agencies had accurately stated their compliance against the ISM controls in their self-assessment compliance reports to the Attorney-General's Department, against the protective security governance guidelines on compliance reporting.[56]

1.30 The audit also considered the selected agencies' overall ICT security posture, having regard to agencies' implementation of IT general controls[57] and the top four mitigation strategies and related controls. The audit did not consider the PSPF mandatory requirements relating to physical security. A recent ANAO performance audit examined the application of physical security requirements by three Australian Government agencies.[58]

1.31 Table A.1 in Appendix 2 outlines the criterion and compliance statements used to assess whether the agencies were fully implementing the mandatory mitigation strategies and related controls.

1.32 Table A.2 in Appendix 2 outlines the criteria and compliance statements used to assess whether the agencies were fully implementing the IT general controls across their systems, and whether dispensations were in place for non-compliant controls.

---

56 The guidelines contain the underlying principles and outline the responsibilities that agencies are required to follow when measuring their compliance against the PSPF mandatory requirements. Attorney-General's Department, *Protective security governance guidelines–Compliance reporting* [Internet], 2012, available from <http://www.protectivesecurity.gov.au/governance/audit-reviews-and-reporting/Pages/Supporting-guidelines-for-audit-reviews-and-reporting.aspx> [accessed 17 June 2013].

57 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.

58 ANAO Audit Report No.49 2013–14, *The Management of Physical Security.*

Approach

1.33 The ANAO examined agency-level implementation of the mandatory ISM strategies and related controls across the enterprise ICT systems—with a focus on the agency's ICT governance to support compliance against these controls and IT general controls. In particular the audit:

- reviewed each agency's (self-assessment) compliance reporting, against the *Protective security governance guidelines*[59]—a written advice from the agency head to the relevant portfolio Minister containing a declaration of compliance with the 33 mandatory requirements of the PSPF;
- interviewed key ICT security personnel for each agency, 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);
- reviewed the work of the agency's internal audit function on compliance with the ISM;
- examined each agency's user access controls that support standard and administrative privileged accounts;
- examined each agency's change management processes that support the authorisation of critical patching of applications and operating systems; and
- consulted with ASD staff.

1.34 To support the development of test protocols against the mandatory ISM strategies and related controls, the audit referenced international policy and practices that informed the PSPF, ISM and the *Top 35 strategies to mitigate targeted cyber intrusions*, such as the National Security Agency's *Critical controls for effective cyber defense*[60] and the National Institute of Standards and

59 Attorney-General's Department, *Protective security governance guidelines—Compliance reporting,* Canberra, 2011.

60 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.

Technology's *Security and privacy controls for federal information systems and organisations*.[61]

1.35 The audit fieldwork was conducted between August and November 2013.

Reporting on audit findings

1.36 In this audit, the ANAO departed from its usual practice of identifying agencies on individual issues due to the risk of disclosing sensitive information about agency ICT systems. In addition, security weaknesses are only addressed at an aggregate level. However, a summary assessment of each agency's performance against the audit objective is provided in Figure 2.2.

Auditing standards and cost

1.37 The audit was conducted in accordance with the ANAO's auditing standards, at a cost to the ANAO of approximately $625 000.

Structure of the report

1.38 The structure of the report is as follows:

- Chapter two provides an overall assessment of agencies' compliance, taking into account their implementation of the four mandatory ISM strategies and related controls, and overall ICT security posture based on their implementation of the mandated strategies and IT general controls;
- Chapter three examines in more detail the selected agencies' compliance with the four mandatory ISM strategies and related controls that protect ICT systems;
- Chapter four examines the selected agencies' IT general controls for logical access and change management that mitigate against internal breaches and disclosures of information; and
- Chapter five considers how agencies can strengthen their overall ICT security posture and improve levels of cyber resilience.

61 NIST Special Publication 800–39 revision 4 provides guidance on managing information security risk.

2. Agency Compliance

This chapter provides an overall assessment of agencies' compliance, taking into account their implementation of the four mandatory ISM strategies and related controls, and overall ICT security posture based on their implementation of the mandated strategies and IT general controls.

Introduction

2.1 The *Australian Government Protective Security Policy* mandates that agencies adopt a risk management approach to protective security. To guide agencies' implementation of ICT security arrangements, the *Australian Government Information Security Manual* (ISM) sets out better practice to help mitigate or minimise the threat to agencies' ICT systems. Mindful that there is no one-size-fits-all model for information security, the ISM is intended as a tool to assist agencies risk-manage the protection of information and systems through the deployment of security controls.

2.2 To take advantage of an expanding set of security controls, and to give agencies greater flexibility and agility to defend their systems, the advice in the ISM is platform non-specific.

2.3 While agencies have discretion to comply with the ISM requirements where appropriate—in accordance with their business needs, threat environment and risk appetite—there are specified ISM strategies and related controls for which compliance is mandatory, as stipulated by the PSPF. These mandatory controls form part of a layered defence primarily designed to protect workstations that are able to receive emails or browse web content originating from a different security domain, particularly from the Internet.

2.4 The ANAO examined agency-level implementation of the four mandatory strategies and related controls across their enterprise ICT systems, and the underpinning IT general controls that support ICT security for logical access and change management. The ANAO assessed compliance at 30 November 2013, and also examined whether initiatives underway position agencies to comply fully with the mandatory controls by 30 June 2014.

Assessing compliance

2.5 In order to access compliance in a consistent manner across the seven selected agencies, the ANAO applied a set of assessment criteria and developed a graphical key[62]; a reporting convention similar to a 'traffic light' report, as outlined in Table 2.1.

Table 2.1: Key to grading scheme for assessing compliance with the mandatory ISM strategies and related controls, and for the IT general controls

Grading scheme for mandatory ISM controls		Grading scheme for IT general controls	
○	Controls not in place and no dispensation authorised by the Agency Head.	△	Control objectives not met.
◔	Controls not in place but a dispensation is authorised by the Agency Head.	◬	Identified controls not in place but compensating controls in place and observed.
◑	Controls not in place but agency is actively implementing, with a minimum of design deliverables in evidence.	▲	Control objectives met.
◕	Controls in place across 80% or more of the agency.	**Agency Compliance Grade**	
●	Controls in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required.	◉	Observed state at 30 Nov. 2013.
		◎	Planned state by 30 June 2014.

Source: ANAO.

2.6 The selected agencies were assessed on their:

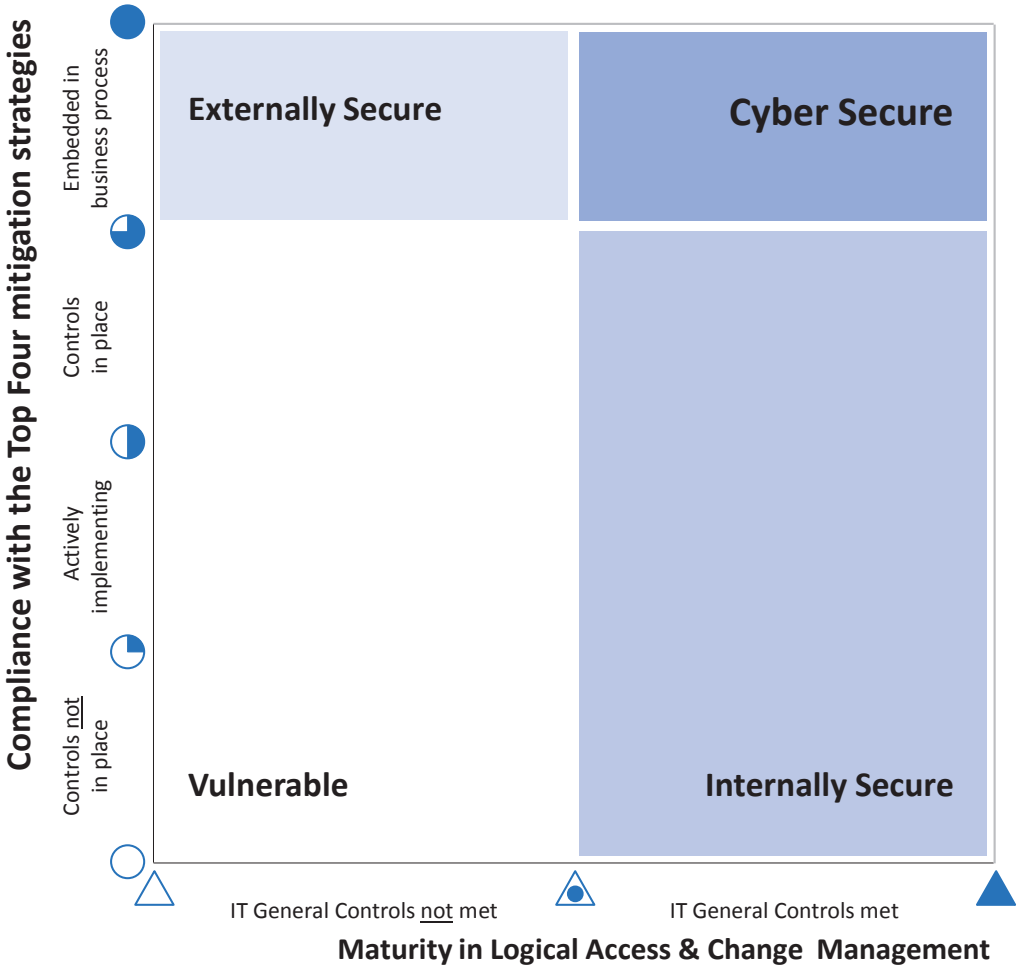
- compliance with the top four mitigation strategies and related controls;
- maturity to effectively manage logical access and change management as part of normal business processes (IT general controls); and
- observed compliance state as at 30 November 2013; and reported planned compliance state by 30 June 2014.

2.7 The ANAO's summary findings for each of the selected agencies are reported in the context of a matrix, shown in Figure 2.1, which indicates agencies' overall level of protection against internal and external threats as a

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

consequence of steps taken to implement the top four strategies and IT general controls. The matrix, which is referred to as the *Agency Compliance Grade,* indicates where agencies are positioned in terms of ICT security zones: *vulnerable* zone; *externally* secure zone; *internally* secure zone, and *cyber secure* zone.

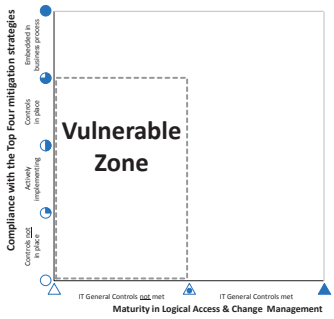
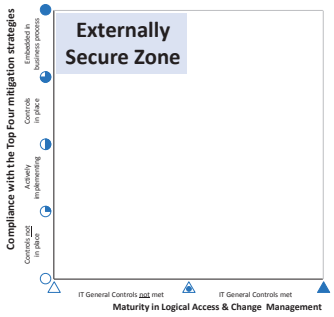
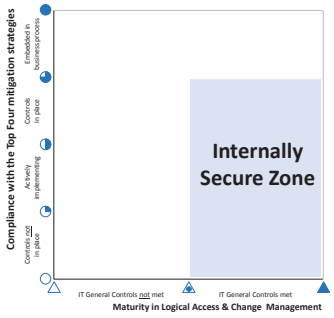
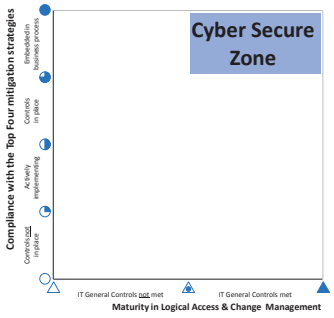
Figure 2.1: Reporting on level of security obtained by implementing the mandatory ISM strategies and IT general controls



Source: ANAO.

2.8 The zones are explained further in Table 2.2 and illustrated in Figure 2.2. An agency's position indicates its overall ICT security posture—in essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

Table 2.2: Definition of the ICT security zones

Zone scheme	Location of the ICT secure zones in the *Agency Compliance Grade*
Vulnerable Zone High-level of exposure and opportunity for external attacks and internal breaches and disclosures of information. • Systemic weakness across the ICT environment relating to protection of information and systems from external attacks and internal breaches and disclosures. • ISM and IT general controls not in place, or inconsistently implemented across the system.	
Externally Secure Zone Reasonable level of protection from attacks and intrusions from external sources—but vulnerabilities remain to breaches and disclosures from internal sources. • Top Four ISM strategies and related controls in place across 80% or more of the agency's ICT systems and are embedded in (or working towards) business processes.	
Internally Secure Zone Reasonable level of protection from breaches and disclosures of information from internal sources—but vulnerabilities remain to attacks from external sources. • IT general controls for logical access and change management are met by the agency.	
Cyber Secure Zone High-level of protection from external attacks and internal breaches and disclosures of information. • Top Four ISM strategies and related controls in place across 80% or more of the agency's ICT systems and IT general controls for logical access and change management are met by the agency.	

Source: ANAO.

Agency compliance grades – summary assessment

2.9 Under the PSPF, agencies must implement the top four mitigation strategies and related controls—application whitelisting, patching of applications and operating systems, and minimise administrative privileges—to satisfy INFOSEC 4. INFOSEC 4 is a key PSPF requirement which states that agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently.

2.10 Based on the PSPF and ISM requirements, the ANAO anticipated that agencies would have the following security controls across their systems:

(a) application whitelisting deployed on desktops and servers;

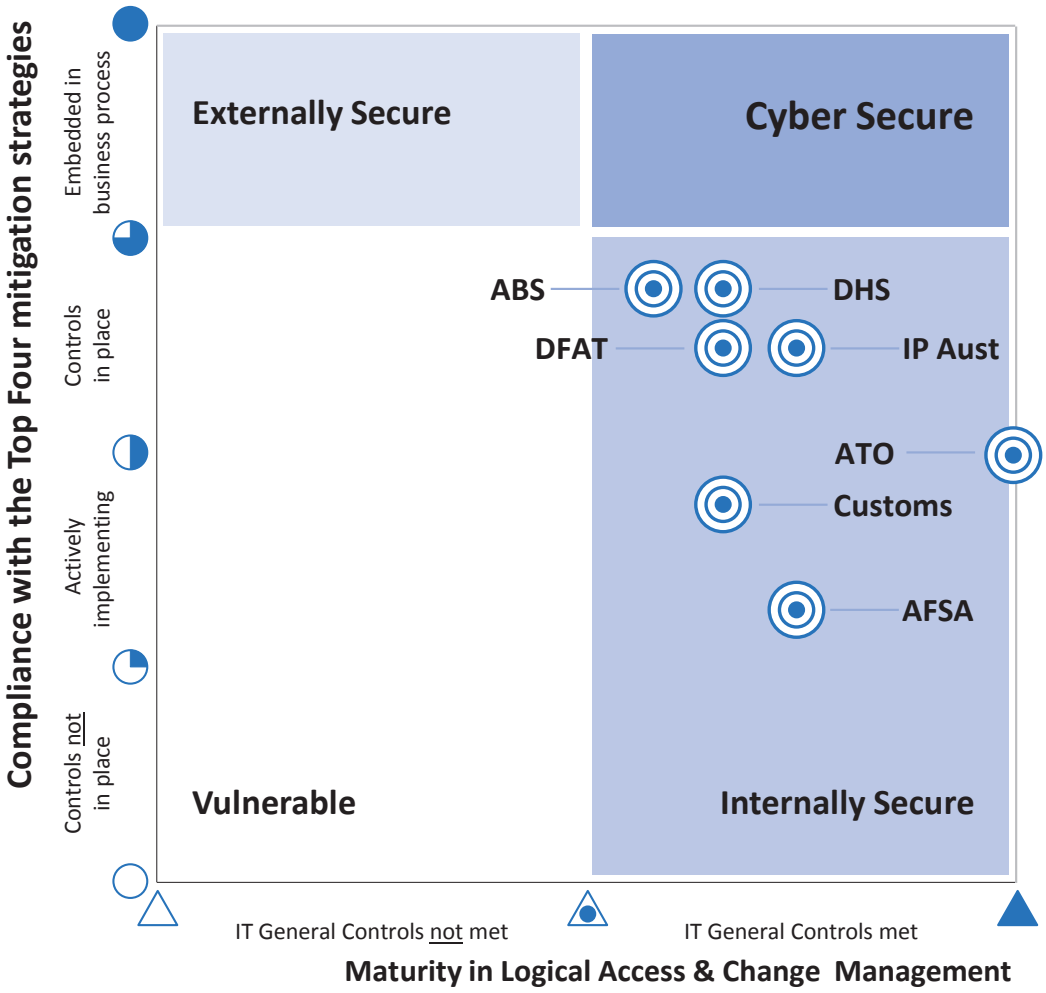
(b) policy and procedures for the security patching of applications and operating systems, supported by a change management process that supports the authorisation of critical patching; and

(c) 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.

2.11 The ANAO conducted interviews, reviewed documented policy and procedures, examined application whitelisting rules, assessed patching strategies against vendor-release threat assessments, and assessed user access and group policy accounts—and found varying states of compliance with the ISM.

2.12 Figure 2.2 summarises individual and comparative agency compliance with the ISM, based on *Agency Compliance Grades*, as at 30 November 2013.

Figure 2.2: Agency Compliance Grade: summary assessment of agencies' compliance with top four mandatory strategies and related controls, and overall ICT security posture



GRADING SCHEME:

- Controls not in place and no dispensation authorised by the Agency Head
- Controls not in place but a dispensation is authorised by the Agency Head
- Controls not in place but agency is actively implementing, with a minimum of design deliverables in evidence
- Controls in place across 80% or more of the agency
- Controls in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required
- Control objectives not met
- Identified controls not in place but compensating controls in place and observed
- Control objectives met
- Observed state at 30 Nov 2013

Source: ANAO. See Figure 2.3 for the agencies' planned state by 30 June 2014.

Note: IT General Controls are policies and procedures developed to deal with identified ICT system risks, including controls in relation to ICT governance, ICT infrastructure, security and access to operating systems and databases, and program change procedures.

Security threat zones

2.13 In summary, each of the selected agencies was located in the *Internally Secure Zone*. The agencies had security controls in place to provide a reasonable level of protection from breaches and disclosures of information from internal sources. However, this is not sufficient protection against cyber attacks from external sources. To comply fully with the PSPF, agencies should also have a reasonable level of protection from external threats. The preferred state is for an agency to be located in the *Cyber Secure Zone*—where both ISM and IT general controls are effectively in place across the agency's enterprise systems, providing a high level of protection against all threats.

2.14 The selected agencies had not yet achieved full compliance with the PSPF and ISM, although each has advised of improvement activities underway.[63] Agencies further advised that factors affecting their current security posture and level of compliance with the four mandated strategies included: competing operational priorities[64]; resource restraints; and accessing specialist skills. In the context of working towards compliance with the mandated requirements, it is important that agencies develop a timetable and process to guide implementation.

2.15 Agency compliance is discussed in more detail in the following paragraphs.

Assessment of agency compliance

Application whitelisting deployed on desktops and servers

2.16 Application whitelisting is a control which protects against unauthorised applications executing on a system. The ANAO observed that the deployment of application whitelisting across agency desktops was a priority activity for all agencies. Three of the seven agencies had implemented application whitelisting across the desktops, while one agency was also actively implementing application whitelisting across its servers.

---

63 Figure 2.3 illustrates the selected agencies' observed compliance state at 30 November 2013, and the planned compliance state by 30 June 2014.

64 For example, ICT resources must be allocated to deliver a range of business outcomes.

2.17 The ANAO examined the application whitelisting rules used by each of the agencies—a set of protocols to identify executable files—and found that in most cases only simple rules were adopted. The ANAO raised concerns when it observed, in the case of two agencies, that their application whitelisting was set to 'audit only mode', which simply logged events that application whitelisting would have blocked, had it been enabled. Both agencies immediately rectified this shortcoming. Of further concern, in the case of four agencies, was that the default policy was not set to deny the execution of software, potentially enabling staff without administration rights to load software on agency systems.

Policies and procedures for security patching of applications and operating systems

2.18 Security patching involves the periodic deployment of software releases designed to fix problems with existing software. The ANAO observed that while all agencies had implemented a patch management strategy, procedure or instruction that aligned with their change management procedures, these approaches were inadequate to cover the patching or upgrade of desktop and corporate applications to address known security vulnerabilities. More attention was given by agencies to the timely deployment of security patches to operating systems at the desktop and servers. All agencies had mitigating controls to prevent attacks or resolve issues to their systems where known vulnerabilities could not be patched.

2.19 In all cases, agencies were non-compliant with the requirements to apply critical security patches within two days from the release of the patches, and only two agencies had demonstrable patching practices enabling them to respond to vendors' routine or *ad hoc* patch releases, such as Microsoft's monthly security patch release. While there may be practical challenges to overcome in applying security patches within mandated timeframes, agencies will experience additional risk exposures the longer they delay implementation.

Management of standard and administrative privileged accounts

2.20 Administrative privileges are the highest level of permission, granted only to trusted personnel to enable them to configure, manage and monitor an ICT system. The ANAO reviewed agencies' group policies for account access, with attention given to the management of privileged accounts. For all agencies: administrative users held separate accounts to perform system administrative duties; were denied email accounts and Internet access; and

privileged accounts were controlled and auditable. However, five of the selected agencies had shortcomings in processes used to capture and maintain audit logs for privileged user accounts, and there were also inconsistent practices across agencies in the administration of group policies.

IT general controls

2.21 The ANAO examined key components of the selected agencies' IT general controls, relating to logical security access and change management. The ANAO observed that the selected agencies, in general, had appropriate and effective access control and change management processes in place. An area for improvement that is relevant for most of the agencies is the access control requirements to the database layer. While other layers of control compensate to varying degrees for weaknesses in this regard, this is an issue that requires early attention.

2.22 The audit findings are discussed further in Chapters Three and Four.

Agencies' planned improvement activities

2.23 The need for continuous disclosure and improvement are features of the Australian Government's protective security framework, with the PSPF Mandatory Requirement GOV–7 requiring agencies to:

> Undertake an annual security assessment against the mandatory requirements detailed in the PSPF, and report their compliance with the mandatory requirements to the relevant portfolio Minister.[65]

2.24 Australian Government agencies are required to use the PSPF compliance reporting process to inform their portfolio Minister(s) and the Attorney-General—who is responsible for national protective security policy and privacy—of progress against mandatory PSPF requirements, and any rationale for non-compliance. The ASD's top four mitigation strategies were mandated with effect from 2013, and must therefore be reported on by agencies. The first of the agencies' self-assessment compliance reports to include an assessment against the mandatory requirements were due in September 2013. However, this did not mean that agencies were expected to

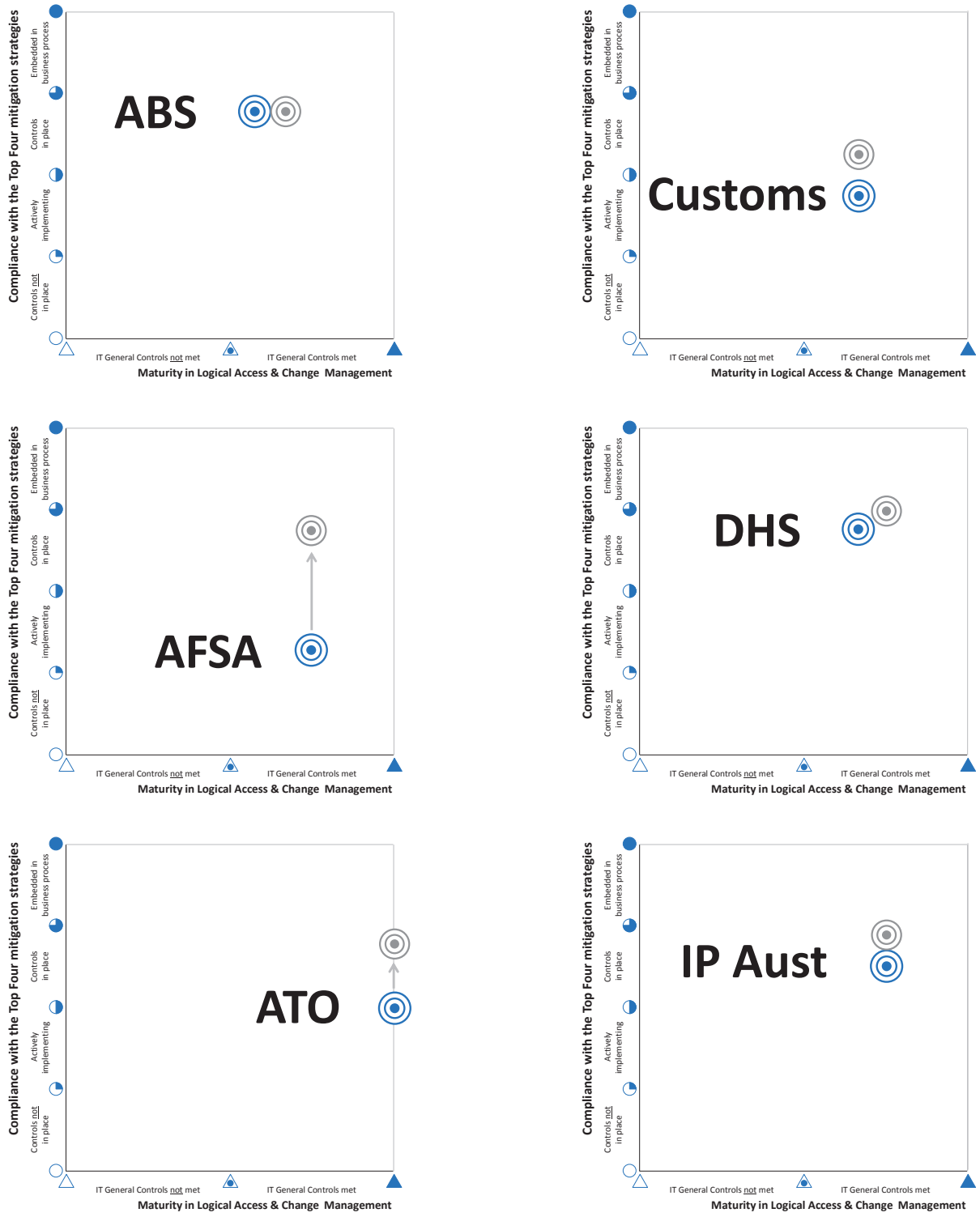
65 In accordance with the guidance set out in the PSPF, this reporting should be incorporated with the compliance reporting against other PSPF requirements and should be sent to: the relevant portfolio Minister; the Secretary of the Attorney-General's Department; and the Auditor-General for Australia.

have successfully implemented the mandatory requirements by this time, and an 18 month implementation period was set.

2.25 The ANAO examined the self-assessment compliance reports, as submitted by each of the selected agencies. In all cases, agencies reported non-compliance for one or more of the mandatory requirements. Five of the seven agencies reported their compliance against each specific control in a narrative statement and/or 'traffic light' report, while two of the agencies made general statements of compliance against the information security requirements (INFOSECs) in the PSPF.

2.26 Agencies also advised the ANAO of plans to implement further initiatives to strengthen security controls with a view to improving compliance with the PSPF and ISM. Figure 2.3 illustrates each *Agency Compliance Grade* in two states: observed compliance with the mandatory strategies and related controls as at 30 November 2013; and the planned state by 30 June 2014. DFAT is not included in the figure as it advised the ANAO that it expects no significant changes to its systems that will alter the department's planned compliance state.

Figure 2.3: Agencies' observed compliance grade and planned state



Source: ANAO analysis. DFAT has initiatives to strengthen the ISM and IT general controls but no significant activities underway that will alter its planned compliance state.

Legend: Observed state at 30 November 2013; Planned state at 30 June 2014.

2.27 The ANAO assessed the selected agencies' plans to achieve compliance by 30 June 2014. Assessments were conducted for agency 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. If effectively and fully implemented, the activities underway would strengthen ISM controls and enhance the level of protection of information and systems, by 30 June 2014. For six of the agencies, the strengthening of one or more of the ISM controls would improve their agency compliance grade.

2.28 Notwithstanding the agency activities planned for implementation by 30 June 2014, and in the absence of further agency initiatives, all of the selected agencies are likely to remain in the *Internally Secure Zone* and not achieve full compliance with the mandatory ISM controls by 30 June 2014, the date specified by the Australian Government. Where agencies are unable to comply fully with mandatory Government requirements within a specified timeframe, it is important that they develop a clear timetable and process to establish a path to compliance and guide implementation.

Conclusion

2.29 The selected agencies 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); observed compliance state as at 30 November 2013; and reported planned compliance state by 30 June 2014.

2.30 The ANAO's summary findings for each of the selected agencies were reported in the context of a matrix, which indicates agencies' overall level of protection against internal and external threats as a consequence of steps taken to implement the top four strategies and IT general controls. The matrix, which is referred to as the *Agency Compliance Grade,* indicates where agencies are positioned in terms of ICT security zones: *vulnerable* zone; *externally* secure zone; *internally* secure zone, and *cyber secure* zone. The zones are explained further in Table 2.2 and illustrated in Figure 2.2. An agency's position indicates its overall ICT security posture—in essence how well the agency is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

2.31 In summary, each of the selected agencies was located in the *Internally Secure Zone*. The agencies had security controls in place to provide a reasonable level of protection from breaches and disclosures of information from internal sources. However, this is not sufficient protection against cyber attacks from external sources. To comply fully with the PSPF, agencies should also have a reasonable level of protection from external threats. The preferred state is for an agency to be located in the *Cyber Secure Zone*—where both ISM and IT general controls are effectively in place across the agency's enterprise systems, providing a high level of protection against all threats.

2.32 Each of the selected agencies has advised of activities underway that if effectively and fully implemented, would strengthen ISM controls and enhance the level of protection of information and systems, by 30 June 2014. For six of the agencies, the strengthening of one or more of the ISM controls would improve their agency compliance grade. Notwithstanding the agency activities planned for implementation by 30 June 2014, and in the absence of further agency initiatives, all of the selected agencies are likely to remain in the *Internally Secure Zone* and not achieve full compliance with the mandatory ISM controls by 30 June 2014, the date specified by the Australian Government.

2.33 Where agencies are unable to comply fully with mandatory Government requirements within a specified timeframe, it is important that they develop a clear timetable and process to establish a path to compliance and guide implementation.

Recommendation No.1

2.34 To achieve full compliance with the mandatory ISM 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.

Australian Bureau of Statistics response:

2.35 *Agreed. As indicated in the report, the agency is well placed in terms of its compliance with the top four ISM controls. Where full compliance has not been possible due to technical constraints imposed by a small number of legacy systems, mitigations have been put in place to reduce the risks associated with the use of these.*

Australian Customs and Border Protection Service response:

2.36 *Agreed.*

Australian Financial Security Authority response:

2.37 *Agreed.*

Australian Taxation Office response:

2.38 *Agreed.*

Department of Foreign Affairs and Trade response:

2.39 *Agreed.*

Department of Human Services response:

2.40 *Agreed. The department continues to implement and embed security practices into business as usual activities and strengthen compliance with the top four ISM controls across the ICT environment.*

IP Australia response:

2.41 *Agreed. IP Australia has a plan in place to improve its capability in this area. It will complete activities in train and following annual reviews, progressively strengthen its compliance with the top four ISM controls.*

3. Implementing Mandatory Strategies and Related Controls

This chapter examines in more detail the selected agencies' compliance with the four mandatory ISM strategies and related controls that protect ICT systems.

Introduction

3.1 In April 2013, the *Australian Government Protective Security Policy Framework* (PSPF) was updated. PSPF mandatory requirement INFOSEC 4 now requires agencies to implement the top four mitigating strategies and related controls listed in the ASD's *Strategies to Mitigate Targeted Cyber Intrusions:*

> Implementation of the 'Top 4' controls[66] is mandatory for all systems able to receive emails or browse web content originating in a different security domain. Under the PSPF, non-compliance with any mandatory requirements must be reported to an agency's relevant portfolio Minister, and also to ASD for matters relating to the ISM.[67]

3.2 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 executed[68];
- patching applications: applying patches to applications and devices to ensure the security of systems[69];
- patching operating systems: deploying critical security patching to operating systems to mitigate extreme risk vulnerabilities; and
- minimising administrative privileges: restricting administrative privileges provides an environment that is more stable, predictable,

66 ANAO comment: the 'Top 4' controls are the same as the four mandatory ISM strategies and related controls.

67 Defence Signals Directorate, *Australian Government Information Security Manual*, *Controls*, 2013, p.115

68 Defence Signals Directorate, *Application whitelisting explained* [Internet], 2012, available from <http://www.dsd.gov.au/publications/csocprotect/application_whitelisting.htm> [accessed 23 May 2013].

69 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].

and easier to administer and support as fewer users can make changes to their operating environment.[70]

3.3 Table 3.1 outlines *Control 1353*—the mandatory ISM controls[71] and their control numbers for each of ASD's top four mitigation strategies.

Table 3.1 Summary of the controls agencies must implement on all systems that receive email or Internet content

Mitigation strategy	Chapter and section in the ISM	Control numbers	
Application whitelisting	Software Security – Application Whitelisting	0843, 0844, 0845, 0846 0847, 0848, 0849	
Patch applications	Software Security – Standard Operating Environments	1349	0940, 1143 1144, 1348
Patch operating systems	Software Security – Standard Operating Environments	0941	
Minimise administrative privileges	Access Control – Privileged Access	0445	

Source: Australian Signals Directorate, *Australian Government Information Security Manual*, *2013 April Release Controls*, p. 115.

Note: Some controls are duplicated between patch applications and patch operating systems as they satisfy both strategies.

3.4 To assess agency compliance, the ANAO examined agency-level implementation of the four mandatory strategies and related controls across their enterprise ICT systems.

Deploying Application Whitelisting

3.5 Application whitelisting is a control which protects against unauthorised applications on a system. 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.

70 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].

71 In accordance with the ISM, *Control 1353* states that agencies must implement the controls indicated in Table 3.1 on all systems able to receive emails or browse web content originating in a different security domain.

3.6 Application whitelisting is often misunderstood or poorly implemented, which can lead to systems appearing more secure than they actually are. Application whitelisting can only be effectively deployed in support of policy which defines applications that users are allowed to run, or can be expected to run, in the course of their duties. The technical implementation of application whitelisting needs to reflect the organisation's policies in this area.

Summary assessment

3.7 To assess agency compliance with application whitelisting across controls, the ANAO examined agency efforts to:

- implement application whitelisting as part of the standard operating environment for desktops and for servers;
- prevent the running of executables not listed in an agency's application whitelisting policy;
- restrict users to running only a predefined set of executables to complete their duties;
- 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.

3.8 The ANAO gave particular attention to agencies' application whitelisting policy—the defined list of trusted executables and authorised applications; and application whitelisting rules—the systems configuration based on the policy, and the restrictions based on group user roles and responsibilities.

3.9 Table 3.2 provides a summary assessment of agency compliance with the seven controls that support application whitelisting.

Table 3.2: Summary assessment of agencies' compliance with application whitelisting controls across the desktop and servers

Control [ISM control number]	No. of agencies per grade				
Application Whitelisting	○	◔	◑	◕	●
Agencies must implement application whitelisting as part of the SOE for both workstations and servers. [ISM 0843]					
Grade for Desktop	0	2	2	3	0
Grade for Servers	5	1	1	0	0
Agencies must prevent a user from running arbitrary executables. [ISM 0844]	2	1	1	3	0
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]	2	1	1	3	0
Agencies must ensure that a user cannot disable the application whitelisting mechanism. [ISM 0846]	1	1	2	0	3
Agencies must ensure that application whitelisting does not replace antivirus and other Internet security software already in place for a system. [ISM 0847]	0	1	2	0	4
Agencies must ensure that system administrators are not exempt from application whitelisting policy. [ISM 0848]	3	1	2	0	1
Agencies must ensure that the default policy is to deny the execution of software. [ISM 0849]	2	1	1	0	3

KEY:
- ○ Control not in place and no dispensation authorised by the Agency Head
- ◔ Control not in place but a dispensation is authorised by the Agency Head
- ◑ Control not in place but agency is actively implementing, with a minimum of design deliverables in evidence
- ◕ Control in place across 80% or more of the agency
- ● Control in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required

Source: ANAO analysis.

Implement application whitelisting as part of the standard operating system

3.10 As discussed in Chapter Two, the deployment of application whitelisting across an agency's desktops was a priority activity for all of the selected agencies. A typical implementation of application whitelisting, as reported by the agencies, involved three phases:

(a) Prepare an application whitelisting strategy[72];

(b) Define the application whitelisting policy; and

(c) Create certificate and file path-based rules to enforce the policy.

3.11 The ANAO found five of the seven agencies had application whitelisting strategies, policies and rules in varying states. Three agencies had implemented whitelisting across their desktop systems; and for desktops, two agencies were actively deploying the strategies. In contrast, only one agency was found to be actively implementing application whitelisting across its servers.

3.12 Microsoft's AppLocker[73] was the preferred application whitelisting tool for six of the agencies as it supports Windows 7 (and above) on desktop operating systems. To define agencies' application whitelist policy, AppLocker was commonly first deployed in Audit Only mode to log events that it would have blocked, had it been enabled.

3.13 In order to test the effectiveness of the application whitelisting rules, the ANAO deployed a script to extract relevant data from agencies' desktop and server operating systems. A sample of 26 functional roles[74] was selected, and the script was run against their group policies. In all cases the ANAO found that agencies had a 'single' application whitelisting policy on their Standard Operating Environment (SOE) builds that applied to all access accounts, both for standard and privileged accounts. Path-based rules were the preferred identification method for executable files (.exe), Installers (.msi) and scripts (.bat, .cmd, .ps), but were not configured for Software Link libraries (.dll).

---

72 Several agencies incorporated their application whitelisting policy into their ICT Operational Policy or Cyber Security Framework, in favour of a standalone application whitelisting artefact.

73 AppLocker is a proprietary application of Microsoft, and can be enforced on computers running Windows 7 Ultimate, Windows 7 Enterprise, or any edition of Windows Server 2008 R2.

74 The ANAO provided agencies with a list of 26 common APS functional roles, such as Help Desk, local administrators, human resources, ministerial liaison.

Deny the running of arbitrary executables

3.14 The ANAO ran system commands on the agencies' Windows operating systems to make an assessment of the effectiveness of the rules to prevent a user from running arbitrary executables. Using Microsoft's calculator application—an embedded application in the operating system—the ANAO copied, saved and ran the application in various folders, such as the user profile's root and temporary directory. In four of the seven agencies the calculator application was successfully run from various directories, validating that the application whitelisting policy was not enforced.

3.15 Of further concern, while the agencies' SOE builds prevented users installing software on their desktops, the running of arbitrary executables was permitted if run from portable storage devices, such as a CDROM or USB drive.

Restrict users to a predefined set of executables

3.16 The ISM states that agencies must restrict a users' access rights so that they can only execute a specific set of predefined executables, as required for the users to complete their duties. For example, human resource staff may require access to certain payroll applications, while the Web Team may require a suite of editing applications which are not licensed for use by other staff.

3.17 The ANAO expected that most agencies would use group policies to restrict access privileges to the user's job function, as a user is only assigned to a group to perform their job function. When user access rights are position based, users added to a given position will inherit all the access permissions granted to that position. When a user moves positions, all the access rights associated with that position are revoked.

3.18 The ANAO observed that in all cases, where path-based rules were used, restrictions were not enforced for memberships of individuals and group policies from gaining access to applications on the systems. Certificate-based rules were commonly used to permit payroll and human resources group policies to access Financial Management Information Systems and Human Resources Management Information Systems, respectively, and offered greater protection from unauthorised accounts.

Prevent the disabling of application whitelisting

3.19 To ensure ongoing protection against unauthorised and malicious programs executing on the system, local administrative privileges should be

denied and further controls used to prevent the disabling of application whitelisting, or from being able to change which files can be executed.

3.20 For AppLocker policy to be enforced, the Application Identity service (AppIDsvc)[75] must be running. This service determines and verifies the identity of executables regardless of their name or file path, and is used by AppLocker to identify executables which should be allowed. Stopping this service will prevent AppLocker policy from being enforced and render whitelisting ineffective to prevent the installation or use of unauthorised executables.

3.21 The ANAO assessed the access controls to AppIDsvc, and found that only three of the six selected agencies that used AppLocker had effective measures to deny access to stop the service of AppIDsvc, and therefore prevent the disabling of AppLocker by this means. The ANAO did not assess other known means to circumvent or disable AppLocker.

Other Internet security software to complement application whitelisting

3.22 The ISM requires agencies to ensure that application whitelisting does not replace antivirus and other Internet security measures already in place for a system. The ANAO examined agencies' systems and found multiple security measures—part of a layered defence—against cyber attacks for each of the selected agencies. Commercial antivirus, web filtering and intrusion detection and prevention software identified were: McAfee VirusScan Enterprise, Trend Micro OSScan, Sourcefire IDS (Snort), Microsoft Forefront Endpoint Protection 2010, and Symantec Endpoint Protection. The ANAO made no assessment on the effectiveness of these commercial products, but concludes that the agencies mitigating security controls were enforced to complement application whitelisting.

System administrators are not exempt from the policy

3.23 System administrators are in a privileged position in terms of access to sensitive information and systems. Accordingly, the risks arising if these users run malicious code or otherwise exploit application vulnerabilities are far higher and consequences more severe.

---

75 For AppLocker rules to be enforced, the AppIDsvc must be set to start automatically in the Group Policy Object. In *AppLocker: Frequently Asked Questions* [Internet], available at: <http://technet.microsoft.com/en-us/library/ee619725(v=ws.10).aspx> [accessed 10 February 2014]

3.24 The ANAO examined agencies' application whitelisting policy and found only one agency had the control in place to ensure system administrators are not exempt from application whitelisting policy. Two of the agencies had the control in place for several privileged group policies, but not for other members. Of concern is that four of the agencies had no controls in place to adhere to their policy on system administrators. The agencies cited administrative overhead—time and limited resources as affecting the conduct of their (daily) system administrative duties, and as reasons for not adhering to their policy. The agencies advised that they understood the associated risk and used a risk-based approach to ensure that employment standards and security awareness education for systems administrators were high, and that their activities were monitored. The ANAO considers that system administrators in the four agencies which had not enforced the relevant policy controls were not effectively monitored.

Default policy is set to deny the running of executables

3.25 The current framework includes a number of 'legacy' controls reflecting the capability of older versions of application whitelisting tools that could be configured to either whitelist (*approved policy*) or backlist (*blocked policy*) executables. The existence of legacy controls reflects the evolving nature of the ICT security environment. Today, AppLocker by default has the policy set to deny the running of executables unless the executable is in the whitelist. The exception to this rule is if AppLocker is set to 'audit only mode', where it simply logs events that it would otherwise have blocked, had it been enabled.

3.26 The ANAO found two of the selected agencies had their application whitelisting set to audit only mode, and another two agencies were updating their SOE to Windows 7 and were at varying stages of deployment across their systems. The three remaining agencies had not altered the default policy and were set to deny the running of the executables. In summary, only three of the seven selected agencies had effectively deployed their application whitelisting policy to deny the running of executables.

Patching Applications

3.27 Security patching[76] involves the periodic deployment of software releases designed to fix problems with existing software. According to ASD, security patching to applications, operating systems and devices is rated as one of the most effective security practices agencies can perform to protect the security of ICT systems.

3.28 Critical patches are patches that address high risk vulnerabilities, such as unauthorised code execution by an intruder using the Internet. 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.

3.29 When a security patch is not available for a known vulnerability there are a number of approaches agencies can deploy to reduce the security risk to a system, such as: resolving the vulnerability through alternative means; preventing exploitation of the vulnerability; containing any exploitation; or implementing security measures to detect intrusions attempting to exploit the vulnerability.

3.30 Applications are software programs that are not part of the core operating system, but which perform necessary organisational functions, such as payroll and inventory recording. Application patch management needs to be considered separately to the operating system primarily because it is likely to be significantly more technically challenging than operating system patching. Most applications will have unique patching methods and requirements. It is important to integrate these into a single process, both from change management and technical perspectives.

3.31 Applications are a common exploitation vector for cyber intrusions for a number of reasons. Some commercial applications are present on the majority of corporate and government ICT systems, and efforts may therefore be made to exploit them. Further, many organisations do not patch (or are not aware of) all the applications on their systems. Intruders may seek to take advantage of the vulnerabilities in applications to gain a foothold on a network, which can be used to attack other systems from within the organisation.

---

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

Summary assessment

3.32 To assess agency compliance with the requirement to patch applications for desktops and servers across agency systems, the ANAO examined agency controls to:

- 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; and
- install the latest version of applications within two days if the upgrade addresses a known critical security vulnerability.

3.33 The ANAO specifically reviewed agency controls and patches deployed for:

- three common desktop applications: Microsoft Excel, Adobe Reader, and Java; and
- two corporate applications: financial management information systems (FMIS) that support payroll functions; and human resource management information systems (HRMIS) that support human resource functions.

3.34 The ANAO anticipated that agencies would have a patch management strategy, policy and procedures to deploy (vendor-issued) security patches for applications and operating systems, and a change management process that supported the authorisation of patches into the production environment.

3.35 The ANAO reviewed the application release notes of security patches issued by Microsoft and Adobe, for the period May to August 2013, and prepared a list of security patches to test against. As mentioned in the previous section, the ANAO deployed a script to extract relevant data from agencies' desktops and servers, and assessed if the security patches were deployed across the agencies' systems, and in a timely manner based on the application vendors' threat assessment. The ANAO also examined agencies' change management records for risk assessments and for authorised changes to release patches into the environment.

3.36 Table 3.3 provides a summary assessment of the selected agencies' compliance with the five controls that support the patching of applications.

Table 3.3: Summary assessment of agencies' compliance with controls to patch applications

Control [ISM control number]	No. of agencies per grade				
Patching Applications	○	◔	◑	◕	●
Agencies must apply all security patches as soon as possible. [ISM 0940]	3	0	3	1	0
Agencies must have a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities. [ISM 1143]	0	1	5	1	0
Agencies must apply all critical security patches within two days. [ISM 1144]	4	1	2	0	0
Agencies must install the latest version of applications as soon as possible. [ISM 1348]	0	0	6	1	0
Agencies must install the latest version of applications within two days if the upgrade addresses a critical security vulnerability. [ISM 1349]	1	1	5	0	0

KEY:
- ○ Control not in place and no dispensation authorised by the Agency Head
- ◔ Control not in place but a dispensation is authorised by the Agency Head
- ◑ Control not in place but agency is actively implementing, with a minimum of design deliverables in evidence
- ◕ Control in place across 80% or more of the agency
- ● Control in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required

Source: ANAO analysis.

Deploy security patches as soon as possible

3.37 According to ASD, once a security patch is released by a vendor, and has been assessed by agency staff for its applicability and the severity of the threat, the patch should be deployed in a timeframe which is commensurate with the severity of the threat/risk. ASD recommends the following deployment timeframes for severity patching, based on risk: *extreme*, within 48 hours; *high*, within 2 weeks; *medium*, within three months; and *low*, within one year.

3.38 Three of the seven agencies did not deploy any security patches: between May to August 2013[77]; during 2013; or since the last upgrade of the applications sampled by the ANAO. Of further concern is that these agencies did not conduct a risk assessment of the release notes of security patches as issued by the application vendors. For another group of three agencies, security patching was conducted on an *ad hoc* basis—when resources were available to assess and deploy the patches, or on some desktops and not for others. The ANAO observed that patches were applied inconsistently at a divisional or business unit level. Only one agency consistently deployed security patches for the sampled applications, and in accordance with the vendors' recommended timeframe based on the threat assessment.

Implement a patch management strategy

3.39 The ANAO examined agencies' documentation supporting a patch management strategy[78] and scored the strategy on its completeness, currency, and alignment to demonstrable patching practices as reported in the change management records. In all cases the selected agencies had a strategy, policy or a procedure to describe the patching of (general or specific) applications, a risk assessment plan, and a description of the change management process to seek authorised approval to release patches into the environment.

Apply critical security patches within two days

3.40 Critical patches are patches that address high-risk vulnerabilities, such as vulnerabilities enabling unauthorised code execution by an intruder using the Internet. Application vendors use different means of communicating vulnerability severity and these methods should allow agencies to quickly undertake an initial assessment of risk and the importance of patches for their environment. However, it remains incumbent on agencies to monitor these alerts and communications and to conduct their own risk assessment based on the impact to their business, operational activities and systems.

3.41 The ANAO found that only two agencies made consistent attempts to deploy critical patches within two days from the vendor releasing a critical security patch. The remaining five agencies adhered to their patch management strategy—notwithstanding their non-compliance with the

77 This is the reporting period assessed for security patches issued by vendors from May to August 2013.

78 This generally sets out the policy and trigger to conduct a risk assessment and to deploy security patches as proposed by vendors.

two day rule—preferring to conduct a considered risk assessment and to deploy the critical security patches in their (routine) patching cycle. Some agencies also cited real or perceived impact to business and ICT operations as reasons for deferring the deployment of critical patches within two days from vendor release.

Install the latest version of applications as soon as possible

3.42 According to ASD, the latest versions of business and corporate applications typically incorporate newer security technologies and mitigate known vulnerabilities. The ANAO interviewed the heads of agency ICT operations, and examined patching management strategies that support the decision to install the latest version of applications as soon as possible from the vendor release. Agencies generally updated business, corporate and supporting applications—such as Adobe Reader and Java—in a timely manner, and enforced agency policy to assess, plan, test and deploy the latest version of the application before deploying into their production environment. Overall, agencies were generally responsive to installing the latest version of applications, and in a timely manner.

Install the latest version of applications within two days to address a known critical security vulnerability

3.43 As discussed, agencies reported difficulties in implementing a 'two day implementation cycle' to patch or install the latest version of an application; resulting in non-compliance with mandatory requirements. Agencies expressed concerns about the risk of hastily upgrading an application into the production environment without a comprehensive systems test—a test and release cycle that usually required a much longer period than two days.

3.44 Instead, agencies cited a preference to conduct a considered risk assessment of the known critical vulnerability and to assess whether existing mitigating controls were in place to: enforce the necessary protection to strengthen existing controls, if required; or to deploy complementary controls. If these parameters were not met, then the agencies gave consideration to expedite the test and release cycle to upgrade the application with the latest version in the system. A review of the change management records found that agencies were more responsive to deploying upgrades for desktop applications (Microsoft Office, Java) than for corporate applications (FMIS, HRMIS), as corporate applications had a potentially greater impact on business if a comprehensive test was not conducted.

3.45 While there may be practical challenges to overcome in applying security patches within mandated timeframes, agencies will experience additional risk exposures the longer they delay implementation.

Patching Operating Systems

3.46 The operating system is the core around which the entire computing environment is built. If it is not stable and secure, then other security considerations are to a large extent weakened. If the operating system is compromised, any action or information handled by that computer is at risk.

3.47 There are many tools available which are capable of providing patches to operating systems, as well as monitoring and auditing their patch levels. Microsoft's primary tool in this area is the *System Centre Configuration Manager* (SCCM), which 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.

Summary assessment

3.48 To assess agency compliance with the requirements to patch operating systems for desktops and servers across the system, the ANAO examined agency controls to:

- 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; and
- implement mitigating controls for operating systems where known vulnerabilities cannot be patched, or security patches are not available.

3.49 The ANAO examined agencies' Windows 7 desktop operating systems, and their Windows, Unix and/or Linux server operating systems. As mentioned in the previous section, the ANAO deployed a script to extract relevant data from agencies' operating systems, and assessed if the security patches were deployed across agency systems, and in a timely manner based on the vendors' threat assessment. The ANAO also examined agencies' change management records for authorised changes to release patches into the environment.

3.50 Table 3.4 provides a summary assessment of the selected agencies' compliance with the five controls that support the patching of operating systems at the desktop and servers.

Table 3.4: Summary assessment of agencies' compliance with controls to patch desktop and server operating systems

Control [ISM control number]	No. of agencies per grade				
Patching Operating Systems	○	◔	◑	◕	●
Agencies must apply all security patches as soon as possible. [ISM 0940]					
Grade for Desktop	1	2	0	2	2
Grade for Servers	2	2	0	2	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	0	2	1	2	2
Grade for Servers	0	2	2	1	2
Agencies must apply all critical security patches within two days. [ISM 1144]					
Grade for Desktop	4	1	2	0	0
Grade for Servers	4	1	2	0	0
Agencies must install the latest version of operating systems as soon as possible. [ISM 1348]					
Grade for Desktop	0	0	1	3	3
Grade for Servers	0	0	1	6	0
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	0	0	2	3	2
Grade for Servers	0	0	2	3	2

KEY:
- ○ Control not in place and no dispensation authorised by the Agency Head
- ◔ Control not in place but a dispensation is authorised by the Agency Head
- ◑ Control not in place but agency is actively implementing, with a minimum of design deliverables in evidence
- ◕ Control in place across 80% or more of the agency
- ● Control in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required

Source: ANAO analysis.

Deploy security patches for the operating system as soon as possible

3.51 Common concerns relating to the patching of operating systems are that the system may no longer function as required, and the patch may impact on the applications supported by the operating system. While it is possible that any patch may change the state of a system enough that it will function differently, ASD recommends that agencies weigh this risk against not patching a given system.

3.52 The ANAO anticipated that agencies' patching practices for operating systems would align with patching practices for applications, as discussed in paragraph 3.39. A review of agencies' change management records relating to the authorisation to release security patches for the operating system found that all agencies gave more attention to deploying security patches at the operating systems level than for patches for applications. The audit team validated that operating system patches were deployed, as scheduled, into the production environment and that four of the seven selected agencies were compliant with the mandatory ISM requirements—deploying security patches within ASD's recommended deployment timeframes.[79]

3.53 Of concern, the three remaining agencies cited alternate patching practices, due to: a lack of regular maintenance windows for server environments; competing business and 24/7 operational activities; or a preference to upgrade the operating system in the context of the next release version and when systems and integration testing was completed by the agency.

Implement a patch management strategy for the operating system

3.54 As discussed, all agencies had a patch management strategy for applications and operating systems. In all cases the selected agencies had a strategy, policy or a procedure to describe the patching of operating systems (desktop and servers), a risk assessment plan, and a description of the change management process to seek authorised approval to release patches into the environment. However, the ANAO found that less attention was given by four of the seven agencies to effectively address the risks associated with patching the operating systems of servers, or did not document their alternate patching practices.

---

79 ASD recommends deployment timeframes for the assessed vulnerability/patch risk ratings that are: *extreme*–within 48 hours; *high*–within 2 weeks; *medium*–within three months; and *low*–within one year.

Apply critical security patches for the operating system within two days

3.55 Agencies cited common practices in applying critical security patches for applications and operating systems. Two agencies made consistent attempts to deploy critical patches within two days from the vendor releasing a critical security patch. The remaining five agencies applied critical patches in accordance with their patch management strategy, preferring to conduct a considered risk assessment and to deploy the critical security patches as part of their (routine) patching cycle or, of concern, to defer patching altogether and upgrading the operating system in the context of the next release version.

Install the latest version of the operating system as soon as possible

3.56 Agencies invest significant resources to maintain and monitor systems—particularly servers—to deliver business systems. The ANAO expected that agencies, as a minimum, would give due consideration to the reported advantages of upgrading their operating systems, and to deploy the latest version of the operating system in a timely manner.

3.57 In all cases the selected agencies were found to conduct risk assessments and to schedule the deployment of the latest version of the operating system, for either desktops or servers, within ASD's recommended timeframes. High load servers or systems that had a high impact on business needs were given priority for updating. One agency was scored lower than the other agencies due to inconsistent or deferred deployment practices to accommodate known 24/7 operational activities.

Implement mitigating controls where known vulnerabilities cannot be patched at the operating system

3.58 When a security patch is not available for a known vulnerability there are a number of approaches to reduce the security risk to a system. According to ASD, this includes resolving the vulnerability through alternative means, preventing the exploitation of the vulnerability, containing the exploit, or implementing security measures to detect intrusions attempting to exploit the vulnerability.

3.59 The ANAO examined agencies' ICT security resilience strategies and mitigating controls to: resolve the vulnerability; prevent the exploitation of the vulnerability; contain the vulnerability; and detect the intrusion. An assessment was made as to whether one or more of these controls were embedded as part of the agency's normal business process. Five of the seven selected agencies had mitigating controls deployed across the system to form

part of a layered defence against intrusions. Detection and prevention controls at the Gateway[80] were the most common control used by agencies, complemented by traffic monitoring capability.

Restrict Administrative Privileges

3.60 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 to failures on systems, and can lead to cyber security incidents. According to ASD, privileged accounts are targeted by adversaries as these can potentially give full access to systems, and the information held by an agency. Ensuring that privileged accounts do not have a channel from within the agency 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.

Summary assessment

3.61 To assess agency compliance with requirements relating to administrative privileges, the ANAO examined agency controls to:

- 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 reuse over time or for multiple accounts; and
- regularly review the privileges allocated to privileged user accounts.

3.62 Administrative privileges are the highest level of permission, granted only to trusted personnel to enable them to configure, manage and monitor a system. Access to such accounts can permit an individual to make any change to the system and to retrieve almost any information from it. While these privileges are necessary for the ongoing administration of a system, they introduce points of weakness to the system that may be exploited.

80 A device on a network—such as a router or firewall—that serves as an entrance to another network.

3.63 According to ASD, administrative privileges should be allocated to separate administrative accounts. These accounts should be logged and monitored to provide the agency with a clear picture of the number of administrative accounts that exist and whether they are active or disabled. Access should be limited to those that require them, and they should be monitored for appropriate use.

3.64 The ANAO examined agencies' policy statements that support the administration of accounts (including standard user and privileged accounts), and the logging and monitoring of accounts (including the number of users for each group policy).

3.65 Table 3.5 provides a summary assessment of the selected agencies' compliance with the ISM control to minimise administrative privileges.

Table 3.5: Summary assessment of agencies' compliance with controls for privileged access accounts

Control [ISM control number]	No. of agencies per grade				
Minimising Administrative Privileges	○	◔	◑	◕	●
Agencies must: • 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]	0	0	2	5	0

KEY:
- ○ Control not in place and no dispensation authorised by the Agency Head
- ◔ Control not in place but a dispensation is authorised by the Agency Head
- ◑ Control not in place but agency is actively implementing, with a minimum of design deliverables in evidence
- ◕ Control in place across 80% or more of the agency
- ● Control in place across the agency, and: maintenance is embedded as part of the normal business process; and controls are monitored and corrective action is taken as required

Source: ANAO analysis.

Privileged accounts are controlled and auditable

3.66 The ANAO expected that agencies would have a mature and documented policy, procedure or guideline for the administration of standard user and privileged accounts, and that the policy would detail protocols—as a minimum—to grant and revoke accounts, identify and authenticate users, and log and monitor privileged user activities. In all cases, the selected agencies had a policy for the administration of user accounts, which were usually complemented by Standard Operating Procedures or guidelines to provide standard and privileged users with instructions on user accounts. The instructions related to: applying for accounts; access entitlements based on business needs; and conditions for account access, including the revocation of access following staff movement or employment termination.

3.67 The ANAO also examined group policies of privileged users to ensure that accounts were controlled and auditable. While there were inconsistent practices across all agencies in the administration of group policies, overall the policies were found to be enforced.

System administrators are assigned separate accounts for administrative duties

3.68 According to ASD, administrators should have access to multiple accounts with differing sets of privileges. For example, a software developer who has a business requirement to install different software frameworks for testing might have a standard user account—to access business applications, email and Internet access, and a (developers) privileged account—with no email or Internet, but access to install software on desktops.

3.69 The ANAO examined agencies' group policies for standard access accounts and system administrator accounts. All of the selected agencies had separate accounts for system administrators, with the account usually identified by a different user name from the standard user account, or with a prefix in the user name to define the account type (john.smith_a for an administrator account), and for one agency a naming convention based on group system access (mainframes).

3.70 The ANAO did not assess the privilege level of accounts against their administrative duties. However, the ANAO did examine administrator accounts for email and Internet access—a known control weakness and a channel for breaches and disclosure of information from within the system. There were two instances where system administrator accounts had access to

email and/or Internet access. For one agency, this control was strengthened as part of the move towards a new Secure Gateway; while the second agency authorised access to email accounts for Exchange Administrators to administer the exchange server.

3.71 Of concern, one agency used *shared* administrator accounts for a database group policy, citing that for routine system maintenance work, it was more efficient to share an account amongst the ICT team. Of further concern, the agency did not have a method of attributing actions undertaken by such accounts to specific personnel. Having unique identifiable users ensures accountability, and the approach adopted by the agency introduced a high and avoidable level of risk.

Limit the number of privileged accounts

3.72 Many administrative tasks may not require administrative privileges to undertake the task, or may be undertaken with a limited subset of those privileges. For example, an Exchange Administrator may not require administrative privileges on any system other than the email servers. As recommended by ASD, access entitlements should be based on business needs—and where possible, kept to a limited number of accounts to reduce opportunities for privileged users to make unauthorised system modifications.

3.73 The ANAO examined agencies' group policies and assessed the number of users assigned against each group policy. In all cases, the ANAO observed that practices to restrict privileged access accounts did not align with their policies, resulting in non-compliance. For example, one agency had over 400 administrative accounts, and was unable to explain the business need for such high numbers; while another agency had multiple group policies to grant access to a database that contained sensitive information, with no set rules to explain why a staff member would apply to one group policy and not to another.

3.74 Despite inconsistent practices, agencies generally made regular assessments of their group policies to restrict access entitlements based on business needs, and revoked accounts where users had not accessed their system account for extended periods—30, 45 or 60 days depending on the agency's policy.

Audit the passphrases of privileged accounts

3.75 Strong identification and authentication mechanisms significantly reduce the risk that unauthorised users will gain access to a system. The ANAO observed that agency practices for complex passphrases for privileged access accounts did not align with their policies, resulting in non-compliance with the ISM. It is incumbent on agencies to enforce the use of complex and lengthy passphrases to access systems, more so where single sign-on[81] is used to access multiple systems.[82] While single sign-on offers convenience for users and productivity benefits for agencies, the related risks need to be managed.

Conclusion

3.76 The selected agencies had not yet achieved full compliance with the top four mitigation strategies and related controls mandated in 2013, and are not expected to achieve full compliance by the target date of mid–2014.

3.77 While the selected agencies demonstrated an understanding of the importance of protecting their systems against cyber attacks, they had nonetheless deferred the deployment of all mandatory ISM controls. Reasons included, competing operational priorities[83]; resource restraints; and accessing specialist skills. There were also instances of agencies adopting practices that were not consistent with their internal policies relating to implementation of the four mitigation strategies. For instance, a preference to conduct a considered risk assessment, for a period longer than that stated in the policy, before deploying critical security patches for a known vulnerability.

3.78 Application Whitelisting, one of the top four mitigation strategies, was in general hastily deployed by agencies, using 'audit only mode' to record executables in use across the system. Agencies did not tend to review and remove unauthorised executables, which is the better practice approach. The agencies adopted file path-based rules to enforce policy, which is the 'weakest' of the available rules to secure a whitelist.

---

81 Single sign-on (SSO) is a user authentication process that permits a user to enter one username and password in order to access multiple applications on the enterprise system. The process authenticates the user for all the applications they have approved rights to on the system, thereby eliminating further prompts when they switch applications for a particular session.

82 The ISM proposes that agencies use multi-factor authentication for privileged access accounts. The ANAO did not examine if the same passphrase was in use by the same user across their multiple accounts (standard account and privileged account).

83 For example, ICT resources must be allocated to deliver a range of business outcomes.

3.79 Security patching of applications and operating systems are two of the top four mitigation strategies, involving the application of updates to computer software to address emerging security vulnerabilities. A responsive and effective security patch management strategy relies on a lifecycle of: preparedness; vulnerability identification and patch acquisition; risk assessment and prioritisation; patch testing and deployment; and verification. While the selected agencies understood the importance of adhering to a patching strategy and policy, they generally adopted an *ad hoc* approach to applying the lifecycle. Agencies cited competing operational priorities to explain decisions to defer security patching on applications and operating systems.

3.80 Minimising administrator privileges is the fourth of the top four mitigation strategies. In each of the selected agencies, user access rights were governed by documented policies, which had regard to job requirements and business needs. In the case of privileged user accounts, such as those with administration rights over IT systems, audit logs were captured to facilitate monitoring and accountability. However, agencies invested little or no effort in monitoring and reviewing the logs of actions by privileged users.

4. IT General Controls

This chapter examines the selected agencies' IT general controls for logical access and change management that mitigate against internal breaches and disclosures of information.

Introduction

4.1 Agencies are custodians of official and personal information and are responsible for managing, protecting and preserving their data holdings. The integrity, security and privacy of such information can be threatened by an internal ICT security event, and agencies must actively manage the risks associated with electronic data transmission, processing and storage; which are now a routine aspect of agency business processes.

4.2 IT general controls (ITGC) are the policies and procedures developed to deal with an agency'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 agency's systems are protected from ICT security threats.

4.3 The ANAO examined agency-level implementation of the underpinning IT general controls that support ICT security for logical access and change management.

Managing logical access controls

4.4 Logical access controls provide protection against unauthorised entry to an ICT system and the information accessible from the system. Enforcing the authorisation of users through the use of logical access controls on a system decreases the risk of unauthorised use and disclosure of official and personal information. As a minimum, agencies must enforce policies and procedures intended to ensure consistency in the identification, authentication and authorisation of staff accessing agency systems, applications and databases. ASD recommends that agencies follow a process to develop an access control list, which typically involves the following steps:

- establish groups of all system resources based on similar security objectives;
- determine the information owner for each group of resources;

- establish groups encompassing all users based on similar functions or security objectives;
- determine the group owner or manager for each group of users;
- determine the appropriate level of access to the resource for each user group; and
- establish and manage delegations for security administration, based on the agency's security policy.

4.5 In circumstances where official information is particularly sensitive, extra ICT security measures need to be in place and enforced on systems to restrict access to staff with appropriate authorisation, and with a 'need-to-know' to conduct their duties.

Summary assessment

4.6 To assess the selected agencies' ICT security for logical access controls across the four systems layers—network, application, database and operating systems—the ANAO examined whether:

- user accounts are appropriately granted, suspended and revoked for privileged and non-privileged users;
- users are uniquely identifiable, authenticated and authorised in accordance with ISM controls;
- privileged user accounts are managed and segregated appropriately from other accounts and duties; and
- privileged user account activity is logged and reviewed to prevent and detect any inappropriate activities.

Network security layer

4.7 Agencies can structure and configure their networks with ICT security controls that will identify, reduce, or address network vulnerabilities from internal source threats. The ANAO expected that most agencies used Windows and Unix (Linux) operating systems at the network layer—supported by Active Directory—and prepared an audit methodology to examine each network layer.

4.8 The ANAO examined agencies' policies and procedures for network access controls, and assessed user access management in relation to staff commencements, terminations and movements (based on a sample of 25 instances of each type of activity). The ANAO also conducted tests to assess the access accounts for standard user and privileged user accounts from 26 functional roles.

4.9 Table 4.1 provides a summary assessment of agencies' compliance with logical access control requirements at the network security layer.

Table 4.1: Summary assessment of agencies' compliance with logical access control requirements at the network security layer

IT General Control	No. of agencies per grade		
Logical Access Management – Network	△	◬	▲
Granting and revoking user access.	0	4	3
Access control (identification, authentication and authorisation).	0	4	3
Management of privileged user accounts.	0	4	3
Audit log and review of privileged user activity.	3	3	1

KEY:
Control objective not met △
Identified control not in place but compensating control/s in place and observed ◬
Control objective is met ▲

Source: ANAO analysis.

Grant, suspend and revoke accounts at the network security layer

4.10 The ANAO reviewed agencies' records for staff commencements, terminations and movements. In all cases, the selected agencies had in place policies and procedures to manage network user access accounts, with a standard workflow and forms in practice, and authorisations recorded, stored and centrally managed. For standard user accounts, agencies grant access to the network based on a user's defined function, role or group policy as set at the commencement of employment, and access is usually amended (suspend, modify or revoke) due to internal movements to another business area. For privileged users, the granting of privileged accounts requires a business case to be raised by the user's business unit director (or above), along with a formal account creation form submitted for approval (ICT Security).

4.11 The agency compliance grade for four of the selected agencies was reduced because: accounts remained active after staff departures; network access rights were not revoked after staff movements to other business areas; or no records existed for known staff movements. In most instances, agencies record their staff movements and terminations in a human resource management information system—and this information is designed to also inform the network user administration team to manually remove the user from the local area network account the next business day after notification, in accordance with agency policy. However, this process does not always take place, and the ANAO observed instances where account deletions occurred five days after staff departures—contrary to the agency's policy—and in an extreme case an account was deleted after 90 days.

Identify, authenticate and authorise accounts at the network security layer

4.12 The ANAO examined agencies' policy and procedures covering users' identification, authentication and authorisation, and assessed whether active users are uniquely identifiable to an employee or contractor. For six agencies, network access control is deployed through Windows Active Directory—to authenticate and authorise all users and computers in a Windows domain type network, and to assign and enforce security policies. Overall, accounts were identifiable and segregated between standard users and privileged user accounts, and shared accounts could be directly attributed to a user for each authentication.

4.13 The audit team also examined policies and system configuration for passphrases in accordance with the ISM, and whether both initial and reset passphrases are required to be changed at the first log on to the system. In most cases, agency policies did not align with practices for passphrases across the networks, or the policy did not reflect the ISM's current requirement for complex passphrases. Four agencies cited difficulties in implementing complex passphrases due to technical limitations imposed by their legacy network systems, requiring dispensations to be issued by the agency head.

Management of privileged accounts at the network security layer

4.14 The ANAO examined agency policies and procedures to determine: what constitutes a privileged account for network access accounts; roles are clearly defined, documented and segregated appropriately; privileged accounts are identifiable from non-privileged accounts; administrative accounts do not have email or Internet access; and multi-factor authentication is enforced for all privileged users.

4.15 Overall, agencies are adhering to their policy to manage privileged accounts, and have effective controls to identify and segregate accounts from standard users and privileged accounts. In three instances, agencies had a business requirement for privileged users to have access to email accounts. Six agencies enforced multi-factor authentication for all privileged users, and therefore were found to be compliant with the ISM.

Log and review the activities of privileged accounts at the network security layer

4.16 The ANAO assessed whether agencies' policies to capture and maintain audit logs for privileged user accounts, are complete, and whether account activities are regularly reviewed and signed off by an appropriate staff member who is independent from the operation. The audit team examined agency policies, interviewed staff, and examined agency procedures to review logs for unauthorised and inappropriate activities.

4.17 In all cases, agencies created audit logs for privileged user accounts as a basis for reviewing recorded activities. However, the practice of reviewing the activities of privileged accounts was not enforced by three agencies. For another three agencies, the logs were not regularly reviewed in accordance with agency policy, or there was no evidence to substantiate that unauthorised user activity was identified or addressed. Of concern, agencies cited difficulties in reviewing the logs due to competing business and operational activities, or due to a lack of expertise to analyse the logs for unauthorised activities and to define trends in inappropriate behaviour on the network. Of further concern, for several agencies, audit logs were stored on the network where privileged users had 'read/write' access to the log—creating a risk that such users could modify the log.

Application security layer

4.18 The application layer within the overall ICT environment is particularly susceptible to cyber attacks, requiring even major software vendors to frequently update and patch their applications against new attack vectors. The timeframe from discovery to recognition and remediation is also increasing. As a minimum, ICT security across the application layer should be built with various levels of authorisation for transaction submissions and approval.

4.19 To accommodate business needs, agencies procure enterprise licences to operate commercial applications across their ICT environment, and in most cases, agreements are in place for updates or for the maintenance of the

applications. For payroll and human resource management activities, agencies use Financial Information Management Systems (FMIS) such as SAP; and a Human Resource Information Management System (HRMIS) such as SAP, PeopleSoft or Aurion. The ANAO prepared an audit methodology to examine each information management system, and prepared test controls that were non-vendor specific.

4.20 Table 4.2 provides a summary assessment of agencies' compliance with logical access control requirements at the application security layer.

Table 4.2: Summary assessment of agencies' compliance with logical access control requirements at the applications security layer

IT General Control	No. of agencies per grade		
Logical Access Management – Applications	△	◭	▲
Granting and revoking user access.	0	0	7
Access control (identification, authentication and authorisation).	0	4	3
Management of privileged user accounts.	0	2	5
Audit log and review of privileged user activity.	0	3	4

KEY:
△ Control objective not met
◭ Identified control not in place but compensating control/s in place and observed
▲ Control objective is met

Source: ANAO analysis.

Grant, suspend and revoke accounts at the applications security layer

4.21 As discussed, the ANAO examined agencies' records for staff commencements, terminations and movements—but in this instance only for staff that had privileged access to the agencies' FMIS and/or HRMIS sensitive functions. Again, all of the selected agencies had in place policies and procedures to manage their information management systems, and were found to effectively manage the granting, suspension and revocation of standard user and privileged users accounts.

Identify, authenticate and authorise accounts at the applications security layer

4.22 Policy and procedures covering users' identification, authentication and authorisation to the FMIS and HRMIS were examined, and in most cases, enforced authorisations provide appropriate restrictions to stop a user from

making changes to the information systems, and in the case of HRMIS, prevented a user from changing their own records. Agencies were also found to effectively manage and differentiate access accounts from staff and contractors, and in most cases contractor accounts have expiry dates set according to their contract end date.

4.23 To obtain access to information management systems, users were required to use single sign-on via the network layer. Four agencies cited difficulties in implementing complex passphrases at the network layer—thus affecting corporate applications—due to technical limitations imposed by their legacy network systems; resulting in non-compliance with the ISM.

Management of privileged accounts at the applications security layer

4.24 In most cases, agencies effectively enforced their policy to manage privileged accounts. Two agencies were scored lower than other selected agencies for having redundant group policies that did not differentiate between user access rights. Multi-factor authentication was enforced for six of the seven agencies, as reported above.

Log and review the activities of privileged accounts at the applications security layer

4.25 The capture and maintenance of audit logs for privileged user activities at the application layer was enforced by all agencies, although not consistently across both FMIS and HRMIS—more for payroll activities than for human resource activities. Of concern, the logs were not reviewed regularly for three of the selected agencies. Considering the importance of the information stored and accessible from these information management systems, these agencies exposed themselves to a higher risk of compliance breaches and disclosures.

4.26 One agency had sound practices to: record detailed activities of privileged user accounts based on group policies; store the logs for three days; and review the logs, after which the log is summarised so that only statistical information is available. A detailed audit record of changes to sensitive data was also maintained as part of the database record.

Database security layer

4.27 Agencies' databases and database management systems are the repositories for official information and require appropriate ICT security measures to protect these assets. Storing particularly sensitive content on databases can worsen the consequences if the database is compromised, and

consideration must be given to the business need for storing information in this way. To ensure that appropriate protective measures are enforced for information, database administrators and database users need to know what level of sensitivity is associated with the database and its contents. For example, storing authentication credentials such as usernames and passwords as plaintext in databases poses a significant risk to agencies if disclosed. In addition to security measures to store information in databases, agencies should enforce administrative credentials, as a minimum.

4.28 The ANAO expected that all agencies conducted payroll and human resource management activities in FMIS and HRMIS, respectively, and that these information management systems were supported by databases. The audit team prepared an audit methodology to examine the databases that supported the information management systems, and prepared test controls that were non-vendor specific.

4.29 The ANAO limited the scope of the assessment to database administrators (DBAs), who are privileged users with administrative access to the database. DBAs extract data from the data warehouse through SQL queries based on an internal business request for information, and conduct administrative tasks to maintain or improve access to information in the data warehouse. Most DBAs will only need a subset of all available privileges to undertake their authorised duties, and for improved security, are restricted to defined roles rather than accounts with default administrative permissions or all permissions.

4.30 Table 4.3 provides a summary assessment of agencies' compliance with logical access control requirements at the database security layer.

Table 4.3: Summary assessment of agencies' compliance with logical access control requirements at the database security layer

IT General Control	No. of agencies per grade		
Logical Access Management – Databases	△	◭	▲
Access control (identification, authentication and authorisation).	1	4	2
Management of privileged user accounts.	3	1	3
Audit log and review of privileged user activity.	5	1	1

KEY:
△ Control objective not met
◭ Identified control not in place but compensating control/s in place and observed
▲ Control objective is met

Source: ANAO analysis.

Identify, authenticate and authorise accounts at the database security layer

4.31 The ANAO examined agencies' policy and procedures covering DBAs identification, authentication and authorisation, and found that two of the seven agencies enforced their policy for both FMIS and HRMIS. Four of the agencies were only partially compliant, or applied their policy inconsistently. At one agency, the policy was enforced in respect to one information management system but not another. The ANAO also found cases where DBAs were given access to more subsets (or all) of the data in the data warehouse, exceeding the requirements of their duties. The affected agencies cited a preference to permit more DBAs with 'global access' to the database in the event of staff absences and collaborative management activities, and also advised that the complexity of the database made it convenient to allow DBAs unrestricted access. Of further concern, two agencies permitted shared accounts between DBAs for the same information management system (FMIS or HRMIS), but only one of these two agencies had controls in place to monitor and attribute the activity to a specific user.

4.32 In four cases the agency policies for complex passphrases at the database security layer did not align with agency policy or mandated practices, and were non-compliant with the ISM.

Management of privileged accounts at the database security layer

4.33 As discussed, the ANAO examined agency policies and procedures to identify DBA privileged accounts and whether: roles are defined and segregated appropriately; accounts do not have email or Internet access; and

multi-factor authentication is enforced. The ANAO's analysis indicated that there were inconsistent practices across the selected agencies.

4.34 Overall, agency DBA group policies were defined by the application (FMIS or HRMIS) that the DBAs supported, rather than the database or its environment, and in most cases the group policy did not differentiate the data set the DBA was restricting access to. Three agencies effectively enforced the segregation of duties of DBA activities from other system functionalities, with privileged accounts only allocated to users with a requirement to perform tasks that related to database administration, support or maintenance.

4.35 The audit team identified three agencies that were unable to account for the excessive number of DBA group policies, or had an excessive number of DBAs assigned an account that was outside their immediate duties, or had DBAs that had not accessed their account within the past 30 days.

Log and review the activities of privileged accounts at the database security layer

4.36 The ANAO assessed agency policies to capture and maintain audit logs for privileged user accounts, and found that in most cases the policy was not enforced. Of significant concern, five agencies did not enforce controls to automatically log DBA activities—a shortcoming further compounded by those agencies permitting shared accounts, as discussed above. For these five agencies, there were no means therefore to review or report on unauthorised or inappropriate activities at the database layer.

Operating systems security layer

4.37 The operating system is the computer's control program, allowing users and their applications to access and share common computer resources (printers, databases), to schedule job processing according to established priorities, and to balance the use of resources among the competing applications. To perform these tasks, the operating system should have effective ICT security controls that protect: *itself from users*—applications should not damage the operating system; *users from each other*—one user must not be able to access, corrupt or destroy the data or program of another user; *users from themselves*—modules within an application must not corrupt or destroy another module; *from itself*—modules within the operating system must not corrupt or destroy another module; *and from its environment*—achieve a controlled termination of activities (due to power failures) from which it can later recover.

4.38 The ANAO examined the operating systems that support agencies' desktops (Windows), FMIS and HRMIS, by developing tests to assess the access accounts for standard users and privileged user accounts from 26 functional roles.

4.39 Table 4.4 provides a summary assessment of agencies' compliance with logical access control requirements at the operating systems security layer.

Table 4.4: Summary assessment of agencies' compliance with logical access control requirements at the operating systems security layer

IT General Control	No. of agencies per grade		
Logical Access Management – Operating Systems	△	◉	▲
Access control (identification, authentication and authorisation).	0	5	2
Management of privileged user accounts.	1	3	3
Audit log and review of privileged user activity.	4	2	1

KEY: Control objective not met △ | Identified control not in place but compensating control/s in place and observed ◉ | Control objective is met ▲

Source: ANAO analysis.

Identify, authenticate and authorise accounts at the operating systems security layer

4.40 The ANAO examined agency policies and procedures covering user identification, authentication and authorisation to the desktop operating system, and the server operating systems that supported FMIS and HRMIS. In six of the seven cases where agency desktops and servers were Windows-based, the policies to authenticate and authorise users were enforced. Also, in five of the seven agencies that used a Unix (Solaris, Linux) operating system to support their FMIS and/or HRMIS, the policies to authenticate and authorise users were enforced. Overall, the ANAO found that agencies maintained and enforced user policies, and accounts were uniquely identifiable or attributed to an employee or contractor, in accordance with internal requirements. For four agencies, the practice for complex passphrases at the database security layer did not align with their policies, resulting in non-compliance with the ISM.

Management of privileged accounts at the operating systems security layer

4.41 The ANAO examined agency policies and procedures to manage privileged accounts, and found in all cases that agencies had group policies that distinguished between standard users and privileged users. Group policies were also enforced for desktop, domain, server, and database administrators who had access to operating systems. One agency which had undergone a recent restructure of its Unix operations, was found not to have enforced its policies, with administrators retained access privileges based on their 'legacy duties' in addition to their current roles and group policy. Further, multi-factor authentication was not enforced by two agencies.

Log and review the activities of privileged accounts at the operating systems security layer

4.42 The ANAO assessed agency policies to capture and maintain audit logs for privileged user accounts, and found that in most cases the policy was not enforced. This is a systemic control weakness that raises questions as to how effectively agencies can identify, respond to, or investigate unauthorised access to privileged user accounts, or inappropriate activities by privileged users.

Change management process

4.43 Changes to an agency's ICT environment are generally managed using a standardised process. A change management process covers changes to all technology and communications components—networks, hardware platforms, application software—and requires appropriate supporting documentation.

4.44 An effective change management process can help ensure that standardised methods and procedures support a formal request for a change to ICT systems. Changes must be controlled adequately, so that: the exposure to risk is minimised; the severity of the impact and service interruption is minimised; and the change is implemented successfully the first time. An effectively implemented change management process will provide for changes to be recorded, assessed, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner.[84]

84 As defined by the Information Technology Service Management Forum (itSMF) in *Foundations of ITIL V3*, Van Haren Publishing, Zaltbommel, 2010 p. 233. The Information Technology Infrastructure Library (ITIL) is an international framework of best practices and provides a systematic approach to the delivery of quality ICT services.

4.45 For changes made to ICT systems, consideration needs to be given to the controls supporting the agency's change management process in the following categories: approval and tracking; testing of changes; rollback procedures; change logs and reporting; emergency changes; policy and governance frameworks; and release management.

Summary assessment

4.46 To assess agencies' change management processes to effectively authorise the implementation of security patching for applications and operating systems, the ANAO examined whether:

- only authorised changes are made to systems, programs and data;
- changes are adequately tested before they are implemented;
- 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.

4.47 The ANAO reviewed agency change records for the reporting period of May to September 2013[85], with particular attention given to change requests seeking authorisation to deploy security patches into the production environment. A sample of 15 or more change records were examined in each agency for normal, standard and emergency changes.

4.48 Table 4.5 provides a summary assessment of agencies' compliance with change management process requirements.

85 This aligns with the reporting period used to assess the security patches issued by vendors from May to August 2013, plus a month to accommodate: the deployment timeframes for patch risk ratings that are assessed as extreme (within 48 hours) or high (within 2 weeks); and the agency's patch management cycle.

Table 4.5: Summary assessment of agencies' compliance with change management process requirements

IT General Control	No. of agencies per grade		
Change Management Process	△	◬	▲
Only authorised changes are made to systems, programs and data.	0	2	5
Authorised changes are correctly reflected in the system and do not adversely impact on other systems and processes.	0	0	7
Changes necessary to the proper operation of the ICT environment or application systems are made in a timely manner.	2	3	2
Emergency changes are controlled.	0	2	5
Unsuccessful changes can be managed without affecting production integrity.	0	0	7

KEY: Control objective not met △ Identified control not in place but compensating control/s in place and observed ◬ Control objective is met ▲

Source: ANAO analysis.

Authorised changes to the system

4.49 Changes should be approved by a change management process involving representatives from all parties involved in the management of the system. This process ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the system. The ANAO examined agency change and release management policies and procedures to determine: the types and scope of changes (standard, normal, emergency changes); whether change requests are classified, reviewed and approved; and whether a segregation of duties exists between change requesters and change implementers.

4.50 Overall, the ANAO found that: all agencies had a mature process to manage requests for change to the system; agency practices aligned with their policies; there was appropriate representation from system administrators and users on the Change Advisory Board; and requests for change, decisions and authorisations were documented and stored in a centralised management system. A sample of request for changes was also examined in each agency, to determine whether users with access to make changes in the production

environment did not have a potential conflict between change requester and change implementer roles. For each agency, there was an appropriate segregation of duties and no identified conflicts.

Changes are tested before implementation

4.51 Before deploying changes into the production environment, authorised requests for change should be passed on to the relevant technical groups to: build the change (configure, code); test the changes; consider remediation or corrective action; and consider the implementation method for the changes. In the case of patching, while the vendor has taken the responsibility to build the change, it remains incumbent on the agency to review the vendor-issued release notes and to conduct a risk assessment on deploying the patches on agency systems—mindful of any bespoke configurations and integration issues with other applications that the vendor is unable to thoroughly assess against.

4.52 In all cases, the ANAO found that agencies tested patches in lower environments before deploying to the production environment, and had documentation and authorised rollback procedures in the event that deployment was unsuccessful during the release window. Several agencies took further steps to first deploy the patches—as a pilot—to a smaller population of users or systems to manage unforseen risks that could compromise business needs and ICT operations due to a 'faulty' patch or integration issue. The ANAO also observed that unsuccessful changes were generally managed without adversely affecting the production environment.

Changes are made in a timely manner

4.53 The ANAO assessed agency change management processes to apply patches and upgrades to applications and the operating system in a timely manner. As discussed, agencies must follow a process to first conduct a risk assessment on the vendor-issued security patches (and a threat assessment), and where found to be appropriate, to enforce the policy to seek an authorised request for change to test and deploy the patches into the production environment. In all cases, the ANAO found that agencies had standard changes (pre-authorised/approved) in place to deploy security patches for applications and operating systems. While a standard change did not remove the responsibility for technical groups to test the patches in lower environments, it did expedite the change process and reduced the need to seek Change Advisory Board approval for each identified patch release. Standard changes were also supported with pre-approved documented rollback procedures.

4.54 Of concern, the ANAO found that security patching was not deployed in a timely manner, as recommended by the vendors' vulnerability assessment and patch risk rating. For five agencies, security patching at the application and operating systems was either: conducted on an *ad hoc* basis; did not adhere to ASD's deployment timeframe; deferred in preference to upgrading the application and operating systems at the next release version; or not deployed. In summary, the ANAO observed patching practices that were not enforced against agency patch management policies, resulting in non-compliance with the ISM.

Emergency changes are controlled

4.55 An emergency change is intended to repair, as soon as possible, a failure in an ICT service that has a large negative impact on the business. In most cases this requires the permission of the Change Advisory Board, but where the 'full' board cannot convene a smaller group is generally identified to make an emergency decision. The ANAO examined agencies' change and release policy for emergency changes, how it is defined, approved, and the conduct of a post implementation review for lessons learned to assess the cause of the emergency change.

4.56 The ANAO found that emergency changes across the selected agencies were well controlled, with authorisations granted by an Emergency Change Advisory Board—via email or phone—and retrospectively documented in the change record after the deployment of the emergency change. For two of the agencies, the ANAO did not find records that post implementation reviews for emergency changes were conducted, although the Change Advisory Board for those agencies discussed the emergency change at the next Board meeting.

4.57 The ANAO also assessed the volume of emergency changes against the total number of change requests for the reporting period May to September 2013, and found that for most agencies, between two and seven per cent were categorised as emergency changes, with one agency recording 20 per cent. For each of the samples examined by the ANAO, the emergency changes were appropriately categorised based on the issues identified and the impact on business.

Changes are implemented or rolled back

4.58 If a request for change is successfully implemented across the system with no impact to business users or to ICT operations, the request for change is closed, and the outcome included in the post implementation review—the

change evaluation. If a change is unsuccessful, and requires a rollback to the past ICT systems state, then change management or the Change Advisory Board should decide if further action is required.

4.59 The ANAO examined agency change and release management policies and procedures for post implementation reviews and rollback procedures, and found that for all of the selected agencies, deployment verification was conducted and signed off by a group other than the team deploying the change, and rollback procedures were documented to a comprehensive level of detail. As discussed, agencies did not conduct post implementation reviews for standard changes—changes categorised for patching of applications and operating systems—but did so where emergency changes were deployed or rollback procedures were conducted for unsuccessful deployments.

Conclusion

4.60 An effective IT general controls 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.

4.61 Agencies' logical access control and change management processes were generally well positioned to deal with internal source threats, which tend to be well known and understood compared to external source threats. The agencies' 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.

4.62 While the selected agencies generally had appropriate and effective logical access control and change management processes in place, an area for improvement relevant for most of the agencies was the control of access to databases. While other layers of control can compensate for weaknesses in this regard to some extent, this is an issue that requires early attention, so as to reduce the risk of external attacks and internal breaches and disclosures of information stored on agency databases.

Recommendation No.2

4.63 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.

Australian Bureau of Statistics response:

4.64 *Agreed. The ABS has, where practical, eliminated the use of shared accounts. Where this has not been possible, mitigations have been put in place to reduce risks associated with the use of shared accounts.*

4.65 *The ABS has implemented an ongoing program of work to enhance audit logging and monitoring activities associated with the use of privileged user accounts.*

Australian Customs and Border Protection Service response:

4.66 *Agreed.*

Australian Financial Security Authority response:

4.67 *Agreed.*

Australian Taxation Office response:

4.68 *Agreed.*

Department of Foreign Affairs and Trade response:

4.69 *Agreed.*

Department of Human Services response:

4.70 *Agreed. The department continues to implement processes which will improve the management of privileged user accounts including logging, monitoring and access controls.*

IP Australia response:

4.71 *Agreed. IP Australia will implement Recommendation 2 as part of its plan to improve its security posture.*

5. Strengthening Agencies' ICT Security Posture

This chapter considers how agencies can strengthen their overall ICT security posture and improve levels of cyber resilience.

Introduction

5.1 Cyber resilience is the ability to continue to provide services while deterring or responding to cyber attacks. To build cyber resilience, agencies should first understand their ICT security posture—their exposure to external and internal threats and vulnerabilities—and how well they are positioned to address threats and vulnerabilities.

5.2 The overall agency compliance grades discussed in Chapter Two reflect the ICT security posture for the seven selected agencies, as at November 2013. The grades illustrate individual agencies' exposure to cyber attacks and their readiness to combat the cyber threat by deploying the top four mitigating strategies across their ICT environment[86], building on the foundation established by IT general controls.

5.3 In summary, each of the selected agencies had security controls in place to provide a reasonable level of protection from breaches and disclosures of information from internal sources, but vulnerabilities remain to attacks from external sources. Further, agencies' security measures from internal source threats are supported by the IT general controls framework. A key factor contributing to agencies' access control and change management processes being consistently stronger than their application of the mandatory ISM controls, is the level of attention given to these control elements over a relatively long period of time.

5.4 However, the selected agencies had not yet achieved full compliance with the four mandatory ISM strategies and related controls, although each has advised of improvement activities underway. Where agencies are unable to comply fully with mandatory Government requirements within a specified

86 The *Agencies' Compliance Grade* is not a definitive assessment of the agencies' IT security posture—it is limited in scope by the assessment made against 14 mandatory ISM controls and IT general controls for logical access and change management process.

timeframe, it is important that they develop a clear timetable and process to establish a path to compliance and guide implementation.

5.5 This chapter considers how agencies can strengthen their overall ICT security posture and improve levels of cyber resilience.

Strengthening cyber resilience

5.6 There are significant differences between agencies in the services delivered, business needs, staff numbers, breadth of client base and the information managed. Agencies' specific requirements will inform the ICT solutions and systems adopted, and a one-size-fits-all approach to combat against cyber attacks is unlikely to be fully effective. Agencies should understand their specific ICT environment so as to adopt an informed ICT security posture appropriate for their circumstances.

5.7 In the context of an evolving cyber threat environment, agencies must have cyber resilience, to enable them to continue providing services while also deterring and responding to external cyber attacks. A sound understanding of an agency's ICT security posture can provide senior management with assurance that effective security measures are implemented to reduce the risk posed by cyber attacks. ICT operational staff will continue to retain day-to-day responsibility for setting and enforcing security policy and procedures across systems. However, additional assurance can be provided by: promoting security awareness across the agency; establishing governance arrangements commensurate with the threat, and informed by risk analysis; maintaining relevant skills and seeking external advice; prioritising implementation of the Top 35 mitigation strategies; and addressing security gaps.

Promoting a security culture

5.8 The PSPF emphasises that the head of each agency is ultimately accountable for the agency's cyber security. The selected agencies have generally established ICT security officers[87], provided information security awareness and training, established security controls to safeguard information, and implemented security measures to protect systems against most known cyber threats. The PSPF also emphasises the need for agencies to develop an

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

appropriate security culture to support the effective conduct of government business.

5.9 Security awareness and initiatives are a shared responsibility within an organisation. Well prepared agencies adopted a mutual obligation approach towards security awareness, responsibility and accountability; where key staff have a duty to monitor and report on observed cyber behaviour. Leading by example, senior managers in these agencies responded to cyber security incidents in a timely manner (reactive), and were informed of cyber trends—the motives, opportunities and emerging technology—that might target and compromise agency systems (proactive). To achieve this outcome, the relevant executives understood their roles and responsibilities to enhance security initiatives for the services they were accountable for, and tended not to expect ICT technical staff to be solely responsible for resolving ICT security matters.

ICT governance

5.10 While several agencies had key ICT security appointments, in some instances they had limited scope to influence processes to implement effective security measures. For example, Chief Information Security Officers (CISO) and Information Technology Security Advisors (ITSA) are appointed to inform the strategic security direction for an agency, and to provide a communication and coordination role to align security information to business functions. The ANAO assessed the roles and responsibilities of CISOs and ITSAs across the selected agencies, and found that for several agencies those roles had limited duties, such as the collation of ICT security incident reports. Few agencies invited their CISO and/or ITSA to senior executive briefings, and they were not routinely invited to contribute to decision-making processes for enhanced security initiatives. Nor did they generally provide updates on emerging global trends relating to cyber threats.

Maintain relevant skills and seek advice

5.11 The ANAO observed that effective agencies had key ICT operational staff with a sound understanding of the threats and vulnerabilities relating to their specific applications and/or security layers (including in respect to the wider ICT network, applications, databases and operating systems). They were aware of known security flaws affecting their system and deployed mitigating controls in the absence of enterprise-wide security measures. One of the selected agencies also had a dedicated Vulnerability Assessment Team with the necessary security capability to assess attack vectors against the agency's

systems, and to monitor and act upon unauthorised user access and inappropriate user activities in a timely manner. The deployment of such a team merits consideration depending on an agency's assessment of risk.

5.12 The ANAO interviewed agencies' executives and found most were aware of the security services provided through AGD and ASD, and a number had engaged the services of ASD to conduct threat and vulnerability assessments through system penetration testing.

Prioritise security initiatives

5.13 Most agencies are faced with ongoing and often competing ICT development priorities. The ANAO interviewed staff and found ongoing demands upon senior executives and ICT operational staff which often had an impact on services and delayed the deployment of new or enhanced ICT security measures. Nonetheless, there remains a responsibility to protect the agency against cyber attacks on a risk basis. Australian Government policy, such as the ISM, recognises the need to prioritise effort in the context of managing risk.

5.14 The ISM is an established information security framework and a reference to support agencies to build and manage their security measures across their ICT environment. Further supported by ASD's guide on the *Top 35 mitigation strategies against cyber intrusions*, agencies are well placed to conduct a comprehensive ICT risk assessment against their systems. Risk assessment enables agencies to understand their ICT security posture, and for management to plan and prioritise security initiatives in order to treat identified risks.

5.15 Agencies which look beyond the four strategies are better placed to manage threats and intrusions. Each of the selected agencies had taken varying steps to implement the remaining 31 controls from the *Top 35 mitigation strategies against cyber intrusions* promulgated by ASD.

5.16 Several agencies were using the Top 35 mitigation strategies as a framework to conduct formal and informal internal audits of their systems. Two of the selected agencies engaged staff to conduct assessments across the ICT environment (business process and systems), established self-reporting activities (Internal Audit), and conducted health checks on the effectiveness of deployed security measures. Figure 5.1 summarises the security initiatives conducted by these two agencies, which reflected better practice.

Figure 5.1: Better Practice Example: Conduct cyber health checks

Better Practice Example Conduct cyber health checks	
Annual ICT security risk assessment activity	Internal Audit conduct an ICT security risk assessment on the agency's progress to deploy the agreed mitigating strategies across the environment, and present the report at a senior executive level briefing. The report includes, as a minimum: compliance against the security controls (now); the compensating controls in the absence of the 'final' controls (interim); the effectiveness of the control in light of emerging cyber trends (changing); and recommendations for new security controls and initiatives based on identified security control gaps (known unknowns).
Periodic ICT security risk assessment activity	Key (non-ICT) staff are engaged to conduct 'health checks' on corporate applications. For example, staff responsible for payroll duties (access to FMIS) and recruitment (access to HRMIS) are well placed to report on inconsistent system performance or anomalies to the integrity of the data. In addition, these key staff should conduct periodic diagnostics on the integrity of the information accessible from the applications[88], with concise reports submitted to ICT Security for assessment and, if necessary, further investigation conducted.
Ongoing ICT security risk assessment activity	Key staff monitor and report on observed anomalies to information and systems, with particular attention given to the official information that they routinely contribute to, access and review. To achieve this outcome, agencies may need to revise security incident reporting procedures.

Source: ANAO.

Addressing security gaps

5.17 The selected agencies had not yet achieved full compliance with the PSPF and ISM, although each has improvement activities underway.[89] Agencies advised that factors affecting their current security posture and level of compliance with the four mandated strategies included: competing operational priorities[90]; resource restraints; and accessing specialist skills.

88 Similar to the conduct of User Acceptance Testing (UAT) prior to deployment of new or updated versions of an application into the production environment, functional test scripts can be developed to access the business integrity of the application, and the data accessing from the application. Due consideration needs to be given to develop scripts that does not compromise the production data, or reduce network performance during key operational periods.

89 Figure 2.3 illustrates the selected agencies' observed compliance state at 30 November 2013, and the planned compliance state by 30 June 2014.

90 For example, ICT resources must be allocated to deliver a range of business outcomes.

Achieving full compliance will require further strengthening of agencies' mandatory ISM controls to achieve a high level of protection for their information and systems.

5.18 The ANAO also found cases where other security gaps were known by agency management or ICT operational staff but were not addressed (*known risks*). Agencies advised that competing priorities could be an impediment to deploying appropriate security measures or mitigating solutions in the short term. Agencies therefore deferred taking immediate action and advised the ANAO of plans to implement further initiatives to address these security gaps as part of forthcoming upgrades to applications, operating systems, or the agency's ICT infrastructure. Of further concern, deployment across agency systems might be delayed for between six to 18 months—a significant period without the appropriate security measures to protect the agency's systems and information from threats and vulnerabilities.

5.19 To strengthen their ICT security posture, the selected agencies should conduct annual threat assessments across the ICT systems, having regard to the *Top 35 Mitigation Strategies*; and implement periodic review by the agency security executive of the overall ICT security posture.

Conclusion

5.20 In the context of an evolving cyber threat environment, agencies must have cyber resilience, to enable them to continue providing services while also deterring and responding to external cyber attacks. A sound understanding of an agency's ICT security posture can provide senior management with assurance that effective security measures are implemented to reduce the risk posed by cyber attacks. While ICT operational staff retain day-to-day responsibility for setting and enforcing security policy and procedures across systems, governance arrangements commensurate with the threat, and informed by risk analysis, can provide additional assurance.

5.21 Security awareness and initiatives are a shared responsibility within an organisation. Well prepared agencies adopted a mutual obligation approach towards security awareness, responsibility and accountability; where key staff had a duty to monitor and report on observed cyber behaviour. Leading by example, senior managers in these agencies responded to cyber security incidents in a timely manner (reactive), and were informed of cyber trends—the motives, opportunities and emerging technology—that might target and compromise agency systems (proactive). To achieve this outcome, the relevant

executives understood their roles and responsibilities to enhance security initiatives for the services they were accountable for, and tended not to expect ICT technical staff to be solely responsible for resolving ICT security matters.

5.22 Further, agencies which seek external advice as necessary, and also look beyond the four mandated strategies, are better placed to manage threats and intrusions. Each of the selected agencies had taken varying steps to implement the remaining 31 controls from the *Top 35 mitigation strategies against cyber intrusions* promulgated by ASD. However, security gaps were known by management in each of the selected agencies. To strengthen their ICT security posture, agencies should conduct annual threat assessments across their ICT systems, having regard to the Top 35 mitigation strategies; and implement periodic review by the agency security executive of the overall ICT security posture.

Recommendation No.3

5.23 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.

Australian Bureau of Statistics response:

5.24 *Agreed. The ABS has implemented processes to review annually the agency's compliance with the controls that are mandated in the Australian Signals Directorate's* Top 35 Mitigation Strategies.

5.25 *The ABS has well established internal governance arrangements that include a Protective Security Management Committee that conducts a periodic assessment of the agency's overall security posture.*

Australian Customs and Border Protection Service response:

5.26 *Agreed.*

Australian Financial Security Authority response:

5.27 *Agreed.*

Australian Taxation Office response:

5.28 *Agreed.*

Department of Foreign Affairs and Trade response:

5.29 *Agreed.*

Department of Human Services response:

5.30 *Agreed. The department undertakes accreditation of its ICT systems in accordance with ISM guidance and continuously assesses the department's ICT security posture.*

IP Australia response:

5.31 *Agreed. IP Australia will conduct regular assessments with regard to the Top 35 Mitigation Strategies to ensure a continuous improvement program is in place. IP Australia will conduct annual threat assessments which will be subject to the availability of funding and other threat assessments being conducted.*

5.32 *IP Australia's agency security executive will implement periodic assessment and review of its overall ICT security posture.*

Ian McPhee — Canberra ACT

Auditor-General — 24 June 2014

Appendices

Appendix 1: Agency responses to the proposed report

GED
5 JUN 2014
9.30

Australian Bureau of Statistics

ABN: 26 331 428 522

ABS House
45 Benjamin Way
Belconnen ACT 2617

Locked Bag 10
Belconnen ACT 2616

Telephone: (02) 6252 5000
Facsimile: (02) 6251 6009

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou

Cyber Attacks: Securing Agencies' ICT Systems

Thank you for your letter to Mr Jonathan Palmer of 12 May 2014 to inform the Australian Bureau of Statistics (ABS) of the proposed cross-agency audit report on *Cyber Attacks: Securing Agencies' IT Systems* .

In that letter you requested that the ABS provide a formal response to the proposed report and a response to each of the report's recommendations.

Response to Each of the Report's Recommendations

Recommendation No. 1	**Australian Bureau of Statistics response**
2.33 To achieve full compliance with the mandatory ISM 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.	**2.34** Agree. As indicated in the report, the agency is well placed in terms of its compliance with the top four ISM controls. Where full compliance has not been possible due to technical constraints imposed by a small number of legacy systems, mitigations have been put in place to reduce the risks associated with the use of these.
Recommendation No. 2	**Australian Bureau of Statistics response**
4.63 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.	**4.64** Agree. The ABS has, where practical, eliminated the use of shared accounts. Where this has not been possible, mitigations have been put in place to reduce risks associated with the use of shared accounts. The ABS has implemented an ongoing program of work to enhance audit logging and monitoring activities associated with the use of privileged user accounts.

Recommendation No. 3	Australian Bureau of Statistics response
5.23 To strengthen their ICT security posture, the ANAO recommends that agencies: (a) conduct annual threat risk assessments across ICT systems, having regard to the *Top 35 Mitigation 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.	**5.24** Agree. The ABS has implemented processes to review annually the agency's compliance with the controls that are mandated in the Australian Signals Directorate's *Top 35 Mitigation Strategies*. The ABS has well established internal governance arrangements that include a Protective Security Management Committee that conducts a periodic assessment of the agency's overall security posture.

Formal Response to the Proposed Report

Appendix 1: Agency responses to the proposed report

Australian Bureau of Statistics (ABS)

The ABS agrees that the report is an accurate assessment of the agency's compliance state as of 30 November 2013 and of the agency's planned state for 30 June 2014.

The ABS supports the recommendations of the report and notes that the agency is well placed in terms of its compliance with the top four ISM controls.

The audit has identified some areas for improvement and the agency has established programs of work to implement these recommendations. Where full compliance has not been possible due to technical constraints imposed by a small number of legacy systems, mitigations have been put in place to reduce the risks associated with the use of these.

Thank you for the opportunity to provide responses to this report.

Yours sincerely

Peter Harper
Deputy Australian Statistician
Population, Labour and Social Statistics Group

3 June 2014

GED
5 JUN 2014
9.30

Australian Government
Australian Customs and Border Protection Service

Chief Executive Officer

Customs House
5 Constitution Avenue
Canberra City ACT 2601

Phone: 02 6275 6800
Email: ESU@customs.gov.au

Dr Tom Ioannou 5/6
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou

Proposed cross-agency audit report on Cyber Attacks: Securing Agencies' ICT Systems.

Thank you for the opportunity to review and comment on your proposed report to Parliament on the status of the cyber security posture of the sampled agencies and our collective and individual compliance with the Australian Signals Directorate (ASD) Top Four controls.

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 Australian Customs and Border Protection Service agrees with the three recommendations (attached) and is enhancing its security culture to address the growing cyber threat. Underpinned by clear policy, supported by security aware leadership the security team has a mandate to achieve compliance with the ASD Top 35.

Yours sincerely

Michael Pezzullo
Chief Executive Officer

31 May 2014

Australian Government

Australian Financial Security Authority

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou

RE: AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE AUDIT OF CYBER ATTACKS: SECURING AGENCIES' ICT SYSTEMS

Thank you for your letter dated 12 May 2014 and for affording AFSA the opportunity to provide comments on the proposed report.

AFSA agrees with the three recommendations contained in section 19 of the report.

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

AFSA would like to thank the Australian National Audit Office for the professionalism and cooperation of their Audit team whilst working on this matter. AFSA is looking forward to continuing this relationship into future audits.

Regards

Gavin McCosker

02 June 2014

Australian Government
Australian Taxation Office

Second Commissioner of Taxation

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou

RE: AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE AUDIT OF CYBER ATTACKS: SECURING AGENCIES' ICT SYSTEMS

Thank you for your letter dated 12 May 2014 and for the opportunity to provide comments on the proposed report on *Cyber Attacks: Securing Agencies' ICT Systems*.

The ATO agrees with the three recommendations contained in the section 19 report.

Attached is the ATO response to the recommendations (Annexure 1) and a 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 Laurie McNeill, Executive Advisor to Bill Gibson, Chief Information Officer, on (02) 6216 3912.

Yours sincerely

Geoff Leeper

21 May 2014

T +61 (0)2 6216 1111 PO Box 900 Civic Square ACT 2608 Australia ato.gov.au

10 JUN 2014

Australian Government

Department of Foreign Affairs and Trade

Secretary

Telephone: 02 6261 2472
Facsimile: 02 6273 2081

3 June 2014

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Dr Ioannou

RE: AUSTRALIAN NATIONAL AUDIT OFFICE PERFORMANCE AUDIT OF CYBER ATTACKS: SECURING AGENCIES' ICT SYSTEMS

Thank you for your letter dated 12th May 2014 on the proposed report on *Cyber Attacks: Securing Agencies' ICT Systems.*

DFAT welcomes the opportunity to comment on the report and agrees with the three recommendations in the report.

The DFAT response to the recommendations is attached along with a summary of our comments to be included in the report.

I would like to thank the Australian National Audit Office team for the professional approach they used in their engagement with us and look forward to using their findings to improve our security posture.

Please contact Mr Tuan Dao, Chief Information Officer, on (02) 6261 2142 or Ms Paula Ganly Chief Information Security Officer on (02) 6261 2556 if you require further information on this matter.

Yours sincerely

Peter N Varghese AO

R G Casey Building, Barton ACT 0221 www.dfat.gov.au

Australian Government

Department of Human Services

Kathryn Campbell CSC
Secretary

Ref: EC14/172

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear ~~Dr Ioannou~~ Tom

Thank you for the opportunity to comment formally on the proposed 'section 19' report arising from the Australian National Audit Office's (ANAO) performance audit of *Cyber Attacks: Securing Agencies' IT Systems*, dated 12 May 2014.

The Department of Human Services (the department) agrees with the ANAO's recommendations.

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

If you would like to discuss the department's response, please do not hesitate to contact Mr Mike Brett, General Manager - ICT Infrastructure, on (02) 6143 6400 or by email mike.brett@humanservices.gov.au.

Yours sincerely

Kathryn Campbell

5 June 2014

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

Australian Government
IP Australia

ABN 38 113 072 755
Discovery House, Phillip ACT 2606
PO Box 200, Woden ACT 2606
Australia

P 1300 651 010
Int +61 2 6283 2999
www.ipaustralia.gov.au

5 June 2014

Dr Ioannou
Group Executive Director
Performance Audit Services Group
Group Executive Director
GPO Box 707
CANBERRA ACT 2601

Cross-agency audit report on Cyber Attacks: Securing Agencies' ICT Systems

Dear Dr Ioannou,

Thank you for the proposed audit report on Cyber Attacks: Securing Agencies' ICT Systems. We have reviewed the report and our response is provided below. As requested we have included our formal response to the overall report and a response to each of the three recommendations.

Formal summary response Para 51, Page 23 –

IP Australia welcomes this report and considers that implementation of the recommendations will enhance the security of its ICT systems. IP Australia agrees with the recommendations in the report and has in place a plan to further strengthen its capability in all these areas. An action plan to address compliance with the Top 4 Strategies is already underway and these recommendations will be added to that plan.

IP Australia has reviewed and is actively working to improve its security posture within a timeframe and resource envelope that can be managed based on its cost recovery model of operation. A risk based approach has been used to prioritise improvements to security and to ensure the highest vulnerabilities are addressed first. With its increase in online services, the increasing threat environment, and the increase in compliance requirements, IP Australia has increased ICT Security resources and initiatives to improve its overall security posture.

Section 2.40, Page 53 – Recommendation No. 1

Agreed. IP Australia has a plan in place to improve its capability in this area. It will complete activities in train and following annual reviews, progressively strengthen its compliance with the top four ISM controls.

Robust intellectual property rights delivered efficiently

Section 4.70, Page 96 – Recommendation No. 2

Agreed. IP Australia will implement Recommendation 2 as part of its plan to improve its security posture.

Section 5.30, Page 104 – Recommendation No. 3

Agreed. IP Australia will conduct regular assessments with regard to the Top 35 Mitigation Strategies to ensure a continuous improvement program is in place. IP Australia will conduct annual threat assessments which will be subject to the availability of funding and other threat assessments being conducted.

IP Australia's agency security executive will implement periodic assessment and review of its overall ICT security posture.

If you require any clarification please contact our CIO David Johnson on (02) 62832008 or david.johnson@ipaustralia.gov.au.

Yours sincerely,

Patricia Kelly
Director General
IP Australia

GED
6 JUN 2014
2.45

Australian Government
Department of Defence
Intelligence & Security

Australian Signals Directorate

Cyber & Information Security
Division
PO Box 5076
KINGSTON ACT 2604
☎: (02) 6265 0555
: joe.franzi@defence.gov.au

ASD/40010/2014

Dr Tom Ioannou TI 6/6
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Dear Dr Ioannou

Proposed cross-agency audit report on Cyber Attacks: Securing Agencies' ICT Systems

Thank you for your letter of 13 May 2014, inviting the Australian Signals Directorate's (ASD) response to the ANAO proposed cross-agency report on Cyber Attacks: Securing Agencies' ICT Systems.

ASD welcomes the ANAO's audit report which assesses select agencies' compliance with the Top 4 Strategies to Mitigate Targeted Cyber Intrusions. ASD is committed to influencing decision making across government on cyber security issues.

ASD endorses the report's recommendations. Please find attached ASD's formal response at Enclosure 1 and general editorial comments at Enclosure 2.

If you require further information on this matter, please contact Yvette Tam, Deputy Director Cyber Security Relationships on (02) 6266 0031.

Yours sincerely,

Joe Franzi
Assistant Secretary Cyber Security

6 June 2014

Enclosure:

1. Australian Signals Directorate's response to the Australian National Audit Office Proposed Cross-Agency Audit Report on Cyber Attacks: Securing Agencies' ICT Systems.
2. Editorial and General Comments

Appendix 2: Audit criteria and compliance statements

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

Application whitelisting

- 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.
- Ensure that the default policy is to deny the running of software.

Patching applications and operating systems

- 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 critical security vulnerability.
- Implement 'alternate' controls where known vulnerabilities cannot be patched, or security patches are not available.

Minimising domain and local administrative privileges

- 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.
- 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 criteria two and three, 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
• 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. • Changes are successfully implemented or rolled back.	
Criterion Three:	**Approved dispensations are in place for any non-compliance with the mandatory ISM controls**
• Controls not in place are identified and reported to the Agency Head. • Where a control is not in place, a dispensation is authorised by the Agency Head.	

Source: ANAO.

Index

A

Access controls

grant, suspend and revoke accounts, 85, 88

identify, authenticate and authorise accounts, 86, 88, 91, 93

log and review the activities of privileged accounts, 87, 89, 92, 94

logical access, 46, 47, 50, 57, 83–90, 93, 99

management of privileged accounts, 86, 89, 91, 94

multi–factor authentication, 86, 87, 92, 94

passphrases, 77, 81, 86, 89, 91, 93

privileged user accounts, 44, 50, 53, 54, 64, 77–94

shared accounts, 80, 86, 91, 92

standard user accounts, 78–79, 85, 88

Agency Compliance Grade, 48, 55, 57

Application whitelisting, 39, 50, 52, 53, 60, 61–67

AppLocker, 66–67

audit only mode, 53, 64, 67, 81

certificate–based rules, 65

path–based rules, 65, 81

Attorney–General's Department (AGD), 35, 43, 104

Audit logs, 54, 67, 82, 87, 89, 92, 94, 95

Australia's National Security Strategy, 40

Australian Cyber Security Centre (ACSC), 40

Australian Government Cyber Security Strategy, 34

Australian Government Information Security Manual (ISM), 36, 37, 38, 41, 42, 43, 44, 46, 50, 52, 55, 58, 60, 61, 65, 66, 75, 78, 81, 86, 87, 89, 91, 93, 98, 99, 101, 104, 105

Australian Government Protective Security Policy, 46, 60

Australian Public Service Information and Communications Technology Strategy, 33

Australian Signals Directorate (ASD), 36, 37, 38, 44, 54, 60, 61, 68, 70, 72, 75, 76, 77, 78, 79, 80, 83, 98, 104, 107

B

Breaches and disclosures, 48, 52, 57, 58, 89, 99, 101

C

Change management, 44, 46, 47, 50, 53, 54, 57, 68, 71, 75, 83, 94–99, 101

authorised changes, 96

Change Advisory Board, 96, 97, 98, 99

emergency change, 95, 96, 98, 99

made in a timely manner, 97

standard change, 97, 99

tested before implementation, 97

Cyber

attacks, 34, 52, 58, 66, 81, 87, 99, 101, 102, 104, 106

intrusions, 33, 34, 35, 38, 68

resilience, 101, 102, 106

security, 35, 40, 77, 102, 103, 106

Cyber Security Operations Centre, 34

D

Defence White Paper, 40

F

Financial Management Information Systems (FMIS), 65, 69, 72, 87–94

G

Group policies, 53, 54, 64, 65, 67, 79, 80, 89, 92, 94

H

Human Resource Management Information Systems (HRMIS), 69, 72, 87–94

I

ICT security measures, 84, 89, 104

ICT security posture, 35, 42, 43, 48, 57, 101–7

ICT security zones

cyber secure zone, 47–52, 57, 58

externally secure zone, 47–52, 57

internally secure zone, 47–52, 57, 58

vulnerable zone, 47–52, 57

Information management systems

Human Resource Management Information Systems (HRMIS), 65

Information security directive (INFOSEC 4), 38, 50, 60

IT general controls, 41, 43, 44, 46, 47, 48, 52, 54, 57, 58, 83, 82–99, 101

K

Key ICT security appointments, 44, 103

M

Mandated ISM strategies and related controls

Top Four mitigation strategies, 38, 39, 43, 44, 46, 47, 48, 50, 52, 54, 55, 57, 60, 61, 81, 82, 101, 105, 107

Minimise administrative privileges. *See* Restrict administrative privileges

P

Patch management strategy, 53, 69, 71, 73, 75, 76, 82

Patches. *See* Security patching

Patching applications, 39, 60, 68–73

Patching operating systems, 39, 60, 73–77

Post implementation review, 98

Protective Security Governance Guidelin*es*, 43

Protective Security Policy Framework (PSPF), 36, 38, 39, 43, 44, 46, 50, 52, 54, 55, 58, 60, 102, 105

R

Restrict administrative privileges, 39, 50, 60, 77–81, 82

S

Security

awareness, 67, 102, 103, 106

critical security patches, 39, 53, 69, 72, 73, 76, 81

culture, 36, 103

patching, 50, 53, 60, 68, 69, 71, 73, 75, 82, 95, 97, 98

risk, 35, 36, 37, 38, 68, 76

vulnerabilities, 39, 53, 69, 73, 82

Security personnel. *See* Key ICT security appointments

T

Top 35 Strategies to Mitigate Targeted Cyber Intrusions, 44, 102, 104, 106, 107

Series Titles

ANAO Audit Report No.1 2013–14
Design and Implementation of the Liveable Cities Program
Department of Infrastructure and Transport

ANAO Audit Report No.2 2013–14
Administration of the Agreements for the Management, Operation and Funding of the Mersey Community Hospital
Department of Health and Ageing
Department of Health and Human Services, Tasmania
Tasmanian Health Organisation – North West

ANAO Audit Report No.3 2013–14
AIR 8000 Phase 2 — C-27J Spartan Battlefield Airlift Aircraft
Department of Defence

ANAO Audit Report No.4 2013–14
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2012 Compliance)
Across Agencies

ANAO Audit Report No.5 2013–14
Administration of the Taxation of Personal Services Income
Australian Taxation Office

ANAO Audit Report No.6 2013–14
Capability Development Reform
Department of Defence

ANAO Audit Report No.7 2013–14
Agency Management of Arrangements to Meet Australia's International Obligations
Across Agencies

ANAO Audit Report No.8 2013–14
The Australian Government Reconstruction Inspectorate's Conduct of Value for Money Reviews of Flood Reconstruction Projects in Queensland
Department of Infrastructure and Regional Development

ANAO Audit Report No.9 2013–14
Determination and Collection of Financial Industry Levies
Australian Prudential Regulation Authority
Department of the Treasury

ANAO Audit Report No.10 2013–14
Torres Strait Regional Authority — Service Delivery
Torres Strait Regional Authority

ANAO Audit Report No.11 2013–14
Delivery of the Filling the Research Gap under the Carbon Farming Futures Program
Department of Agriculture

ANAO Report No.12 2013–14
2012–13 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.13 2013–14
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2013
Across Agencies

ANAO Audit Report No.14 2013–14
Explosive Ordnance and Weapons Security Incident Reporting
Department of Defence

ANAO Audit Report No.15 2013–14
The Indigenous Land Corporation's Administration of the Land Acquisition Program
Indigenous Land Corporation

ANAO Audit Report No.16 2013–14
Administration of the Smart Grid, Smart City Program
Department of the Environment
Department of Industry

ANAO Audit Report No.17 2013–14
Administration of the Strengthening Basin Communities Program
Department of the Environment

ANAO Audit Report No.18 2013–14
Administration of the Improving Water Information Program
Bureau of Meteorology

ANAO Audit Report No.19 2013–14
Management of Complaints and Other Feedback
Australian Taxation Office

ANAO Audit Report No.20 2013–14
Management of the Central Movement Alert List: Follow-on Audit
Department of Immigration and Border Protection

ANAO Report No.21 2013–14
Pilot Project to Audit Key Performance Indicators

ANAO Audit Report No.22 2013–14
Air Warfare Destroyer Program
Department of Defence
Defence Materiel Organisation

ANAO Audit Report No.23 2013–14
Policing at Australian International Airports
Australian Federal Police

ANAO Audit Report No.24 2013–14
Emergency Defence Assistance to the Civil Community
Department of Defence

ANAO Audit Report No.25 2013–14
Management of the Building Better Regional Cities Program
Department of Social Services
Department of the Environment

ANAO Audit Report No.26 2013–14
Medicare Compliance Audits
Department of Human Services

ANAO Audit Report No.27 2013–14
Integrity of Medicare Customer Data
Department of Human Services

ANAO Audit Report No.28 2013–14
Review of Child Support Objections
Department of Human Services
Department of Social Services

ANAO Audit Report No.29 2013–14
Regulation of Commonwealth Radiation and Nuclear Activities
Australian Radiation Protection and Nuclear Safety Agency

ANAO Audit Report No.30 2013–14
Administering the Code of Good Manufacturing Practice for Prescription Medicines
Department of Health

ANAO Audit Report No.31 2013–14
The Australian Electoral Commission's Storage and Transport of Completed Ballot Papers at the September 2013 Federal General Election
Australian Electoral Commission

ANAO Audit Report No.32 2013–14
Delivery of the Hearing Community Service Obligation
Department of Health
Department of Human Services
Australian Hearing Services

ANAO Audit Report No.33 2013–14
Indigenous Employment in Australian Government Entities
Across Agencies

ANAO Audit Report No.34 2013–14
Implementation of ANAO Performance Audit Recommendations
Department of Agriculture
Department of Human Services

ANAO Audit Report No.35 2013–14
Managing Compliance of High Wealth Individuals
Australian Taxation Office

ANAO Audit Report No.36 2013–14
The Administration of the Parliamentary Budget Office
Parliamentary Budget Office

ANAO Audit Report No.37 2013–14
Management of Services Delivered by Job Services Australia
Department of Employment

ANAO Audit Report No.38 2013–14
Establishment and Administration of the National Offshore Petroleum Safety and Environmental Management Authority
National Offshore Petroleum Safety and Environmental Management Authority

ANAO Audit Report No.39 2013–14
Compliance Effectiveness Methodology
Australian Taxation Office

ANAO Audit Report No.40 2013–14
Trials of Intensive Service Delivery
Department of Human Services

ANAO Audit Report No.41 2013–14
Commercialisation Australia Program
Department of Industry

ANAO Audit Report No.42 2013–14
Screening of International Mail
Department of Agriculture
Australian Customs and Border Protection Service

ANAO Audit Report No.43 2013–14
Managing Compliance with Environment Protection and Biodiversity Conservation Act 1999 Conditions of Approval
Department of the Environment

ANAO Audit Report No.44 2013–14
Interim Phase of the Audits of the Financial Statements of Major General Government Sector Agencies for the year ending 30 June 2014
Across Agencies

ANAO Audit Report No.45 2013–14
Initiatives to Support the Delivery of Services to Indigenous Australians
Department of Human Services

ANAO Audit Report No.46 2013–14
Administration of Residential Care Payments
Department of Veterans' Affairs

ANAO Audit Report No.47 2013–14
Managing Conflicts of Interest in FMA Agencies
Across Agencies

ANAO Audit Report No.48 2013–14
Administration of the Australian Business Register
Australian Taxation Office
Australian Securities and Investments Commission
Department of Industry

ANAO Audit Report No.49 2013–14
Management of Physical Security
Australian Crime Commission
Geoscience Australia
Royal Australian Mint

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

Better Practice Guides

The following Better Practice Guides are available on the ANAO website:

Administering Regulation	June 2014
Implementing Better Practice Grants Administration	Dec. 2013
Human Resource Management Information Systems: Risks and controls	June 2013
Preparation of Financial Statements by Public Sector Entities	June 2013
Public Sector Internal Audit: An investment in assurance and business improvement	Sept. 2012
Public Sector Environmental Management: Reducing the environmental impacts of public sector operations	Apr. 2012
Developing and Managing Contracts: Getting the right outcome, achieving value for money	Feb. 2012
Public Sector Audit Committees: Independent assurance and advice for chief executives and boards	Aug. 2011
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities: Delivering agreed outcomes through an efficient and optimal asset base	Sept. 2010
Planning and Approving Projects – an Executive Perspective: Setting the foundation for results	June 2010
Innovation in the Public Sector: Enabling better performance, driving new directions	Dec. 2009
SAP ECC 6.0: Security and control	June 2009
Business Continuity Management: Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Fairness and Transparency in Purchasing Decisions: Probity in Australian Government procurement	Aug. 2007
Implementation of Programme and Policy Initiatives: Making implementation matter	Oct. 2006