[P.P.4S

Government
of South Australia

Report

of the

Auditor-General

Supplementary Report

for the

year ended 30 June 2016

Tabled in the House of Assembly and ordered to be published, 15 November 2016

Second Session, Fifty-Third Parliament

Security management of information systems: November 2016

By authority: P. McMahon, Government Printer, South Australia

2016

General enquiries regarding this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000

Website: www.audit.sa.gov.au

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
DX 56208
Victoria Square
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

14 November 2016

The Hon R P Wortley MLC
President
Legislative Council
Parliament House
ADELAIDE SA 5000

The Hon M J Atkinson MP
Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

Report of the Auditor-General: Supplementary Report for the year ended 30 June 2016: Security management of information systems: November 2016

As required by the *Public Finance and Audit Act 1987*, I present to each of you my Supplementary Report for the year ended 30 June 2016 'Security management of information systems: November 2016'.

Content of the Report

Part A of the Auditor-General's Annual Report for the year ended 30 June 2016 referred to audit work that would be subject to Supplementary reporting to Parliament. This report provides detailed commentary and audit observations on the review of key components of information security management at 10 SA Government agencies to determine whether the sampled agencies were effectively managing information security in the certain areas.

Acknowledgements

The audit team for this report was Andrew Corrigan, James Baker and Brenton Borgman.

I also express my appreciation for the cooperation and assistance provided by the staff of the 10 SA Government agencies reviewed during the course of the audit.

Yours sincerely

Andrew Richardson
Auditor-General

Table of contents

Security management of information systems: November 2016

1 Executive summary 1
- 1.1 Introduction 1
- 1.2 Audit conclusion 1
- 1.3 Key audit findings 2
- 1.4 Recommendations 3
- 1.5 Agency responses 4

2 Background 5
- 2.1 Overview 5
- 2.2 Recent information security trends 6
- 2.3 Frameworks and best practice guidance 6
- 2.4 Information security responsibilities 9

3 Audit objective and scope 11
- 3.1 Objective 11
- 3.2 Audit scope 11
- 3.3 Agencies reviewed 11
- 3.4 Attribution of review findings 12
- 3.5 Limitations 12

4 Legacy servers 13
- 4.1 Introduction 13
- 4.2 Mitigating controls to protect legacy servers 14
- 4.3 Audit approach 14
- 4.4 Agencies operate unsupported legacy servers 15
- 4.5 Insufficient mitigating controls applied to protect legacy servers 19

5 Patch management 21
- 5.1 Introduction 21
  - 5.1.1 Background 21
  - 5.1.2 Responsibilities for patch management 22
  - 5.1.3 Prior year reviews of patch management 23
- 5.2 Audit approach 23
- 5.3 Servers identified with missing operating system security update patches 23
- 5.4 Servers identified with missing database security update patches 25
- 5.5 Core information system application, database and operating system not patched at one agency 26
- 5.6 No documented policies or procedures for patch management or change management 27
- 5.7 IT policies and procedures not reviewed promptly 28
- 5.8 Regular monitoring of patching compliance was behind schedule and does not assess all servers and workstations 29
- 5.9 Insufficient documentation of patching exemptions 30
- 5.10 Patch compliance reports not available for servers 30

Table of contents

6 Privileged user access management 32
6.1 Introduction 32
6.2 Audit approach 33
6.3 Domain-level privileged access not effectively managed 34
6.4 Excessive access granted to local administrators 36
6.5 No formal periodic review of Active Directory privileged users 37
6.6 User access and IT security policy/procedure deficiencies 38
6.7 Terminated employee reports not received or reviewed promptly 39
6.8 Findings from Microsoft review of Active Directory environment not yet remediated 40
6.9 Privileged user activities not sufficiently logged and monitored 41
7 Mobile devices 43
7.1 Introduction 44
7.1.1 Background 44
7.1.2 Mobile device data access methods 44
7.1.3 Recommended security controls 45
7.2 Audit approach 46
7.3 Security controls applied to mobile devices do not meet best practice guidelines 46
7.4 Mobile device access not restricted by individual device 47
7.5 Security controls applied to Outlook Web Access could be strengthened 48
7.6 Insufficient reporting of agency mobility usage 50
7.7 Mobile device policies and procedures not regularly reviewed or approved 50
8 Application whitelisting 52
8.1 Introduction 52
8.2 Audit approach 53
8.3 Application whitelisting not implemented at two agencies 54
8.4 No documentation or approval recorded for a software installation 55
8.5 Periodic application reviews not performed and documentation not retained 56
8.6 Information security procedures and guidelines in draft status 57
9 Additional issues identified 58
9.1 Introduction 58
9.2 Additional areas of non-compliance with the Top 10 objectives identified at one agency 58
9.3 Progress of implementing Top 10 objectives were not reported to the Office for Digital Government at one agency 59

1 Executive summary

1.1 Introduction

Information systems play a crucial role in storing, processing, modifying and transmitting agency financial data. SA Government agencies increasingly rely on these systems to deliver their core services. They are also entrusted with increasing amounts of data.

Accordingly, SA Government agencies need to implement sufficient information security controls to reduce exposure to a range of security threats.

The number, type and sophistication of cyber security threats to Australia continues to increase. Within the SA Government, agencies have increased their reporting of security events and incidents. Reported SA Government events and incidents increased by 49% between January and July 2016.

In 2015-16, we reviewed key components of information security management at 10 SA Government agencies. Our audit objective was to determine whether the sampled agencies were effectively managing information security in the areas shown in figure 1.1.

Figure 1.1: Information security components included in our review

Legacy servers	A server using an outdated computer operating system that needs either upgrading or replacing, as it no longer receives vendor security patches.
Patch management	A piece of software that is designed to fix defects or vulnerabilities, or provide updates to an information system.
Privileged user access management	Users with privileged access permissions have the ability to access sensitive data and change security settings within agency systems. Accordingly, this access needs to be appropriately restricted and monitored.
Mobile devices	Includes devices such as smartphones and tablets. Before connecting to agency networks, certain security controls should be applied to avoid exposure or inappropriate transfer of sensitive agency data.
Application whitelisting	Designed to protect against unauthorised and malicious programs executing on a computer. Only specifically selected programs and software libraries can be executed, based on a predefined whitelist.

This assessment was based on a combination of mandated SA Government requirements and best practice guidelines (refer section 2.3).

We reviewed legacy servers at all 10 agencies. For the other components, we selected subsets of different agencies for our testing.

1.2 Audit conclusion

We found that agencies are not effectively managing several key components of information security included in our review scope.

The deficiencies and opportunities for improvement that we identified increase risks to the confidentiality, integrity and availability of government agencies' systems and data.

Eight of the 10 agencies we reviewed were operating unsupported legacy servers, with several not implementing sufficient mitigating controls. However, we noted that all agencies were working to decommission these legacy servers.

Two of the four agencies we reviewed had not effectively managed operating system and database patching. In addition, neither of these agencies had effectively managed privileged user access in line with mandated requirements and best practice guidance.

We also identified several opportunities for improvement in whole-of-government mobile device controls. Finally, we confirmed that two agencies had not implemented suitable controls to secure their workstations from running unapproved software.

1.3 Key audit findings

Agencies operating unsupported legacy servers (section 4)

Eight of the 10 agencies we reviewed were operating unsupported legacy servers (as at August/September 2016). We identified 233 legacy servers in operation across the 10 agencies (13% of all servers operating at these agencies).

All agencies are working to decommission these legacy servers. However, the risk exposure and extent of mitigating controls applied to protect these servers varies between agencies. Several agencies have not implemented sufficient mitigating controls in the interim.

Two of the four agencies reviewed were not effectively managing patching (section 5)

Most agencies we reviewed had defined policies and procedures to manage the patching process. However, we identified servers with missing operating system or database security update patches at three of the four agencies reviewed. Additionally, we identified that:

- a core information system application, database and operating system was not patched at one agency
- two agencies had deficiencies in their patch management and change management policies/procedures
- there were deficiencies in patching compliance checking processes and reporting
- there was insufficient documentation of patching exemptions at one agency.

Agencies were not effectively managing privileged user access to Active Directory (section 6)

The two agencies we reviewed were not effectively managing privileged user access to Active Directory in line with the Information Security Management Framework requirements (refer

section 2.3). We noted instances of potentially excessive domain-level privileged access and privileged access permissions on local computers. We also identified that:

- no formal periodic review of Active Directory privileged users
- deficiencies in user access and IT security policy/procedure(s)
- terminated employee reports were not received or reviewed promptly
- privileged user activities were not sufficiently logged and monitored.

Security controls applied to mobile devices do not meet best practice guidelines (section 7)

The two agencies we reviewed should improve controls to effectively manage the use of mobile devices to access agency resources and data. Although both agencies had defined policies and procedures to manage mobile devices, we identified that:

- security controls applied to mobile devices did not meet best practice guidelines
- mobile access was not restricted by individual device
- security controls applied to Outlook Web Access could be strengthened
- there was insufficient reporting of agency mobility usage
- mobile devices policies and procedures were not regularly reviewed or approved.

We confirmed that a number of mobile device controls are managed at the whole-of-government level. Accordingly, most of the issues we identified may also apply to other agencies.

Agencies have not implemented application whitelisting (section 8)

We reviewed two agencies and confirmed that neither had implemented application whitelisting. However, one agency was actively considering this after a recent security incident involving a malicious application. We also identified that:

- no documentation or approval was recorded for a software installation at one agency
- periodic application reviews are not performed at one agency and documentation of them is not retained at another agency
- information security policies at one agency are in draft, pending review and approval.

1.4 Recommendations

We made a series of recommendations to each agency reviewed to address the issues identified. These included:

- continuing to decommission legacy servers and considering implementing additional mitigating controls
- strengthening controls to identify, implement, document and monitor patches
- improving policy and procedure coverage across the areas reviewed
- implementing additional restrictions to privileged user accounts and regular account reviews to meet Information Security Management Framework requirements

- assessing whether agencies should implement additional controls and regular reporting processes for mobile devices
- implementing application whitelisting on servers and workstations, as well as regular software reviews.

Sections 4 to 9 detail our recommendations.

1.5 Agency responses

In their responses, most agencies advised us that they had decommissioned additional legacy servers since our audit. Most were planning to decommission all remaining legacy servers as soon as possible. Time frames for completing this varied between agencies.

Most agencies also agreed with our recommendations regarding implementing additional security controls to protect their legacy servers. However, a number of agencies are focused mainly on decommissioning the servers.

Two agencies advised us that they believe the risks that application whitelisting or other mitigating controls are designed to manage are unlikely to arise. One of these confirmed that the remaining legacy servers are behind two firewalls and are not directly accessible via the internet.

Agencies are also assessing the feasibility of our recommendations regarding improvements to mobile device security controls.

The Department of the Premier and Cabinet and the other agencies we reviewed advised us that they would assess the availability of technical controls to implement our recommendations regarding implementing additional security controls for mobile devices. They will assess the costs and benefits of these controls in consultation with an external vendor.

Agencies responded positively to our remaining review findings and recommendations with details of planned remediation.

Sections 4 to 9 provide additional details of agency responses.

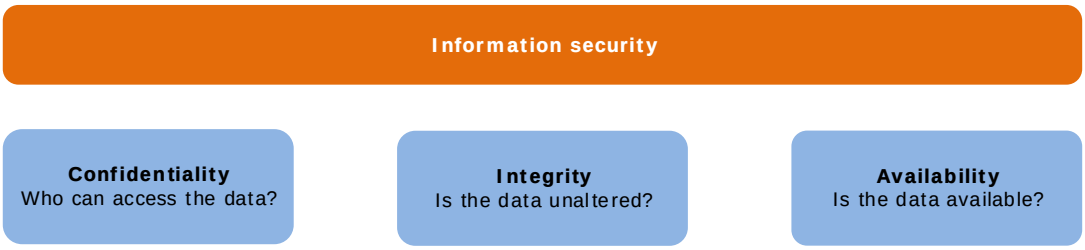
2 Background

2.1 Overview

Information security refers to processes and methodologies designed and implemented to protect any form of confidential, private and sensitive information from unauthorised access, use, disclosure, disruption, modification or destruction.[1]

Agencies need to implement sufficient information security controls to ensure the confidentiality, integrity and availability of their systems and data.

Figure 2.1: Overview of key information security concepts



SA Government systems and data are exposed to many different security threats,[2] including those shown in figure 2.2.

Figure 2.2: Examples of security threats to SA Government systems and data

Malware	Malicious software designed to facilitate unauthorised access, damage or disruption to a system.
Ransomware (including Cryptolocker)	Extortion through malware that locks a computer's content and requires victims pay a ransom to regain access.
Denial of Service attacks	Attempts to prevent legitimate access to online services (typically a website) by consuming the amount of available bandwidth, or the processing capacity of the computer hosting the online service.
Cyber intrusion (or hacking)	A successful attempt by a cyber adversary to gain access to a computer or device without the owner's permission.
Spear phishing (socially engineered emails)	Emails targeting specific people, often containing a hyperlink or an attachment. When opened, they attempt to download malicious code to a workstation to enable a cyber adversary to conduct further malicious activities.

1 SANS Institute 2016, *Information security resources*, viewed 1 November 2016, <https://www.sans.org/information-security/>.

2 *Threat report* 2015, Australian Cyber Security Centre, viewed 1 November 2016, <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf>.

2.2 Recent information security trends

Australia

The number, type and sophistication of cyber security threats to Australia continues to increase. Between January 2015 and June 2016, the Australian Signals Directorate (ASD), an intelligence agency in the Australian Government Department of Defence, responded to 1095 cyber security incidents on Australian Government systems. These events were considered serious enough to warrant operational responses.[3]

SA Government

The number of reported security events and incidents affecting the SA Government continues to rise, increasing by 49% between January and July 2016.

However, this increase may not necessarily indicate increased activity targeting SA Government networks. It may instead highlight improvements in agencies' awareness and event detection and reporting.

Phishing and malware are the two largest reported categories and pose significant risks to government systems. Between January and July 2016, over 90% of reported SA Government malware incidents related to ransomware.

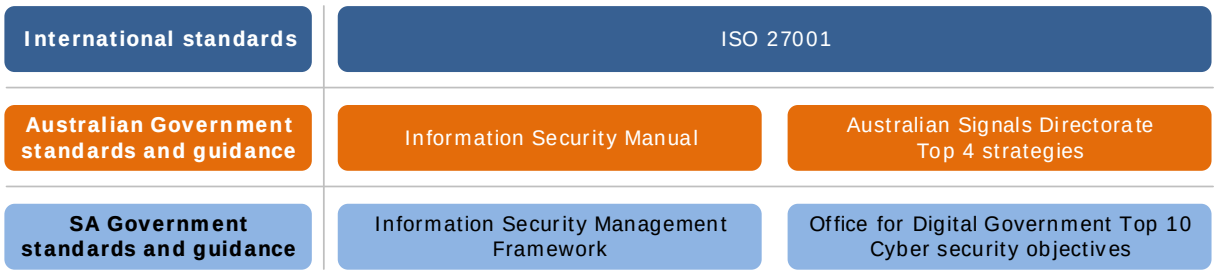
Reported denial of service attacks also increased during the same period. These attacks targeted websites and other online services hosted outside of the shared SA Government network, StateNet.

Over this period, several SA Government websites were also defaced. This is an attack on a website that changes the visual appearance of the site.

2.3 Frameworks and best practice guidance

There are a number of frameworks and best practice guidance for information security, including specific frameworks developed at the Australian and SA Government levels:

Figure 2.3: Frameworks and best practice guidance for information security



ISO 27001

ISO 27001[4] is an international specification detailing best practice requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

---

[3] *Threat report* 2016, Australian Cyber Security Centre, viewed 1 November 2016, <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf >.

[4] International Organisation for Standardisation 2016, *ISO/IEC 27001 – Information security management*, viewed 1 November 2016, <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.

An ISMS aims to preserve the confidentiality, integrity and availability of information by applying a risk management process. ISMS implementation also gives stakeholders confidence that organisations have adequately managed risks and fully understand and appreciate agency assets/systems. Stakeholder may also gain confidence through certification processes.

Australian Government Information Security Manual

The Information Security Manual is designed to help Australian Government agencies to apply a risk-based approach to protecting their information and systems.[5]

The manual supports the principles and strategic priorities outlined in the Australian Government's cyber security strategy. It includes information about specific cyber security threats and helps agencies to determine appropriate controls to protect their information communications technology (ICT) systems.

Although not directly applicable to SA Government agencies, the Information Security Manual serves as a reference for agencies to understand the types of controls they could implement to mitigate security risks.

Australian Signals Directorate Top 4

The ASD has developed a list of strategies to mitigate targeted cyber intrusion (or hacking). The list is informed by ASD's experience in operational cyber security.

The Top 4 mitigation strategies are shown in figure 2.4.:

Figure 2.4: Top 4 mitigation strategies

1. Application whitelisting	2. Patching applications
Using application whitelisting to help prevent malicious software and unapproved programs from running.	Patching applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office.
3. Patching operating systems	**4. Administrative privileges**
Patching operating system vulnerabilities and avoiding the use of legacy operating systems (such as Microsoft Windows XP or Windows Server 2003).	Restricting administrative privileges to operating systems and applications based on user duties.

The ASD's cyber security operations centre estimates that at least 85% of cyber intrusion techniques could be prevented by implementing the Top 4 mitigation strategies.

SA Government Information Security Management Framework (ISMF)

The ISMF addresses the SA Government's cyber security requirements and consists of 40 policies, supported by 140 standards. It is a risk-based approach that aligns with the Australian Government's Protective Security Policy Framework and ISO 27001.

---

[5] *Information Security Manual (Principles)* 2016, Australian Government Department of Defence, viewed 1 November 2016, <http://www.asd.gov.au/publications/Information_Security_Manual_2016_Principles.pdf>.

The ISMF supports contemporary industry practices to secure information stored, processed, transmitted or otherwise manipulated using ICT. The ISMF requires that agencies implement necessary control measures to adequately protect their information and associated assets.

The Department of the Premier and Cabinet (DPC) Circular PC030 'Protective Security Management Framework' requires SA Government agencies to comply with the ISMF.

SA Government Top 10 cyber security controls

In September 2015, Cabinet approved 10 cyber security resilience and preparedness objectives (the Top 10). These objectives focus on areas with the greatest impact on reducing the risks to agencies' ICT systems and enhancing system resilience.

The Top 10 objectives are shown in figure 2.5.

Figure 2.5: Top 10 cyber security resilience and preparedness objectives

Top 10 objective	Description
Administrative rights	Overall reduction, better management and reporting across government
Governance	Embed information security within corporate governance arrangements, increased accountability and informed decision making
Cyber security incident management	Increasing our capabilities, improving accountability, reporting and oversight
Information classification	Understanding the value of information and applying protection efforts accordingly
Patching operating systems	Reducing the opportunity for attackers to exploit known vulnerabilities
Patching applications	Better management of applications and software to reduce opportunity for attackers to exploit known vulnerabilities
Web security standards	Increasing resilience and better visibility, management and control
Penetration testing	Improved resilience of existing and new websites and web applications
ISMF progression	Expanding scope to include information assets that are important to the business and personally identifiable information
Protecting user environments	Reducing the likelihood and effectiveness of cyber intrusions and automatic compromise techniques

SA Government agencies were required to lodge Top 10 implementation plans with the Office for Digital Government (ODG), a division of DPC, by 2 May 2016.

After submitting their initial implementation plans, agencies report their progress in implementing the Top 10 objectives to the ODG through questionnaires. At the time of our review, agencies were required to report quarterly to the ODG. This subsequently changed to six-monthly reporting.

The ODG is also required to provide annual updates to Cabinet. These reports are based on the questionnaires completed by agencies and are not independently audited.

The ODG will review the Top 10 objectives annually and update these objectives as required to address emerging cyber security risks.

We reviewed results from the first quarter Top 10 report and found that:

- 33 of 45 agencies had reported their implementation progress to the ODG
- agencies reduced the number of accounts with administrative privileges from over 10 000 in 2013 to 6000 in 2016
- further work is required in several areas of privileged user access management.

We also confirmed that:

- one of the 10 agencies in our review had not yet reported its implementation progress to the ODG
- another agency had developed an action plan to only partially address its security deficiencies under the Top 10 requirements. Full compliance was not planned due to resourcing and other constraints.

Section 9 provides further details on Top 10 compliance.

2.4 Information security responsibilities

Within the SA Government, a number of government entities play a role in securing government systems and networks. These include the following.

Office for Digital Government

The ODG helps agencies to align with the strategic direction outlined in the SA Government's 'South Australia Connected' ICT strategy. This includes providing tools, strategies and policies to support agencies as they transform their services to digital.

The ODG also progresses the ICT security and resilience agenda outlined in the Top 10. This includes coordinating agencies' Top 10 progress updates and providing agencies with general guidance on information security issues.

The ODG's Watch Desk coordinates the across-government cyber security incident reporting scheme within South Australia. Agencies are required to report cyber security events and incidents to the Watch Desk.

The ODG is not responsible for resourcing or financing across-government information security programs.

Department of the Premier and Cabinet

DPC is the control agency for ICT failure. This involves coordinating agencies, suppliers and other stakeholders to return ICT operations to a normal state after a failure of government ICT services.

DPC also manages several across-government ICT contracts and the StateNet network, including whole-of-government firewall and security arrangements. Across-government ICT contracts include:

- the Messaging and Business Communication Services contract for email services
- the Distributed Computing Support Services contract. This involves agency servers being managed by an external contractor.

These contracts are designed to provide the SA Government with cost savings through agencies' participation.

Agency responsibilities

Ultimately, individual SA Government agencies are responsible for securing their own systems and data. Consequently, agencies need to ensure that they implement sufficient controls to meet ISMF and other requirements.

Agencies must also report any security events or incidents to the ODG Watch Desk.

3 Audit objective and scope

3.1 Objective

The objective of our review was to determine whether agencies were effectively managing the following aspects of information security:

- legacy server operating systems
- patch management (operating systems and selected databases)
- privileged user access management
- mobile devices
- application whitelisting.

3.2 Audit scope

We assessed whether agencies had implemented policies and procedures for each relevant review component. We also reviewed listings of each agency's servers to assess the extent of legacy Windows servers in operation, and whether agencies had implemented mitigating security controls for them.

In the area of patch management, we assessed whether agencies had remediated the issues we identified in a previous audit performed in 2014-15. We also reviewed whether controls were implemented to identify, assess, implement and monitor operating system and selected database patches.

We assessed whether privileged user access to Active Directory was sufficiently restricted, logged and monitored. We also verified that agencies were conducting regular reviews of their privileged users for appropriateness.

Our assessment of mobile devices determined whether agencies had implemented sufficient controls to manage access to agency resources and data from mobile devices.

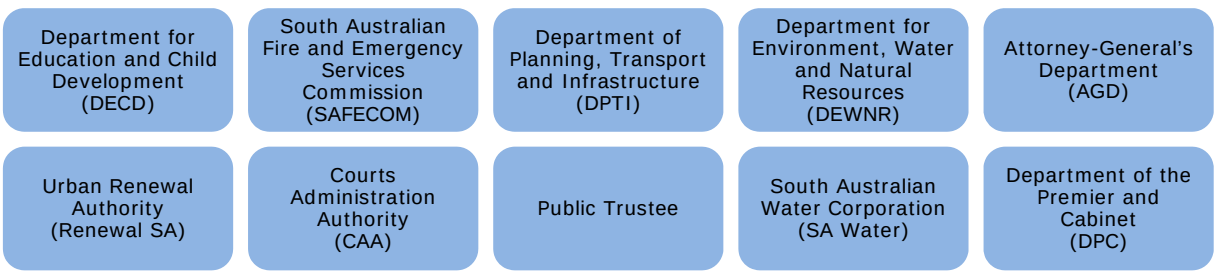
Finally, our application whitelisting assessment verified whether controls exist to prevent users (including malicious users) from executing unauthorised applications or software libraries.

For each area reviewed, we assessed controls implemented against mandated or recommended controls in relevant standards and guidelines (refer section 2.3). In some areas, such as mobile devices, elements of our assessment were based on best practice recommendations. Agencies will need to review the costs and benefits of implementing these recommended controls.

3.3 Agencies reviewed

We reviewed components of the scope across the 10 agencies listed in figure 3.1.

Figure 3.1: Agencies included in our review scope



As shown in figure 3.2, we reviewed whether agencies were effectively managing legacy servers at all 10 agencies. For the remaining review components, we assessed subsets of agencies (shown in no particular order).

Figure 3.2: Review components assessed at each agency

	Agency									
Review component	1	2	3	4	5	6	7	8	9	10
Legacy servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Patch management	✓	✓	✓	✓						
Privileged user access management				✓	✓					
Mobile devices					✓	✓				
Application whitelisting							✓	✓		

3.4 Attribution of review findings

We acknowledge that aspects of our review findings should be handled sensitively as they may highlight targeted security weaknesses at certain agencies. Accordingly, we have not attributed specific review findings to individual agencies or identified specific agency servers in this Report.

We provided a management letter to each of the 10 agencies reviewed. These letters detailed our findings and recommendations on the specific issues identified at each agency.

3.5 Limitations

We have not assessed all review components across the 10 agencies reviewed.

We have not assessed the adequacy of the agencies' information security management systems (ISMS). This review is not intended to provide a full assessment of agencies' compliance with ISMF requirements.

4 Legacy servers

Summary of key findings

SA Government agencies have not effectively decommissioned legacy Windows servers after the cut-off dates for Microsoft support.

This increases the risk of unauthorised access to sensitive information stored on these servers due to unpatched security vulnerabilities.

We identified that:

- there were 233 legacy servers operating across the 10 agencies we reviewed (13% of all servers operating at these agencies)
- eight of the 10 agencies reviewed still had legacy servers in operation (as at August/September 2016)
- all 10 agencies are working to decommission their legacy servers
- several agencies have not implemented sufficient controls to mitigate the increased risk of continuing to operate these servers.

Summary of key recommendations

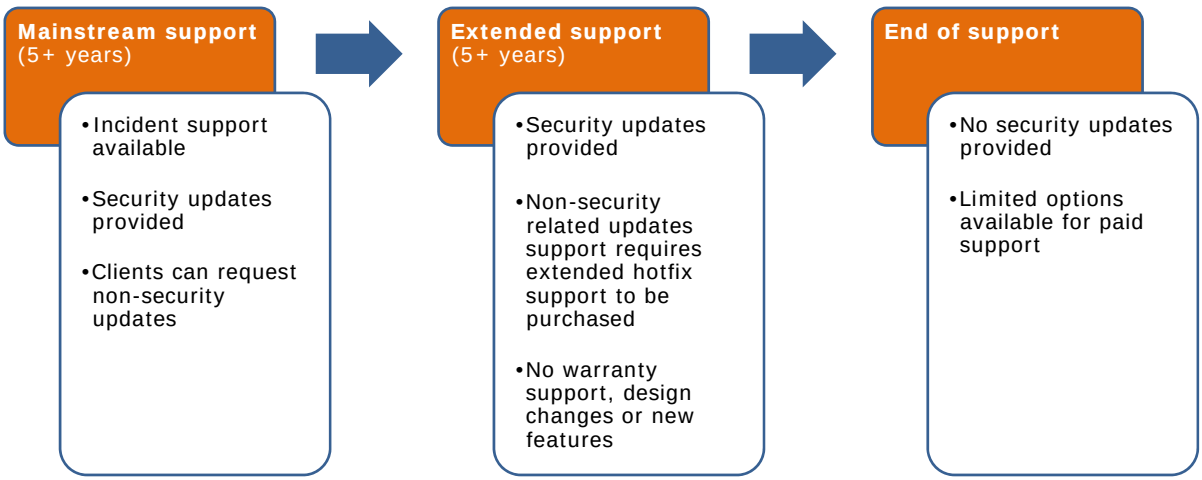
- Agencies should decommission legacy Windows servers as soon as practicable.
- Until decommissioned, agencies should consider implementing additional controls to mitigate the increased risk of continuing to operate these servers.

4.1 Introduction

A legacy operating system is an outdated computer operating system that needs either upgrading or replacing, as it is no longer receives vendor security patches.

Support time frames for Microsoft Windows server operating systems typically follow a staged support lifecycle, as shown in figure 4.1.

Figure 4.1: Microsoft operating system product lifestyle



Two legacy server operating systems that Microsoft has ceased supporting are Windows Server 2003 and Windows 2000 Server.

Figure 4.2: End of support dates for legacy Windows servers

Operating system	Original release date	End of support date
Windows 2000 Server	17 February 2000	13 July 2010
Windows Server 2003	24 April 2003	14 July 2015

Microsoft does not provide security updates (patches) to protect servers running these operating systems from new vulnerabilities. Therefore, continuing to operate these server operating systems increases risks to the confidentiality, integrity and availability of agency data and operations.

4.2 Mitigating controls to protect legacy servers

The ASD recommends that organisations using Windows Server 2003 or earlier versions upgrade to a newer, supported operating system. Where organisations could not achieve this by 14 July 2015, it recommended that they review the risk assessment for their ICT environment and implement additional controls to reduce their risk exposure.

Recommended mitigating controls include:

- implementing an application whitelisting solution (refer to section 8 for details) to detect and prevent certain malicious activity on legacy servers
- avoiding the use of privileged accounts on servers for non-administrative activities
- implementing a third-party software-based application firewall, or a 'virtual patching'[6] solution using an intrusion detection/prevention system
- disabling unnecessary functionality (such as non-essential services) or common intrusion methods.

4.3 Audit approach

Our objective was to determine whether agencies had decommissioned legacy Windows servers after the cut-off date for Microsoft support and migrated services to a supported operating system.

We assessed whether:

- there were legacy Windows Server 2003 or Windows 2000 servers remaining in operation
- effective mitigating controls had been implemented to reduce the risks of operating legacy servers
- agencies had not entered into extended support contracts for patching Windows Server 2003 servers.

[6] Virtual patch – the security enforcement layer of the intrusion detection/prevention system analyses network traffic directed at the legacy server and intercepts perceived attacks while in transit. If effective, the malicious traffic never reaches the server.

To assess this, we reviewed server listings from 10 SA Government agencies on two occasions between November 2015 and September 2016. We compared the two listings to assess agencies' progress in decommissioning any remaining legacy servers. We also discussed arrangements for decommissioning servers or implementing mitigating controls with agencies' ICT staff.

4.4 Agencies operate unsupported legacy servers

Audit recommendations

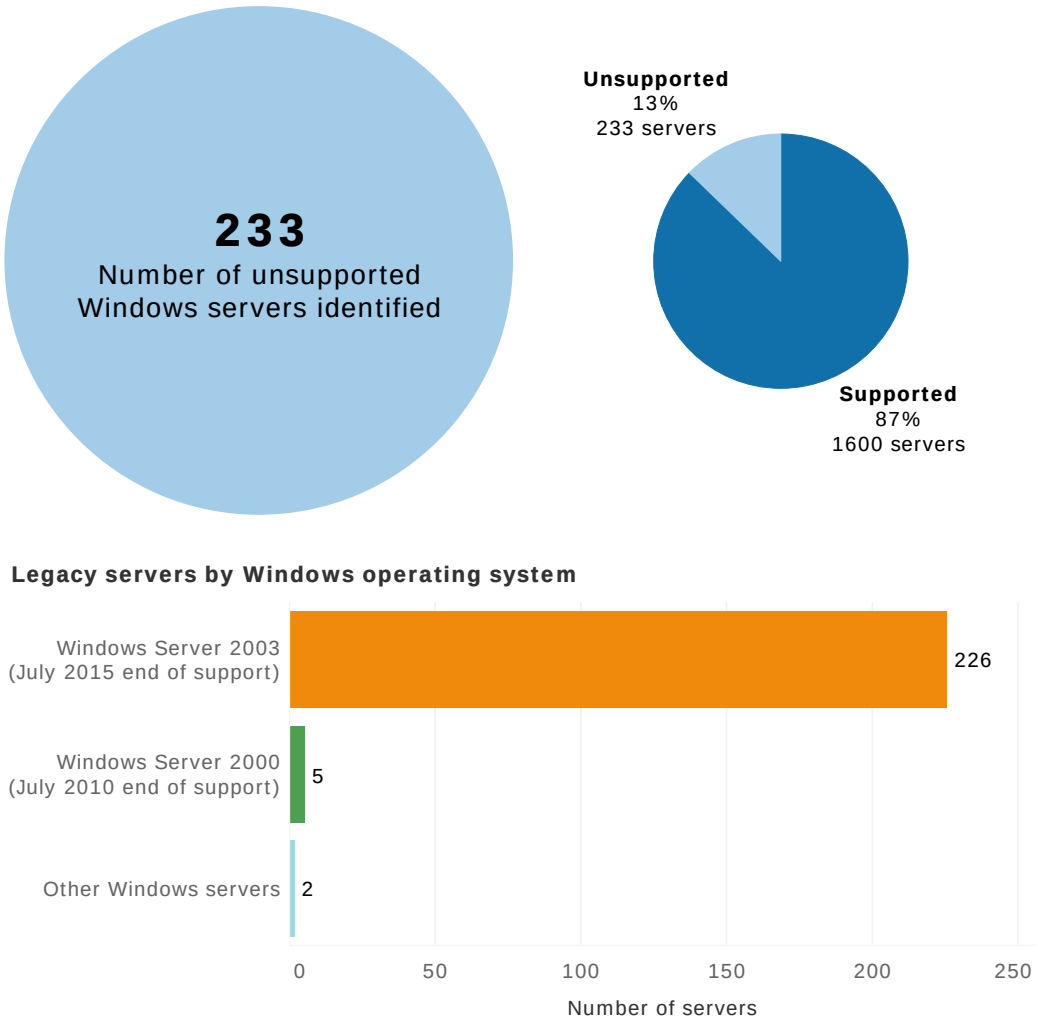
Agencies should decommission remaining Windows Server 2003 and Windows 2000 servers as soon as practicable.

Findings

Number of legacy servers

Of the 10 agencies we reviewed, eight were operating unsupported legacy servers. We identified 233 unsupported Microsoft Windows servers in total as at August/September 2016. This represents 13% of all servers managed by these agencies.

Figure 4.3: Summary of Windows servers by support status and operating system



We identified five Windows 2000 Server instances at two of the 10 agencies reviewed. These servers pose additional risk to those agencies' network environments. This is because they have been unsupported (and have therefore not received security patches) for more than six years.

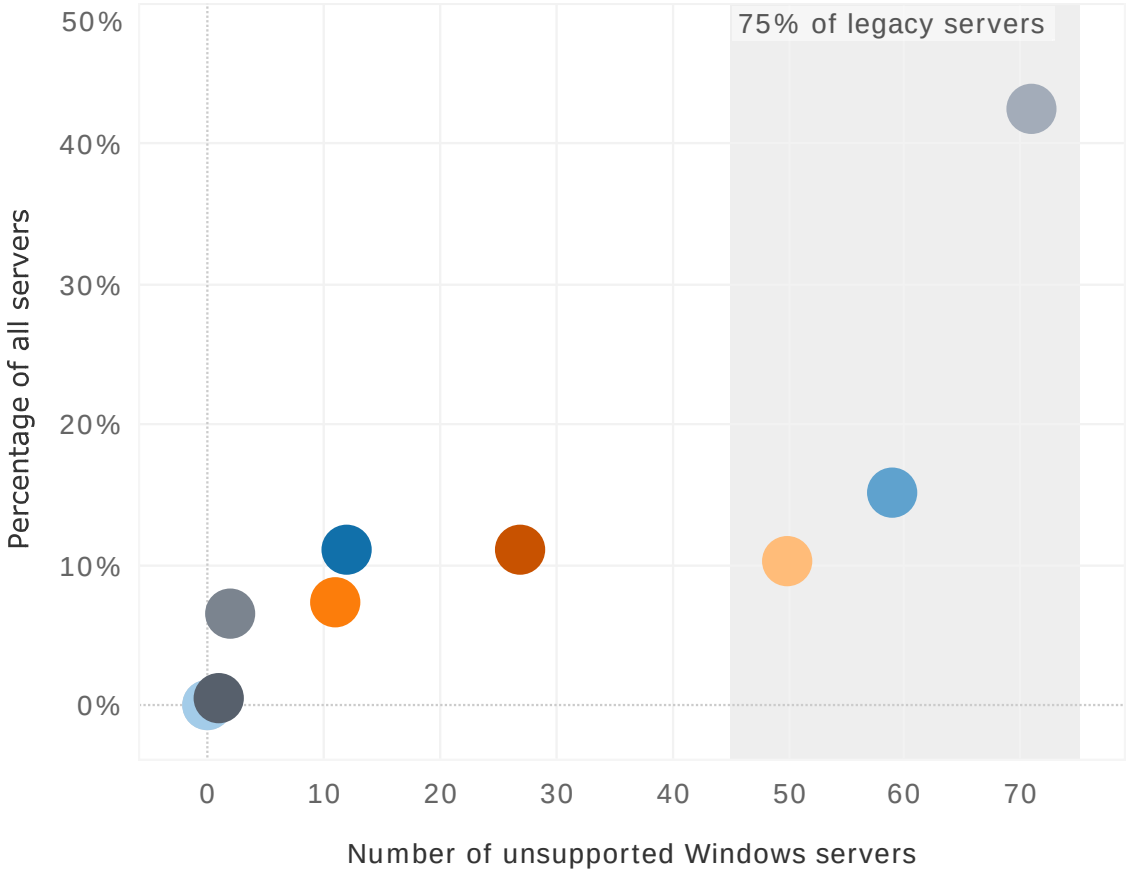
Where agencies use unsupported server operating systems, there is an increased risk of malicious modification or exposure of agency data and operations.

Agency comparison

We confirmed that over 180 of the legacy servers identified were concentrated within three agencies. This represents 75% of legacy servers across the agencies reviewed.

Figure 4.4 shows the number and percentage of unsupported servers at each of the 10 agencies we reviewed.

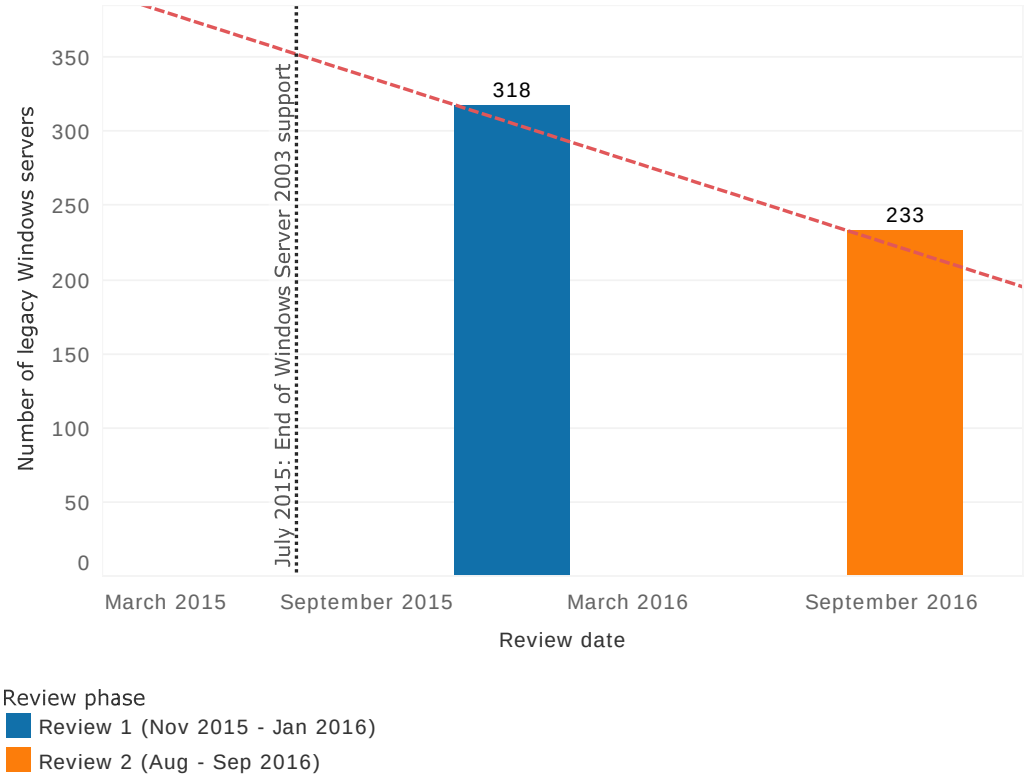
Figure 4.4: Number and percentage of unsupported legacy servers by agency reviewed



Progress in decommissioning servers

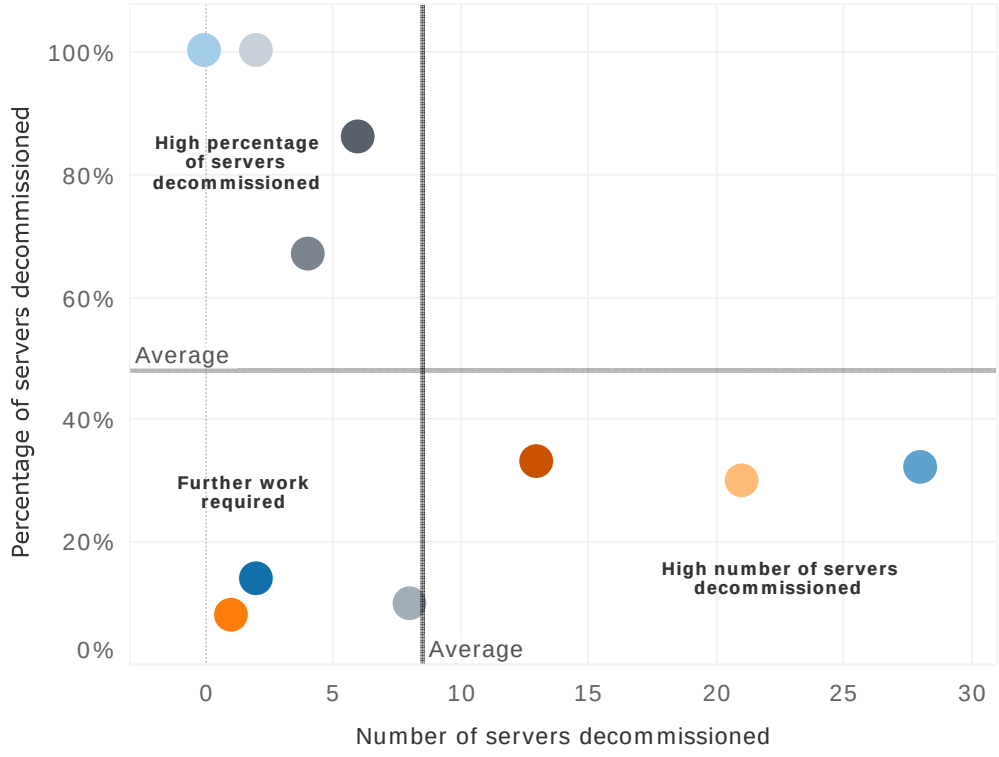
We noted that agencies with legacy servers decommissioned 85 servers between November 2015 and September 2016. This is a 27% reduction in legacy servers.

Figure 4.5: Total number of legacy servers by review date



During this time, agencies decommissioned between 8% and 100% of their legacy Windows servers. Figure 4.6 shows the number and percentage of servers decommissioned by agency.

Figure 4.6: Number and percentage of legacy servers decommissioned



In all cases, agencies had started to decommission their legacy servers. However, until all existing applications on a given server are migrated, the server cannot be decommissioned.

Due to machinery of government changes, some agencies had additional legacy servers brought under their support during the review period.

The time frames and arrangements for decommissioning the remaining legacy servers differed between agencies:

- At the time of our review, two agencies had not finalised time frames for decommissioning the remaining legacy servers.
- Another agency expects to decommission most legacy servers by 31 December 2016. We were advised that three servers cannot be immediately decommissioned, due to interface requirements with the SA Government's PABX. The agency does not expect to resolve this issue until the SA Government finalises an upgrade of certain PABX infrastructure.
- Two agencies expect to decommission all legacy servers by 31 December 2016 and another agency by 30 June 2017.
- One agency expected to allocate additional resources from October 2016 onwards to progress legacy server decommissioning. This process had previously been delayed due to a number of high-priority business projects.
- Another agency advised us that the two remaining legacy servers related to its core information system. We were advised that these servers cannot be decommissioned until the information system is upgraded or replaced (refer section 5.5).

One of these agencies also advised us that it had engaged an external supplier to remediate the remaining servers. This includes phases for legacy server and applications discovery, as well as migration to a newer operating system.

The agency with 71 legacy servers (the highest number and proportion of legacy servers of the 10 agencies reviewed) advised us that:

- 46 legacy servers needed to have all applications removed before a request to the vendor could be submitted to start formal decommissioning
- 25 legacy servers had all applications removed but were awaiting formal decommissioning.

For the legacy servers awaiting formal decommissioning, the risk of security vulnerabilities affecting sensitive data or applications is reduced. However, until fully decommissioned, these servers remaining on agency networks still pose a risk to the overall security of the server fleet. For example, if compromised, the servers may allow access to other agency systems and may enable a denial of service attack within the internal network.

Agency responses

Agencies responded positively to our review findings and recommendations with details of planned remediation.

In their responses, most agencies advised us that they had decommissioned additional servers since our audit and were planning to decommission all remaining servers as soon as possible. Time frames for completing this varied between agencies.

One agency advised us that its progress in decommissioning servers had been delayed by staff resourcing issues, which it was currently seeking to address.

4.5 Insufficient mitigating controls applied to protect legacy servers

Audit recommendations

Until legacy servers are decommissioned, agencies should consider implementing additional controls to mitigate the increased risk of using them. This should include:

- implementing application whitelisting on the server
- avoiding the use of privileged accounts on servers for non-administrative activities
- implementing a third-party software-based application firewall, or a 'virtual patching' solution using an intrusion detection/prevention system
- disabling unneeded functionality (such as non-essential services) or common intrusion methods.

Findings

We identified that several agencies had not implemented sufficient mitigating controls in line with ASD recommendations. Of the agencies yet to decommission their legacy servers, none had fully implemented the recommended best practice mitigating controls.

Figure 4.7: Extent of mitigating controls implemented

The three agencies marked as 'partial' had multiple controls in place to protect legacy servers, including:

- disabling unneeded functionality (such as non-essential services) or common intrusion methods.
- avoiding the use of privileged accounts on servers for non-administrative activities
- implementing a 'virtual patching' solution using an intrusion detection/prevention system.

In response to our queries, one agency advised us that it believed the controls implemented were sufficient to mitigate the risk of legacy servers being exposed to security vulnerabilities. It accepted the residual risk and was instead focusing on decommissioning the remaining servers. This was subject to funding approval to upgrade or replace that agency's core information system.

Several agencies reiterated that the none of their servers, or few of their servers, were directly accessible via the internet.

We also noted that one agency entered into extended arrangements with Microsoft for paid support of the across-government messaging servers. These servers at the time were running Windows Server 2003 and required an extended three-month support arrangement from July 2015 to September 2015.

This was a costly interim exercise (support arrangement fee of $150 000, excluding GST) and did not cover all legacy servers at that agency.

Where mitigating security controls have not been fully implemented, agencies are exposed to increased risk of security vulnerabilities.

Agency responses

Most agencies responded positively to our recommendations. For example, one agency confirmed that it has since ceased using privileged accounts on servers for non-administrative tasks. Additional mitigating controls would be considered at several agencies should the remaining servers not be decommissioned within expected time frames.

Another agency advised us that its Windows Server 2003 fleet is subject to greater operational dependencies, which means that it is not practical to have all servers decommissioned within the next year. In the interim it will implement additional controls on these servers.

Two agencies advised us that they believe the risks that application whitelisting or other mitigating controls are designed to manage are unlikely to arise. One of these confirmed that the remaining legacy servers are behind two firewalls and are not directly accessible via the internet.

5 Patch management

Summary of key findings

Two of the four agencies we reviewed had not effectively managed operating system and database patching. This increases the risk that agencies have not applied critical security patches. This could affect the confidentiality, integrity and availability of agency systems and data.

We identified the following issues:

- servers with missing operating system and database security update patches
- a core information system application, database and operating system not patched at one agency
- deficiencies in patch management and change management policies/procedures at multiple agencies
- deficiencies in processes for patching compliance checking and reporting
- insufficient documentation of patching exemptions at one agency.

Summary of key recommendations

Agencies should:

- review servers identified with missing patches and ensure that they apply all applicable security patches
- ensure that they identify patching requirements promptly, through regular review of security bulletins
- document policies for patch management and change management. Ensure that policies and procedures are reviewed regularly and updated as required
- ensure that assurance practices include regularly assessing patching compliance levels for servers and workstations
- retain sufficient documentation of patching exemptions for all servers.

5.1 Introduction

5.1.1 Background

A patch is a piece of software that is designed to fix defects or vulnerabilities, or provide updates to an information system.

Agencies need to patch their information systems regularly to maintain ongoing security over their systems and data. This includes operating systems, databases and applications.

Figure 5.1 shows an example of a recent patch that Microsoft released to resolve multiple vulnerabilities it identified.

Figure 5.1: Example of a recent Microsoft patch release

Security bulletin number	MS016-007
Title	Security Update for Microsoft Windows to Address Remote Code Execution (3124901)
Published	January 2016
Affects	All supported releases of Microsoft Windows (including desktop and server operating systems)
Summary	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.

As outlined in section 2.3, the ASD lists patching operating system vulnerabilities as one of the four most effective strategies to mitigate the risk of targeted cyber intrusion (or hacking).

Additionally, ISMF Standard 134 requires agencies to review information assets and systems periodically, to verify compliance with security implementation standards and controls. Agencies are required to document and plan procedures for examining hardware and software to ensure that known security patches and fixes have been implemented.

System documentation should specify a maximum time frame within which security patches have to be applied. This ensures that systems are not compromised by vulnerabilities that have been addressed using vendor patches or recommended configuration changes.

Requirements for patching operating systems and applications are also included in the Top 10 cyber security objectives (refer section 2.3).

5.1.2 Responsibilities for patch management

Most SA Government agencies use the outsourced Distributed Computing Support Services (DCSS) arrangements. This involves servers being managed by an external contractor, including aspects of the patching process.

Figure 5.2 shows the typical split of responsibilities between agency staff and DCSS providers as part of each stage of the patching process for servers.

Figure 5.2: Allocation of responsibilities for patching

Server patching process step	Agency ICT staff	DCSS provider
Identifying required patches	✓	✓
Assessing patches for suitability	✓	✓
Approving patches for implementation	✓	
Implementing patches		✓
Monitoring patching compliance	✓	✓

At the time of our review, agency ICT staff typically managed all stages of the patching process for workstations in-house.

5.1.3 Prior year reviews of patch management

During 2014-15, we reviewed patch management processes at two agencies, and provided them with a number of recommendations to address control weaknesses.

To address weaknesses in policies and procedures, we recommended that server operating system patching follow a formal change management process. This included documentation of approved, implemented or exempted patches. Exemptions should be reviewed regularly to ensure their validity.

We also recommended that agencies ensure regular patch compliance scans of servers and workstations are performed. Results of compliance scans should be reviewed to ensure all appropriate patches are applied.

Both agencies responded that the identified deficiencies would be remediated. This included updating policies and procedures, as well as ensuring regular reviews of operating system patching compliance.

5.2 Audit approach

Our objective was to determine whether agencies were effectively managing the patching of server operating systems and databases.

We assessed whether:

- prior audit findings from the 2014-15 patch management audits at two agencies had been remediated
- patch management policies and procedures were in place and current
- controls to identify, assess, implement and monitor patches were operating effectively
- agency servers were up to date with all available and applicable patches.

Our review scope for this component included the two agencies tested in 2014-15 and two additional SA Government agencies.

5.3 Servers identified with missing operating system security update patches

Recommendations

Agencies should:

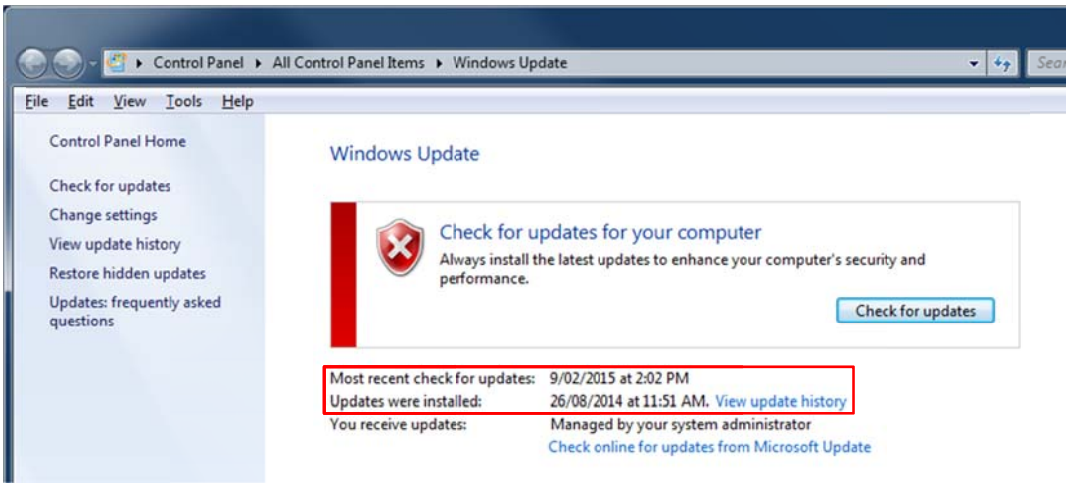
- review the servers identified with missing patches and ensure that they apply all applicable security patches
- retain sufficient documentation of patching exemptions for all servers
- ensure that the assurance practices include assessing patching compliance for all agency servers, irrespective of server environment or operating system.

Findings

To verify whether agencies had correctly patched server operating systems with all available and applicable patches, we selected samples of Windows and Unix servers for review at each agency. Sample sizes varied depending on the number of servers that each agency operated.

For each Windows server selected, we inspected the Windows Update control panel to confirm whether all available and required patches were installed.

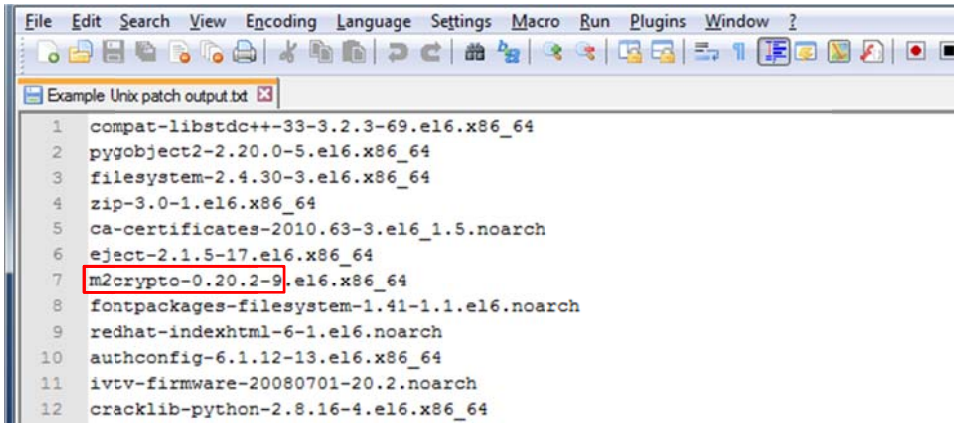
Figure 5.3: Example of the Windows Update control panel
This shows that security patches have not been installed since August 2014



The Unix servers we reviewed included Solaris and Red Hat Enterprise Linux servers.

For these servers, we inspected the version numbers of key system packages on each server to confirm whether the server had been patched with selected recent security vulnerabilities.

Figure 5.4: Example output from a Unix server used to verify patching status
We verified the version numbers of key system packages against available information on vendors' websites to verify patching status



Through this testing, we identified Windows and Unix servers with missing operating system security update patches.

Figure 5.5: Patch testing results

Patch testing result	Agency 1	Agency 2	Agency 3	Agency 4
Windows servers				
Servers are up to date with all applicable patches	✗	✓	✓	✓
Number of servers reviewed	15	10	5	5
Number of servers identified with missing patches	5	0	0	0
Unix servers				
Servers are up to date with all applicable patches	n/a	✗	n/a	✗
Number of servers reviewed	0	5	0	1
Number of servers identified with missing patches	n/a	3	n/a	1

We did not test Unix servers at all four agencies, because two had no or a limited number of Unix servers in their environments.

Based on information provided and discussions with agencies, we identified several causes for servers missing security update patches. These included instances where:

- servers had only recently been provisioned and had not yet entered support by the external vendor. Agency ICT staff were patching these servers manually but had overlooked recent updates
- servers had not been correctly configured to receive patches
- servers had recently been transferred to the agency's ICT team due to an organisational restructure.

In several instances, agencies were unable to provide us with documentation of patching exemptions for servers with missing patches (refer section 5.9).

Additionally, one agency could not provide us with sufficient evidence that its Solaris servers had been patched with Oracle's critical patch advisory for July 2016.

Where critical patches are not applied, there is an increased risk of unauthorised access to systems or data through an unpatched security vulnerability.

Agency responses

Agencies responded positively to our findings with details of planned remediation. This included extending the scope for server patching assurance reviews to include all relevant agency servers.

5.4 Servers identified with missing database security update patches

Recommendations

Agencies should:

- review the servers identified with missing database patches and ensure that all applicable security patches are applied

- ensure that database security patching requirements are promptly identified through regular review of security bulletins.

Findings

We also assessed the effectiveness of database security patching at two agencies. For each agency, we obtained a listing of databases used in the agency's core operations. The two agencies reviewed used Microsoft SQL Server for multiple databases.

To verify whether each agency had correctly patched its Microsoft SQL Server databases, we verified the current version number for a sample of databases. We confirmed this against information available on Microsoft's patching information website.

Our testing results for Microsoft SQL Server patching are summarised in figure 5.6.

Figure 5.6: Testing results for Microsoft SQL Server patching

Patch testing result	Agency 1	Agency 2
Database patching: Microsoft SQL Server		
Servers are up to date with all applicable patches	✓	✗
Number of servers reviewed	3	3
Number of servers identified with missing patches	0	2

Of the three servers reviewed at one agency, two servers had not been patched for a Microsoft vulnerability released in July 2015. The most recent update applied to these servers was Service Pack 3, which was released in September 2014.

This vulnerability, where left unpatched, may allow an attacker to execute malicious code on the database server in certain cases. We could not obtain any documentation of a patching exemption to indicate that the agency assessed this patch.

Where critical patches are not applied, there is an increased risk of unauthorised access to systems or data through an unpatched security vulnerability.

Agency responses

The applicable agency advised us that it has reviewed the two servers identified. The missing database security update patches were expected to be applied to the two servers by November 2016.

We were also advised that the agency is enhancing its processes to identify, assess and remediate information technology vulnerabilities, as well as weaknesses or exposures in ICT resources and processes. A vulnerability management standard, which includes processes for database security patching, will be finalised in November 2016.

5.5 Core information system application, database and operating system not patched at one agency

Recommendations

The agency should continue to pursue options to upgrade or replace the core application and underlying infrastructure to mitigate the risks identified.

Findings

One agency we reviewed uses an enterprise resource planning system to deliver financial administration and client services.

We confirmed that the application, operating system and associated database for the core information system at that agency have not been patched since 2008. The agency advised us that it did not apply patches or system updates due to its assessment of the risk of potential disruption to the integrity and availability of the system. However, this approach exposes the agency to additional risk via unpatched security vulnerabilities.

The vendor continues to provide maintenance support for the version of the application implemented. However, security update patches and bug fixes are no longer released.

Two servers running the Solaris 8 operating system no longer receive security update patches from the vendor. Our testing also confirmed that certain security patches released prior to the end of Solaris 8 vendor support had not been applied. This included a patch released for the Shellshock Bash vulnerability in October 2014. The agency advised us that it did not apply this patch to the applicable servers, as these servers were not publically accessible via the internet.

We inspected documentation confirming that the servers for the agency's public website had been patched. Although this reduces the overall risk exposure, applicable servers may still be susceptible to this vulnerability if a malicious user is able to access the internal network.

Parts of the application run in a virtual machine environment. Although the guest virtual machines run the Solaris 8 operating system, the underlying host runs Solaris 10 and is patched as required.

The agency also advised us that a proposal for 2015-16 funding to commence the procurement process for a replacement system was not approved.

Operating unsupported applications, operating systems and databases increases the risk of system failure and exposure to security vulnerabilities. This may cause significant disruption to agency operations, or cause the exposure of sensitive personal and financial data.

Agency responses

The agency advised us that it will continue to promote the business case to replace its core information systems. Until the systems are replaced, the agency will continue to manage the security of the applicable servers consistent with ISMF requirements.

5.6 No documented policies or procedures for patch management or change management

Recommendations

Agencies should document policies for patch management and change management, covering the following aspects shown in figure 5.7.

Figure 5.7: Patch management and change management

Patch management policy	Change management policy
• identifying and assessing patches • implementing patches (including time frames) • monitoring patching compliance • defining roles and responsibilities.	• requesting changes and approving changes for development • developing and testing changes • authorising changes for implementation • implementing changes • maintaining segregation of duties • defining roles and responsibilities.

We also recommend that agencies implement all patches as part of a formal change management process. Lower-risk patches could be classified as 'standard changes' to reduce the need for excessive approval processes.

Findings

Our review identified that one agency patched their non-critical servers and all workstations automatically using Windows Update, with ICT staff manually patching critical servers.

Although this agency was patching their systems, the agency did not have any documented policies or procedures for patch management or change management. There was limited documentation of how specific patches had been identified, tested or implemented. The patching process did not follow a formal change management procedure.

Documented policies, procedures and work instructions are an integral part of an organisation's control environment. Where they are not in place or not current, employees may not understand their roles and responsibilities and may not meet management's expectations.

Additionally, where information system changes (including patches) do not follow a formal change management process, there is a risk that implemented changes do not meet business requirements or adversely impact server operations.

Agency responses

The agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

5.7 IT policies and procedures not reviewed promptly

Recommendations

Agencies should review IT policies and procedures regularly (ie at least annually) and update them as required.

Findings

We identified that IT policies and procedures relating to patch management and change management were not reviewed promptly at one agency. However, the patch management procedure was reviewed and approved after we commenced our audit.

Where policies and procedures have not been reviewed regularly, there is a risk of inconsistent patch management or change management processes. This increases the potential exposure of security vulnerabilities.

Agency responses

The agency responded positively with details of planned remediation. This included ensuring that relevant business units are reviewing and updating key documentation as appropriate.

5.8 Regular monitoring of patching compliance was behind schedule and does not assess all servers and workstations

Recommendations

Agencies should ensure that their ISMF assurance processes include regularly assessing patching compliance levels for all servers and workstations. Instances of missing patches should be investigated and the results documented.

Findings

One of the agencies we reviewed had implemented an ISMF assurance program and was performing a number of processes to verify ISMF compliance. This included the following processes to review patching compliance:

- The ISMF assurance program includes a six-monthly review of Windows and Unix server patching compliance. This is performed by reviewing a small sample of servers individually to confirm that all applicable patches have been applied to each server. This process does not include all agency servers.
- The IT Security Advisor performs a monthly scan of all Windows servers using an automated tool to verify patching compliance. Presently, the scan does not include Unix servers. Results of the scan are not formally documented.

At the time of our review (September 2016), the agency had not completed the July 2016 ISMF assurance review of server patching compliance.

Without a regular monitoring process in place for monitoring patching compliance for all servers and workstations, systems may not be up to date with all available security updates and patches. This increases the risk that a workstation or server will be vulnerable to an unpatched security weakness.

Agency responses

The agency advised us that it will now include regular assessment of patch compliance levels for all servers (both Windows and Unix) and workstations as part of ongoing ISMF assurance activities.

5.9 Insufficient documentation of patching exemptions

Recommendations

Agencies should retain sufficient documentation of patching exemptions for all servers.

This should include the details of specific servers and patches to be exempted from the patching process, as well as the rationale of each exemption.

Findings

In some cases, agencies may choose to exempt certain operating system patches or individual servers from the regular patching process. This may be due to compatibility issues with installing a particular patch, or the patch not being relevant to a server's primary function.

One agency advised us that patches and exemptions are documented as part of a release management process. This includes quality assurance processes for previous releases. However, it could not provide documentation of patching exemptions for any of the servers we identified with missing security update patches (refer section 5.3).

If comprehensive patching exemption documentation is not maintained, agencies cannot determine whether certain patches have been deliberately omitted from servers or whether patches have been missed. This increases the potential exposure of security vulnerabilities.

Agency responses

The applicable agency advised us that the sampled servers were not exempt from the patching process. Instead, they had not yet been identified as being owned by the agency.

We were advised that the agency was reviewing all servers in a shared network environment to determine which servers it was responsible for managing. It will then remediate servers are required.

It expects to complete this process by the end of January 2017.

5.10 Patch compliance reports not available for servers

Recommendations

Agencies should expand the scope of coverage for computers managed within Microsoft System Centre Configuration Manager (SCCM) or similar software to include servers, where applicable. This would allow agencies to generate patching compliance reports for servers.

Alternatively, agencies may be able to obtain patching compliance reports from their DCSS providers.

Agencies should review patching compliance reports regularly and investigate any discrepancies identified (such as servers with missing patches).

Findings

We confirmed that one agency uses Microsoft SCCM to manage operating system patching for workstations. Microsoft SCCM allows the agency to generate regular reports showing a summary of operating system patching compliance.

Figure 5.8: Example report from Microsoft SCCM
This shows the percentage of agency workstations that have been updated with each required security patch

Microsoft System Center 2012 R2 Configuration Manager

Compliance 3 - Update group (per update)

Update Group ID	Update Group
16785981	All Updates

Title	Article ID	Bulletin ID	Installed	Required	Not Required	Unknown	Total	% Compliant
Cumulative Security Update for ActiveX Killbits for Windows 7	2900986	MS13-090	69	1	223	4	297	98.32%
Cumulative Security Update for Internet Explorer 11 for Windows 7	3148198	MS16-037	1	0	287	9	297	96.97%
Cumulative Security Update for Internet Explorer 11 for Windows 7	3154070	MS16-051	0	5	280	12	297	94.28%
Cumulative Security Update for Internet Explorer 11 for Windows 7	3160005	MS16-063	35	29	215	18	297	84.18%
Cumulative Security Update for Internet Explorer 11 for Windows 7	3170106	MS16-084	14	11	185	87	297	67.00%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	3142042	MS16-039	229	5	54	9	297	95.29%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	3135983	MS16-035	234	3	53	7	297	96.63%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	3142024	MS16-065	222	11	52	12	297	92.26%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	3163245	MS16-091	141	21	48	87	297	63.64%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	2894844		69	0	224	4	297	98.65%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	2911501	MS14-009	69	0	224	4	297	98.65%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	2931356	MS14-026	69	0	224	4	297	98.65%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	2968294	MS14-057	69	0	224	4	297	98.65%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	2972100	MS14-057	69	0	224	4	297	98.65%
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	3023215	MS15-048	69	2	222	4	297	97.98%

We inspected a recent compliance report from Microsoft SCCM for this agency and confirmed that 93% of all workstations had all available and applicable patches installed.

However, the agency did not use Microsoft SCCM for its servers. As a result, it could not generate equivalent patching compliance reports for its servers.

Our sample testing of the agency's server operating systems and databases did not identify any instances of missing security update patches.

Despite this, where compliance reports are not available, agencies cannot easily verify that all servers are up to date with all available and applicable patches. This may increase the risk of sensitive data being exposed via an unpatched security vulnerability.

Agency responses

The agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

6 Privileged user access management

Summary of key findings

The two agencies we reviewed were not effectively managing privileged user access to Active Directory (AD) in line with ISMF requirements. This includes domain-level privileged access and privileged access permissions on local computers.

As a result, there is an increased risk to the confidentiality and integrity of sensitive systems and data.

We also identified:

- no formal periodic review of AD privileged users
- deficiencies in user access and IT security policies/procedures
- terminated employee reports were not received or reviewed promptly
- privileged user activities were not sufficiently logged and monitored.

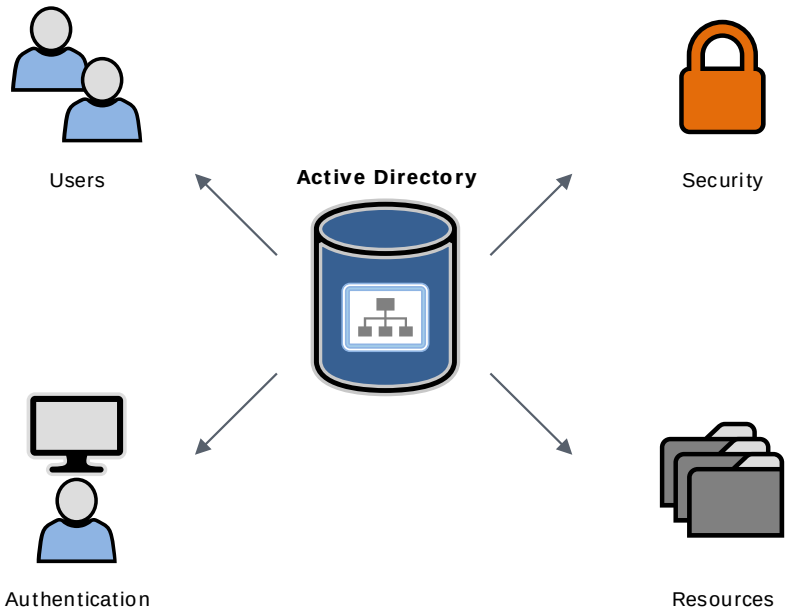
Summary of key recommendations

- Assign domain-level privileged access within AD to individual accounts for each employee requiring access.
- Restrict access to local administrator rights based on user duties.
- Ensure that separate accounts are established to segregate standard and administrative user activities.
- Implement a formal, documented process to review AD users in line with ISMF requirements.
- Document a policy for AD user access management. Ensure that IT policies and procedures are reviewed regularly and updated as required.
- Ensure that terminated employee reports are provided regularly and promptly. Once provided, agencies should review the reports and delete applicable user accounts as soon as practicable.
- Consider opportunities to log and monitor privileged user activities in line with ISMF guidelines and agencies' accepted level of risk.

6.1 Introduction

AD is a centralised information system within the Microsoft Windows server environment. It is used to manage network user authentication, data security and distributed resources.

Figure 6.1: Active directory



AD is also used by system administrators to assign security policies, deploy software and apply critical software updates to servers and end-user workstations.

AD users with domain-level privileged access permissions can access sensitive data and change security settings across an entire network. Users with local administrator permissions can install unauthorised software and change system settings on their local computers.

It is crucial that agencies manage privileged AD user access effectively to reduce the risk of unauthorised access to sensitive information. Requirements for effectively managing administrative rights (incorporating administrative rights for AD) are included in the Top 10 cyber security objectives (refer section 2.3).

ISMF Standard 78 states that agencies must restrict and control privileges. They should implement a formal authorisation process to grant and deny access to information resources.

ISMF Guideline 25 also recommends that agencies strictly control, monitor and audit the allocation and use of privileged access for positions of trust. Privileged accounts should be used for authorised duties only.

Agencies should conduct periodic reviews of privileged AD users for appropriateness. This includes documenting the results of the review and removing any excessive permissions.

Finally, agencies need to minimise their use of local administrator accounts on user workstations.

6.2 Audit approach

Our objective was to determine whether agencies are effectively managing privileged AD user access.

To determine this, we assessed whether:

- defined policies and procedures exist to manage privileged AD user access
- privileged AD user access is restricted to employees who need access to system administration functions as part of their job roles/functions
- periodic reviews of privileged AD user access are conducted and results documented
- the use of local administrator accounts on desktop PCs is minimised
- separate AD user accounts are established for performing system administration functions
- privileged user activities are logged and monitored.

We selected two agencies for review.

6.3 Domain-level privileged access not effectively managed

Recommendations

Agencies should regularly review privileged user access permissions for appropriateness.

This process should include regular reviews of domain administrator permissions, with results documented. Access should be removed where it is no longer required as part of their job role or system requirements.

Domain-level privileged access to AD should be assigned to ICT employees individually.

Separate accounts should be established for each employee's privileged and standard activities.

Findings

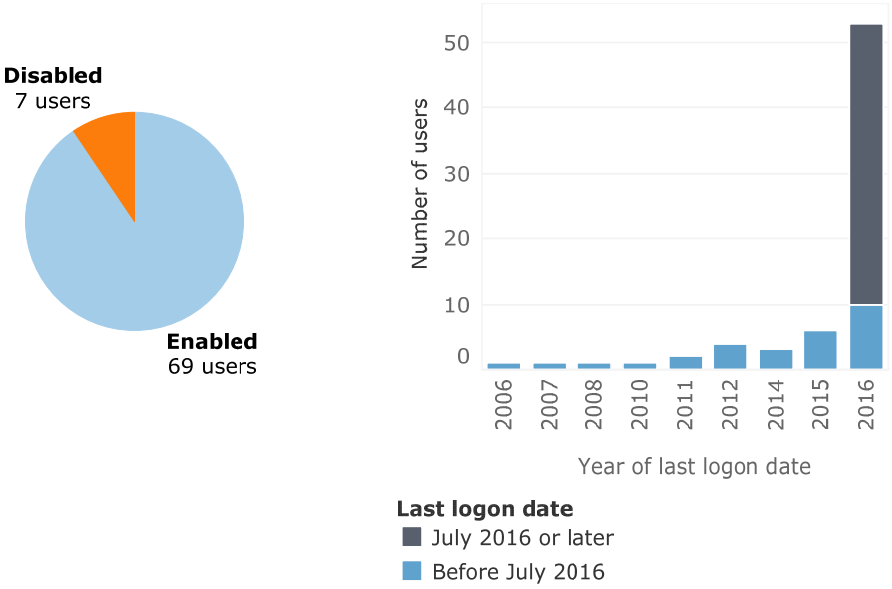
Domain-level privileged access permissions allow assigned users to access sensitive data and change security settings across an entire network.

We reviewed lists of all users in the two agencies' AD environments. Through this, we assessed whether the extent and nature of domain-level privileged access permissions assigned was appropriate.

Potentially excessive access assigned

We confirmed that one agency has potentially granted excessive domain-level AD privileged access. We identified 76 privileged user accounts, seven of which were disabled.

Figure 6.2: Privileged user accounts by status and last logon date



At the time of our review, we noted that 33 of these accounts were not accessed since July 2016. This suggests that some of these accounts are not required and should be disabled or removed.

The agency advised us that all of the privileged user accounts identified are used by the external DCSS provider. Agency employees do not have access to these accounts. Agency ICT staff requiring privileged access are added to a different permissions group, which provides a lower level of access.

The agency also advised us that it had started to review AD privileged users for appropriateness (refer section 6.5).

Given the extent of access assigned, there is an increased risk of unauthorised access to, or modification of, sensitive data and system settings.

Privileged access assigned to a shared account

At the second agency reviewed, we identified that domain administrator access has been assigned to a shared account. The agency advised us that three ICT staff have access to the account.

As a partial mitigating control, we were advised that the agency uses group policies in AD to prevent changes to the domain administrator accounts. Group policies are also used to ensure that Windows user account control is enabled on all workstations.

We acknowledge that every AD network requires a user with domain-level privileged access permissions. However, based on the use of a shared account, we are unable to verify that privileged access is restricted to appropriate personnel. This is because we cannot verify who has access to the password for the shared account.

The shared account arrangement reduces the accountability of individual users. Therefore, there is an increased risk of unauthorised access or changes to sensitive data or system security settings.

Agency responses

One agency confirmed that it has recently started reviewing and updating processes for managing privileged access. This commenced as part of the agency's project to address the Top 10 objectives. The agency acknowledged that this process should continue as per our audit recommendations.

The agency also advised us that it is reviewing domain access in conjunction with the DCSS vendor. It expects to complete this process by 30 November 2016.

The second agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

6.4 Excessive access granted to local administrators

Recommendations

Agencies should review whether local administrator rights have been assigned to users appropriately.

Access should be restricted based on user duties in line with ASD recommendations. Where not required for the user's job, local administrator rights should be removed.

Findings

Local administrator permissions allow assigned users to install unauthorised software on their local computers. Users with these permissions are also able to modify certain local system and security settings.

The ASD recommends that administrative privileges be restricted based on user duties. This includes the assignment of local administrator permissions.

At the time of our review, one agency had granted local administrator rights to approximately 600 workstations. This represented 75% of all workstations at that agency.

The second agency had granted local administrator rights to 414 workstations. The agency's corporate ICT asset management policy states that users must not install unauthorised software on ICT equipment. Users with local administrator rights can bypass this policy requirement.

Where users have been granted local administrator permissions, there is an increased risk of unauthorised changes to system and security settings, or the installation of unapproved software. The risk of malicious code exploiting security vulnerabilities is also increased for these users.

Agency responses

The first agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

The second agency advised us access granted to local administrators has been an area of challenge for some time. This is because it has a significant number of desktop applications that require local administrator access for specific purposes.

This agency commenced a process in September 2016 to review local administrative access. We were advised that, as at October 2016, it had reduced the number of local administrator accounts to 248. These accounts are being reviewed in detail. Progress on this review is reported to the department's ICT Assurance and Governance Committee on a monthly basis.

It also advised us that although the permissions assigned technically allow users to install unauthorised software, long-standing policies and procedures were in place to prevent such action. Any variations to the agency's standard operating environment are required to be submitted and approved by the ICT change advisory board.

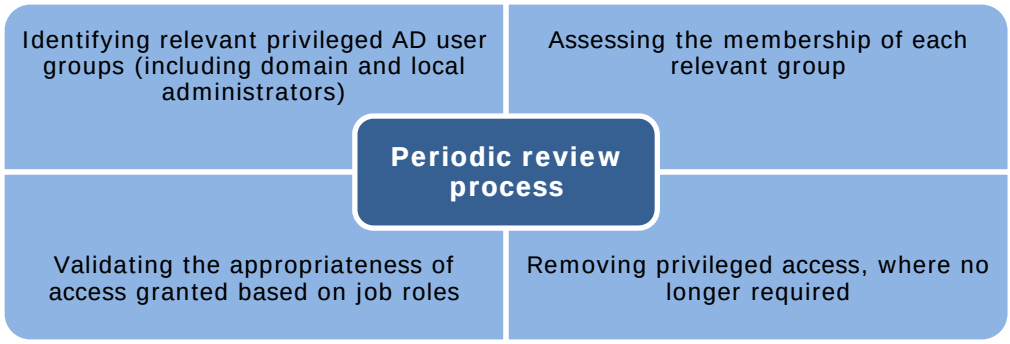
6.5 No formal periodic review of Active Directory privileged users

Recommendations

Agencies should implement a formal, documented process to review AD users in line with ISMF requirements.

The user access review should be performed regularly (ie at least annually). Review processes should include the aspects shown in figure 6.3.

Figure 6.3: Recommended periodic review process for AD users



Findings

ISMF Standard 80 requires agencies to conduct periodic reviews of users' access rights to maintain effective controls over access to data and information services.

We identified that one agency has no formal or documented process in place to periodically review AD users.

After we commenced our audit, the second agency we reviewed advised that its ICT assurance team had started reviewing local and domain administrators. Their aim was to reduce the number of privileged accounts across the agency network environment. The agency had started applying interim measures to review privileged accounts, until a formal procedure is approved and implemented.

At the time of our review, this process had not been fully implemented. A draft procedure and standard for managing user access privileges is awaiting approval of the information management policy (refer section 6.6).

Until a periodic user review process is implemented for privileged users (domain and local administrators), agencies cannot verify that the level of access granted to users is appropriate. This increases the risk of unauthorised access to, or modification of, sensitive data and system settings.

Agency responses

The first agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

The second agency advised us that the approval for its draft procedure to manage access privileges was pending the approval of the higher-level information management policy. The revised procedure includes period access reviews as per our audit recommendation.

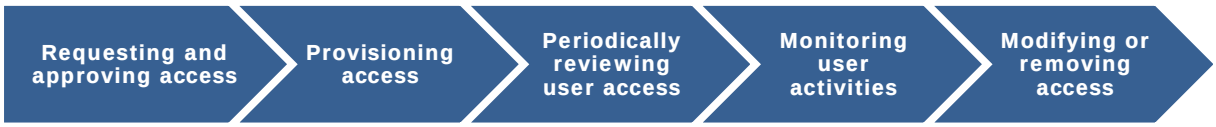
However, the agency has implemented an interim process to regularly review access permissions. This process has been endorsed by the ICT assurance and governance committee. The process is formally documented in a register.

6.6 User access and IT security policy / procedure deficiencies

Recommendations

Agencies should document a policy for AD user access management. Figure 6.4 shows the functions for standard and privileged AD users that should be covered.

Figure 6.4: Recommended functions for user access management



Agencies should review IT policies and procedures regularly (ie at least annually) and update them as required.

Findings

No documented policies or procedures for user access management

One of the agencies we reviewed did not have any documented user access policies or procedures.

IT security policies outdated

As part of our review, we obtained several agency policies relating to IT security. Several policies at both agencies were outdated and had not been regularly reviewed.

The policies we obtained from one agency were last updated in January 2008.

At the other agency, the policy relating to privileged access management had not been updated since March 2010. Responding to our initial observations, that agency advised us that all ICT policies were reviewed in 2015 and were found to be relevant. However, not all documents were updated at the time.

That agency also advised us that a decision was made not to update existing policy documents, as it is developing a new information management policy. The information management policy replaces a number of ICT policies, standards and procedures.

Documented policies, procedures and work instructions are an integral part of an organisation's control environment. Where they are not in place or not current, employees may not understand their roles and responsibilities and may not meet management's expectations.

Agency responses

The first agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

The second agency advised us that the information management policy was recently approved and is about to be communicated. It now establishes the foundation for replacing the agency's ageing, yet still relevant, ICT policies, standards and procedures that remain in effect.

It advised us that is has reviewed the recommendations outlined and will continue to review and update ICT policies and procedures in line with its policy framework and the information management policy.

6.7 Terminated employee reports not received or reviewed promptly

Recommendations

Agencies should liaise with Shared Services SA (SSSA) to ensure that SSSA provides terminated employee reports regularly and promptly.

Once provided, agencies should review the reports and action any user account deletions as soon as practicable.

Findings

ISMF Standard 78 requires agencies to implement a formal process for granting and denying access to information resources.

We found that SSSA provides regular reports to one of the agencies we reviewed. These reports detail the employees who have recently terminated their employment with the agency. SSSA extract the reports from the CHRIS payroll system.

Agency ICT staff then contact the line manager for each terminated employee and confirm whether system access can be removed.

The agency advised us that SSSA does not always provide these reports promptly after employee terminations. At the time of our review (September 2016), the most recent report available for terminated employees was from July 2016.

Where terminated employee reports are not received or reviewed promptly, employees or contractors no longer working within agencies may still have active user accounts. This increases the risk of unauthorised access to sensitive agency data.

Agency responses

The agency advised us that it has developed an action plan to address several information security deficiencies. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

6.8 Findings from Microsoft review of Active Directory environment not yet remediated

Recommendations

The agency should remediate the issues identified in Microsoft's report as soon as practicable. This should include developing a detailed remediation plan, with time frames for implementation.

Findings

In late 2015, Microsoft assessed the AD environment at one of the agencies covered by our review. The assessment included interviewing certain agency staff and running software tools to collect data from targeted systems. Results from the review were classified into either 'health assessment' findings or 'risk/security' findings.

Microsoft's review identified that, while the overall health assessment rating for AD was medium, the overall risk level for the AD environment was rated as critical. This was based on identifying several high-risk issues, including those shown in figure 6.5.

Figure 6.5: High-risk issues for the AD environment (identified by Microsoft)

Security

- password policy allows reversible encryption
- user accounts not requiring a password
- blank passwords are permitted
- Local Area Network Manager password hash is stored

Server configuration

- low disk space
- age of the hardware
- drivers are more than 10 years old
- missing settings

Disaster recovery documentation

- documentation does not cover common scenarios

At the time of our review, the agency had not remediated all findings from Microsoft's review.

The agency advised us that after the report was finalised, the DCSS provider, Microsoft, and the agency's ICT services team discussed the report findings. The DCSS provider has remediated certain findings in the short term, but further discussion and planning is needed to remediate the remaining findings.

We were also advised that a remediation action plan is being prepared, with the plan expected to be presented to a governance committee in early November 2016.

Microsoft's report recommends that critical issues identified be remediated immediately. Given the elapsed time between Microsoft finalising the report and the agency developing a detailed remediation plan, the risk of exposure to security vulnerabilities or operational issues across the AD environment is increased.

Agency responses

The agency acknowledged that it needs to document actions completed by the DCSS provider and remaining actions in a remediation plan based on Microsoft's action plan.

The remediation plan is expected to be presented to the ICT assurance and governance committee by the end of November 2016.

6.9 Privileged user activities not sufficiently logged and monitored

Recommendations

Agencies should consider opportunities to log and monitor privileged user activities in line with ISMF guidelines and agencies' accepted level of risk.

This should include periodic reviews of privileged user activity logs, with follow-up investigation as required.

Findings

ISMF Guideline 23 recommends that agencies implement appropriate event logging and monitoring processes to capture and examine events that may have an impact on the confidentiality, integrity or availability of information assets.

The guideline recommends that agencies log a number of events, including:

- user account and record actions, including access and changes
- successful and rejected authentication attempts, particularly for trusted user roles
- changes to information asset configuration, privileges or security-related services, including endpoint protection and intrusion detection systems
- privileged activities and any associated access control system alerts, including system or service start/stop.

Both agencies we reviewed log successful and rejected authentication attempts as part of standard AD event logging. However, neither agency logged or monitored the activities of AD privileged users.

Where privileged user activities are not sufficiently logged and monitored, user accountability is reduced. This may increase the risk that malicious behaviour is not detected or prevented.

Agency responses

Agencies advised us that they will review the recommendations and guidelines as per our Report. One agency had commenced initial discussions with the DCSS vendor regarding user activity logging and any associated overheads.

7 Mobile devices

Summary of key findings

The two agencies we reviewed had not implemented recommended best practice controls to effectively manage the use of mobile devices to access agency resources and data. We identified that:

- security controls applied to mobile devices do not meet best practice guidelines
- mobile access was not restricted by individual device
- security controls applied to Outlook Web Access (OWA) could be strengthened
- there was insufficient reporting of agency mobility usage
- mobile device policies and procedures were not regularly reviewed or approved.

We confirmed that a number of mobile device controls are managed at the whole-of-government level. Accordingly, some of the issues we identified may also apply to other agencies.

Where recommended controls have not been implemented over mobile devices, there is an increased risk to the confidentiality and integrity of sensitive agency data.

Summary of key recommendations

DPC should provide additional guidance to agencies about implementing mobile device management (MDM) software or other technical controls.

Agencies should:

- assess the feasibility of implementing an MDM software solution for corporate and personal mobile devices
- implement technical controls to restrict access to agency data by individual mobile devices
- assess the need to implement additional security controls across OWA, including two-factor authentication, restricting OWA to approved mailboxes only, and introducing controls to restrict users' access to download sensitive attachments in emails
- establish a regular reporting process for Microsoft Exchange mailboxes to meet business requirements and validate mailbox configuration
- review mobile device policies and procedures regularly (ie at least annually) and update them as required.

Although not all of these recommendations are based on mandatory ISMF requirements, they represent a more secure practice and may help to mitigate a number of potential risks.

7.1 Introduction

7.1.1 Background

Mobile devices, such as smartphones and tablets, allow access to SA Government resources and data remotely. Granting access to these resources and data can improve business efficiency, productivity and employee flexibility. However, they also introduce a number of risks. As summarised by the ASD, these risks can include:

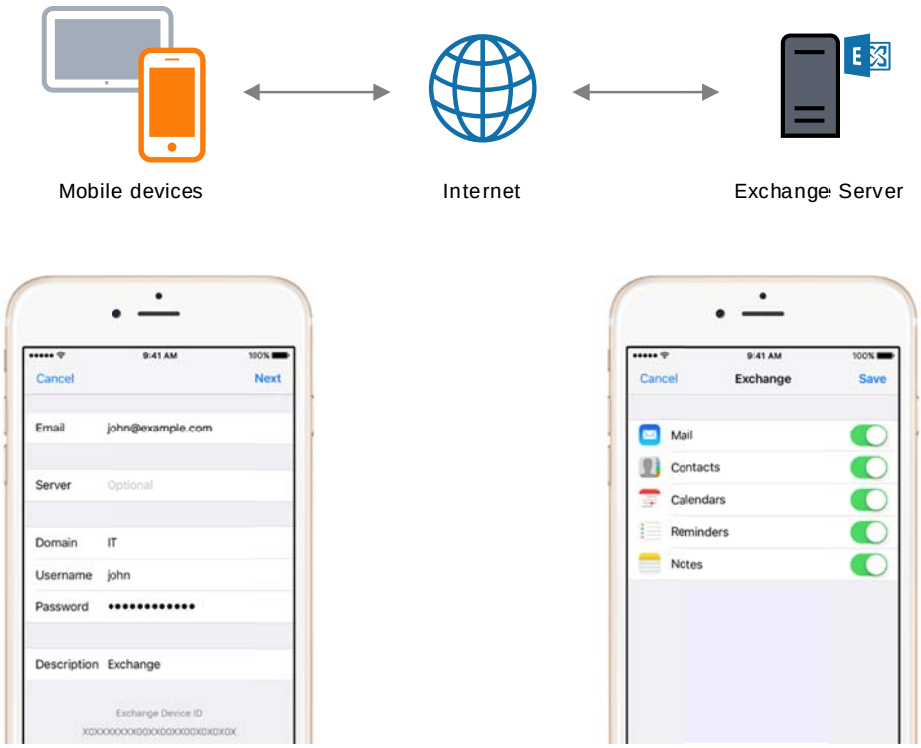
- loss or theft of devices storing unprotected sensitive data
- use of unapproved applications and cloud services to handle sensitive data
- inadequate separation between work-related use and personal use of a device
- reduced assurance over the integrity and security of devices that are not corporately managed.

7.1.2 Mobile device data access methods

Microsoft Exchange ActiveSync

Microsoft's Exchange ActiveSync functionality is a secure connection method for accessing and synchronising email, calendar and contact data to mobile devices as shown in figure 7.1. Exchange ActiveSync is the primary method permitted for users to access agency data on approved mobile devices.

Figure 7.1: Examples of Microsoft Exchange ActiveSync configuration on an iOS device



Microsoft Exchange ActiveSync enforces a minimum set of security requirements for connected devices. Mandatory requirements include:

- a PIN code to access the device
- a set lockout time
- a set number of attempts an incorrect PIN can be entered before the device data is wiped.

Outlook Web Access

OWA allows users to access their email, calendar and contacts via a web browser, including a browser on a mobile device. This service is offered as part of the whole-of-government Messaging and Business Communication Services contract (MBCS).

Examples of the OWA logon page and the functionality provided are shown in figure 7.2.

Figure 7.2:
OWA logon page on a desktop computer
Access is also available via mobile devices

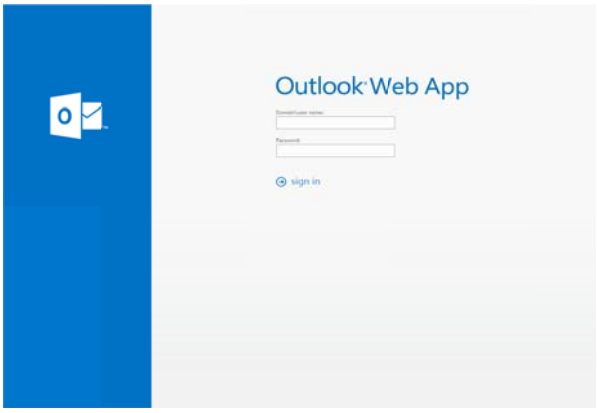
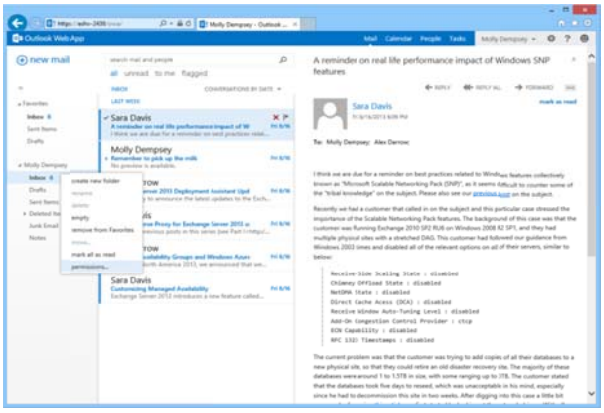


Figure 7.3:
Example of email functionality in OWA



7.1.3 Recommended security controls

ISMF Standard 141 requires agencies to establish and maintain security measures that ensure proportionate protection of endpoint devices. These measures should be relative to the confidentiality, integrity and availability of information being accessed or processed on these devices.

In addition, ISMF Guideline 18 states that agencies should implement policies, procedures and controls to prevent unauthorised device access, including those shown in figure 7.4.

Figure 7.4: ISMF recommendations for preventing unauthorised device access (by classification)

All information classifications	'For Official Use Only' and higher classifications
• establish a policy governing the use of mobile devices, including 'bring your own device' • manage all mobile devices through an MDM tool • require that mobile devices outside of physical security controls are not left unattended.	• encrypt sensitive information on mobile devices according to agency information security policies • establish procedures for sensitive mobile device information output, transfer, reallocation and disposal • implement formal procedures for accessing business information across public networks.

MDM software allows agencies to monitor, manage and secure mobile devices across multiple device types. This includes the ability to identify unauthorised mobile devices connecting to the network. The software can also isolate sensitive agency data within 'containers' or standalone apps on a mobile device.

7.2 Audit approach

Our objective was to determine whether agencies are effectively managing the use of mobile devices to access agency resources and data.

This included assessing whether:

- defined policies and procedures exist for requesting access to agency data from a mobile device
- agencies have implemented recommended controls to manage mobile devices and access to sensitive data, including via the use of MDM software
- sensitive data accessible via mobile devices is encrypted in transmission and while stored on devices.

We reviewed two SA Government agencies. DPC was not originally included, but feedback from the agencies we reviewed suggested that a number of mobile device controls are managed at a whole-of-government level. For example, certain controls are managed by an external vendor as part of the MBCS contract. We understand that DPC's Strategic Procurement team manages this contract.

Accordingly, we made a series of recommendations for DPC to consider. This includes improvements to mobile device controls at a whole-of-government level. We made similar recommendations to the two other agencies reviewed.

7.3 Security controls applied to mobile devices do not meet best practice guidelines

Recommendations

DPC should provide additional guidance to agencies about implementing MDM software or other technical controls.

Agencies should assess the feasibility of implementing an MDM software solution for corporate and personal mobile devices.

As part of this, agencies should ensure that access is restricted to sensitive agency data. This should include considering:

- segregating agency data from other data on mobile devices (including data on personal devices)
- enforcing the encryption of agency data stored on mobile devices
- preventing the copying or transfer of agency data to other mobile apps, email accounts or cloud services.

Findings

We found that a number of agencies had not implemented MDM software or other controls to meet best practice guidelines.

One of the agencies we reviewed advised us that it was discussing options for implementing MDM with external vendors. This includes exploring the MDM software available through the across-government Network Carriage Service contract. At the time of our review, the agency was still in discussions with vendors and had not finalised a time frame to implement an MDM solution.

Agencies advised us that they rely on whole-of-government security controls within Microsoft Exchange ActiveSync (refer section 7.4). However the whole-of-government controls have certain limitations, meaning that agencies are unable to:

- segregate agency data from other data on mobile devices (including data on personal devices)
- enforce the encryption of corporate data stored on mobile devices
- prevent the copying or transfer of agency data to other mobile apps, email accounts or cloud services.

There is therefore an increased risk of exposure or inappropriate transfer of sensitive agency data.

Agency responses

DPC advised us that it will review the above recommendation and assess the availability and ability of technical security controls or MDM software to provide additional guidance for agencies to reinforce security on mobile devices.

It expects to complete this assessment by February 2017.

Agencies confirmed that they would seek advice from DPC given that security controls for mobile devices need to be addressed across all agencies. Agencies also confirmed that they would assess MDM functionality to determine the benefits of enhancing existing controls against the associated risks and business benefits. One agency was planning to prepare a business case during the first quarter of 2017. This business case will assess the costs, benefits (including risk mitigation) and risks of MDM or other solutions to manage risks associated with mobile devices.

7.4 Mobile device access not restricted by individual device

Recommendations

Agencies should implement technical controls to restrict access to agency data by individual mobile devices. This may require agencies to liaise with DPC and/or the external vendor for the whole-of-government MBCS contract.

Alternatively, agencies should consider restricting access to data by individual devices as part of a potential MDM implementation (refer section 7.3).

Findings

At the agencies we reviewed, employees wishing to use Microsoft Exchange ActiveSync on a mobile device needed to complete an application form and have it approved.

Once approved, agency ICT staff configure the relevant account in an online portal. This activates Microsoft Exchange ActiveSync features for the user's account, rather than specifying an individual device. This allows the user to connect from any mobile device with their logon credentials.

Although a device connecting through Microsoft Exchange ActiveSync must meet certain security requirements (such as a mandatory PIN code), the user is able to add multiple devices that can access potentially sensitive agency data on:

- personal devices, contravening some agencies' established policies
- multiple corporate devices, where access has not been formally approved.

This increases the risk of potential exposure of sensitive data from an unapproved mobile device.

Agency responses

DPC advised us that it will assess the availability of additional technical controls to provide the ability for agencies to restrict access to their data by individual mobile devices.

It expects to complete this assessment by February 2017.

Agencies advised us that they are assessing MDM functionality to address this specific recommendation. One agency was also planning to review its mobile device procedures to identify whether they could be updated to include the requirement to approve mobile device access by individual device.

7.5 Security controls applied to Outlook Web Access could be strengthened

Recommendations

Agencies should assess the need to implement additional security controls across OWA, including:

- enabling two-factor authentication for OWA outside of StateNet
- restricting OWA to approved mailboxes only by default
- assessing opportunities to restrict users' access to download sensitive attachments in emails via OWA.

This may require agencies to liaise with the external vendor for the MBCS contract.

Findings

We identified that access to OWA is granted by default to all new mailboxes managed by the MBCS contract. Some agencies advised us that as a compensating control, they manually disable OWA when creating new mailboxes.

OWA access is restricted via single-factor authentication using employees' AD usernames and passwords. This means that OWA access follows the same password and account lockout settings as AD. However, we noted that two-factor authentication (such as the use of a token device or temporary SMS code) is not required. DPC advised us that OWA was exempted from the StateNet conditions of connection.

Additionally, there are no restrictions enabled in OWA to prevent users from downloading attachment files from potentially sensitive email messages.

To help reduce this risk, some agencies advised us that users are required to classify the sensitive data in emails using specialised software. However, there were instances where technical controls had not been implemented to restrict sharing or downloading emails and attachments based on the assigned classification.

DPC and the external vendor advised us that a third party solution may need to be investigated to provide this functionality at an additional cost. This functionality is not presently provided by the external vendor.

Although two-factor authentication and OWA file restrictions are not mandatory ISMF requirements, they represent a more secure practice and mitigate a number of potential risks.

An OWA user would still need to authenticate within existing AD security settings. However, implementing these additional controls significantly reduces the likelihood of unauthorised access.

We acknowledge the need to balance security requirements with aims for increased employee flexibility and mobility. However, the current level of security controls applied to OWA across multiple government agencies increases the risk that sensitive agency data is exposed or inappropriately downloaded to a personal computer.

Agency responses

DPC advised us that it will assess the requirement and availability of additional security controls for OWA. It expects to complete this assessment by February 2017.

One agency advised us that it is currently assessing MDM functionality within its existing environment to assess the benefits of enhancing existing controls against risks and business requirements. The recommended approach will ultimately be considered at a future ICT committee meeting during 2017.

The other agency confirmed that it will engage with DPC and the external MBCS vendor about additional security controls to be addressed on an across-government level. We were advised that discussions had commenced with the vendor.

Although two-factor authentication may not be available at the agency level for OWA, the agency was seeking further information to confirm this. The MBCS vendor advised that an SMS-based two-factor solution for all government agencies may be possible.

Additionally, the agency confirmed that access to OWA was disabled by default under the previous contract arrangements but is now enabled by default under the MBCS arrangements. It has requested that the MBCS vendor change the default setting.

7.6 Insufficient reporting of agency mobility usage

Recommendations

DPC should liaise with the external MBCS vendor to establish a regular reporting process for Microsoft Exchange mailboxes, including mailbox user details, OWA/Exchange ActiveSync configuration and the specific devices being used to access the mailbox.

DPC should also confirm the frequency of the reports needed to meet business requirements and validate mailbox configuration.

Findings

Under the previous SA Government Electronic Messaging Service contract, SA Government agencies received regular reports on Microsoft Exchange mailboxes. The reports included each mailbox's user details and the status of OWA or Microsoft Exchange ActiveSync mobility features (enabled or disabled).

At the time of our review, the MBCS vendor had not finalised the equivalent reporting for the new contract. However, agencies advised us that ad hoc reports could be requested from the vendor if required. We understand that some agencies have requested additional reports on mailboxes from the vendor. At the time of our review, the vendor was only supplying reports about service levels.

Without these regular reports, agencies are unable to confirm the number of mailboxes and the status of mobility features for all mailboxes. This includes identifying the specific mobile devices each user has configured to access their mailbox.

This increases the risk that additional devices have been configured for Microsoft Exchange ActiveSync mobility outside of standard approval processes and agencies are unable to detect their use.

Agency responses

DPC and other agencies confirmed that they are continuing discussions the MBCS vendor to establish the required reporting process.

7.7 Mobile device policies and procedures not regularly reviewed or approved

Recommendations

Agencies should review mobile device policies and procedures regularly (ie at least annually) and update them as required.

Findings

We obtained several policies and procedures relating to mobile devices. We found that a number of these policies and procedures at one agency were overdue for review or were still in a draft status. This included:

- mobile devices policy
- electronic communications guideline
- acceptable use of information assets policy.

Documented policies, procedures and work instructions are an integral part of an organisation's control environment. Where they are not in place or not current, employees may not understand their roles and responsibilities and may not meet management's expectations.

Agency responses

The agency advised us that it has commenced a program of reviewing IT policies. Since the audit, four new policies have been distributed for staff consultation prior to formal approval. A further five policies are expected to be distributed for staff consultation by 31 December 2016.

The standard review period for policies at the applicable agency is two years.

8 Application whitelisting

Summary of key findings

We reviewed two agencies and confirmed that neither had implemented application whitelisting. This means that the agencies cannot fully prevent unauthorised or malicious programs and software libraries from executing.

However, one agency was considering implementing application whitelisting after a recent security incident involving a malicious application. Application whitelisting would likely have prevented this malicious activity, or minimised the impact of the incident.

We also identified that:

- no documentation or approval was recorded for a software installation at one agency
- periodic application reviews are not performed at one agency and documentation is not retained at another agency
- information security policies at one agency are in draft, pending review and approval.

Summary of key recommendations

Agencies should:

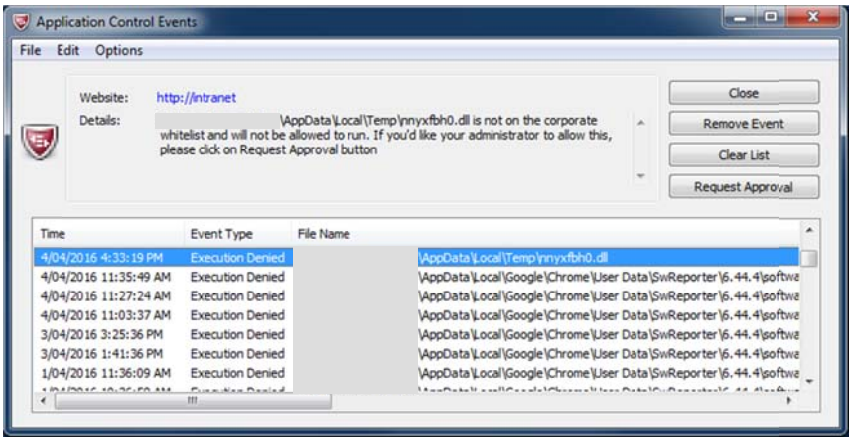
- implement application whitelisting on servers and workstations in line with the recommendations of the ISMF and the ASD
- ensure that all software installation requests are documented and their approval recorded by the IT service desk
- implement quarterly reviews of all applications installed on workstations
- document the results of each periodic application review performed, removing inappropriate or unneeded applications
- review and approve the information security procedures and guidelines promptly.

8.1 Introduction

Application whitelisting is a security control designed to protect against unauthorised and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries can be executed, based on a predefined whitelist. All other programs and software libraries are prevented from executing.

Figure 8.1: Example log from application whitelisting software

The log confirms that the user could not execute non-approved programs and software libraries



The ASD considers application whitelisting to be the number one security practice in terms of return on investment. Additionally, controls in ISMF Standard 141 require agencies to consider implementing application whitelisting to prevent the use of applications that have not been sanctioned by the agency, are not adequately tested or are not required by the user to perform their duties.

ISMF Guideline 18 states that agencies should implement a formal policy prohibiting the use of unauthorised applications. Agencies should also implement processes for authorising applications for deployment into the production environment, as well as suitable configuration techniques to prevent unauthorised applications from being executed. Applications should be deployed based on device users' role-specific functions and activities.

For operating environments where information is classified as 'Sensitive: Legal' or Sensitive: Commercial', ISMF Guideline 18 recommends that agencies conduct quarterly application reviews and examine unapproved applications. All operational application updates should be logged and monitored, with whitelisting discrepancies reported to the relevant business owner.

The SA Government's Top 10 cyber security objectives include a requirement that agencies implement application whitelisting in logging mode at a minimum. The Top 10 recommends that agencies strongly consider fully implementing application whitelisting, with central collection of logs and enforcement.

8.2 Audit approach

Our objective was to determine whether agencies are effectively securing their servers and workstations using application whitelisting.

We assessed this by determining whether:

- defined policies and procedures prohibit the use of unauthorised applications and require approval of applications for deployment into the production environment
- agencies have implemented technical controls to prevent the execution of unauthorised applications and software libraries using a predefined whitelist
- where information is classified as 'Sensitive: Legal or Commercial', periodic application reviews are performed to review unapproved applications.

8.3 Application whitelisting not implemented at two agencies

Recommendation

Agencies should implement application whitelisting on servers and workstations in line with ISMF and ASD recommendations.

Findings

Neither of the two agencies we reviewed had implemented application whitelisting on any of their servers or workstations.

Further, we determined that seven government agencies (including one of the agencies we reviewed) experienced an IT security incident in May 2016 involving a malicious application known as Cryptolocker. Cryptolocker encrypts any network folders and files it has access to, then demands a ransom for decryption of the files.

At the agency we reviewed, Cryptolocker encrypted approximately 5000 files on the network. IT personnel were able to recover most affected files from a backup tape created the previous night. However, application whitelisting would likely have prevented this malicious activity, or minimised the impact of the incident.

In August 2016, that agency advised us that it was in discussions with a software vendor to procure an application whitelisting solution. It advised that if the procurement was approved, the solution would be implemented by 31 December 2016.

In the absence of application whitelisting, both agencies advised us that they had implemented the following restrictions for software installations on workstations:

- there is limited access to domain administrator and local administrator rights on servers and workstations
- processes exist for requesting and approving software installations via IT service desks
- one agency's web gateway blocks certain web services with potential security risks (such as the cloud file sharing service, Dropbox).

Where application whitelisting has not been implemented, agencies cannot fully prevent unauthorised and malicious programs and software libraries from executing.

Agency responses

Both agencies responded positively with details of planned remediation.

One agency advised that it will define a program of activity to implement appropriate whitelisting. Initially, the program will determine the most appropriate form of application whitelisting and develop the business case for implementation, The program will analyse application whitelisting options and develop a business case by end of June 2017. The implementation project will run from July to December 2017.

The other agency advised us that it had already commenced identifying an appropriate solution, with assistance from the ODG.

The agency has since identified a suitable software solution, which will be piloted on a number of workstations during November 2016. The results of this testing will be evaluated. Assuming a positive result, the agency expects a full rollout of application whitelisting controls by 31 December 2016.

8.4 No documentation or approval recorded for a software installation

Recommendations

Agencies should:

- ensure that all software installation requests are documented and their approval recorded by the IT service desk
- reiterate requirements for staff to submit requests for software installations to the service desk.

Findings

As noted in section 8.3, the two agencies we reviewed have established processes for requesting and approving software installations via the IT service desk. However they had not implemented application whitelisting. Given this, we reviewed a sample of software installations on workstations in each agency.

Our testing at one agency identified that one of the three sampled software installations reviewed did not have a request logged with the IT service desk. We could not identify any documented approval for this software.

Where software installation requests are not documented and approved, there is a risk that inappropriate or unsuitable software is installed on end user workstations. This may increase the risk of malicious software activity.

Agency response

Users within the agency do not normally have administrative rights on their computers to install software. An exception to this is the developers within the ICT team. These developers regularly install and/or update many unique pieces of software to assist them in their work.

In this instance, the software was installed by a developer with administration rights to their assigned PC. The developer concerned has been counselled and the software has been removed.

The agency will review whether current practices for developers are sufficient or whether more stringent controls need to be implemented. It will also immediately ensure that all staff with local administrator or privileged rights are reminded of their responsibilities.

The agency will also review local administrator or privileged rights and ensure that only appropriate personnel are provided with such rights.

It expects to complete these processes by June 2017.

8.5 Periodic application reviews not performed and documentation not retained

Recommendation

Agencies should implement quarterly reviews of all applications installed on workstations.

Agencies should also document the results of each periodic application review performed. Inappropriate or unneeded applications should be removed from workstations.

Findings

For agency environments where information is classified as 'Sensitive: Legal' or 'Sensitive: Commercial', ISMF Guideline 18 recommends that agencies conduct quarterly reviews of installed applications. These reviews should examine any unapproved applications.

Both of the agencies we reviewed use Microsoft SCCM to manage their workstations. This includes the ability to generate reports on installed software.

Figure 8.2 lists the issues we identified at the two agencies we reviewed.

Figure 8.2: Extent of application reviews implemented

Agency 1	**No formal application review process:** • Microsoft SCCM reports are available but are not formally reviewed. • An external vendor conducts an annual Microsoft licencing review to assess expected versus actual number of software installations. This review does not include all installed software. • We were advised that the agency has reviewed other software products previously. However, these have not been reviewed within the last 12 months.
Agency 2	**Application reviews conducted but not documented:** • All workstation applications are reviewed every two to three months to identify non-standard software. These reviews are performed using a report from Microsoft SCCM. • Although this process is a proactive control, we noted that the agency does not document the results of these reviews.

Where all installed applications are not regularly reviewed for appropriateness, there is a risk that unauthorised or potentially malicious applications are running on workstations.

Where documentation of application reviews is not maintained, we cannot verify that the reviews are being performed regularly.

Agency responses

Agencies responded positively with details of planned remediation. Both agencies advised us that they expect to implement our recommendation by December 2016.

8.6 Information security procedures and guidelines in draft status

Recommendations

Agencies should have approved information security policies, procedures and guidelines in place.

Agencies should review policies and procedures regularly (eg at least annually) and update them as required.

Findings

At the time of our audit, one agency was reviewing its framework of IT policies. The agency advised us that this review aimed to streamline the approval and administration of their policies.

We noted that 18 of the agency's information security procedures and guidelines were in draft and had not been approved. This included policies and procedures relating to software installations.

Documented policies, procedures and work instructions are an integral part of an organisation's control environment. Where they are not in place or not current, employees may not understand their roles and responsibilities and may not meet management's expectations.

Agency responses

The agency responded positively with details of planned remediation. It is expected all procedures will be reviewed and approved by April 2017.

9 Additional issues identified

Summary of key findings

- There were additional areas of non-compliance with the Top 10 objectives at one agency.
- One agency had not reported its progress on implementing the Top 10 objectives to the ODG.

Summary of key recommendations

- Agencies should remediate areas of non-compliance or partial compliance with the requirements of the Top 10 objectives.
- Agencies should submit quarterly submissions to the ODG and annual submissions to Cabinet promptly, under the mandated process.

9.1 Introduction

During our review, we identified additional issues relating to agencies' compliance with the Top 10 cyber security objectives (administered by the ODG).

These issues are detailed below.

9.2 Additional areas of non-compliance with the Top 10 objectives identified at one agency

Recommendation

Agencies should remediate the areas of non-compliance or partial compliance with the requirements of the Top 10 objectives.

Findings

We reviewed a September 2016 memo to one agency's ICT and Strategy Board about that agency's compliance with the Top 10 cyber security resilience and preparedness objectives. The memo and the agency's first quarter self-assessment response highlight many areas of non-compliance or partial compliance with the Top 10 requirements, in addition to the areas covered by our audit.

These additional areas of non-compliance or partial compliance include:

- no security vetting and clearances for users with administrative privileges
- no security vetting for IT Security Advisor and Agency Security Executive appointments
- no dedicated IT Security Advisor
- no information security governance
- no information security response plan

- no information classification systems within ICT environments
- limited application of classification and dissemination limitation marking on official information assets
- no routine penetration testing of sector websites and web applications
- limited progress towards developing and implementing an information security management system that complies with the ISMF
- limited technical interventions to protect user environments
- limited assurance that web services and web applications maintain compliance with SA Government security standards
- no resources within existing team to address deficiencies.

The memo includes an action plan to partially address the deficiencies raised. Although the plan addresses many of the requirements and assesses actions, activities and resources required in both the short and longer terms, it does not attempt to deliver full compliance against the Top 10 requirements.

This is because it was internally assessed by the agency that full compliance cannot be achieved in a practical or cost effective way. For example, requirements for assigning dissemination limiting markers on all records created or amended from May 2012 would involve reviewing over three million records.

The memo identifies a need for 2.5 FTEs for 12 months and a residual of 1.5 FTEs ongoing.

The cyber security control deficiencies identified represent a high risk for that agency. Specifically, where agencies do not fully comply with Top 10 requirements and better practice recommendations, there is an increased risk of security vulnerabilities affecting the confidentiality, integrity and availability of agency data.

We acknowledge that these risks will need to be assessed against the estimated remediation costs, with action taken where deemed feasible.

Agency response

The agency advised us that it has developed an action plan to address the information security deficiencies highlighted in the memo. However, at this stage, it was unable to allocate the necessary resources due to budget constraints. It will continue to pursue resourcing options through upcoming budget processes.

9.3 Progress of implementing Top 10 objectives were not reported to the Office for Digital Government at one agency

Recommendation

Agencies should submit quarterly submissions to the ODG and annual submissions to Cabinet promptly, under the mandated process.

Findings

One agency we reviewed had not reported to the ODG on the Top 10 objectives. At the time of our audit, the agency had not prepared a submission for quarter 1 or quarter 2, 2016.

The agency advised us that it intends to submit a report to the ODG as soon as possible.

If these reports are not submitted, the ODG cannot determine agencies' progress in meeting the Top 10 objectives. Therefore, the ODG cannot adequately inform Cabinet of agencies' implementation progress, in line with the Cabinet-approved process.

Agency response

An Implementation Plan for the Top 10 security objectives will be established and lodged with the ODG by end of December 2016. The agency will then provide annual updates to the plan as requested.

We were advised that the agency has made significant progress in the implementation of the Top 10, even if this has not been documented.

The agency has submitted the report for the second quarter on the Top 10 objectives to the ODG and will continue to provide the quarterly reports as requested.