Report of the Auditor-General

Auditor-General's Department

Report 2 of 2024

ICT asset management

Government of South Australia

[P.P.4T

Report of the Auditor-General

Report 2 of 2024

ICT asset management

Tabled in the House of Assembly and ordered to be published, 6 February 2024

First Session, Fifty-Fifth Parliament

By authority: T. Foresto, Government Printer, South Australia

2024

The Auditor-General's Department acknowledges and respects Aboriginal people as the State's first people and nations, and recognises Aboriginal people as traditional owners and occupants of South Australian land and waters.

Auditor-General's
Department

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000

Tel +618 8226 9640

ABN 53 327 061 410

audgensa@audit.sa.gov.au

www.audit.sa.gov.au

5 February 2024

President Legislative Council Parliament House ADELAIDE SA 5000	Speaker House of Assembly Parliament House ADELAIDE SA 5000

Dear President and Speaker

Report of the Auditor-General:
Report 2 of 2023 *ICT asset management*

As required by the *Public Finance and Audit Act 1987*, I present to each of you this Report.

Content of the report

The increased complexity of ICT environments and risk of cyber security threats is reinforcing the need for agencies to have clear visibility and understanding of their ICT assets. To protect these assets and meet the requirements of the South Australian Cyber Security Framework, all agencies need to establish and maintain ICT asset management controls.

Our objective was to conclude on the ICT asset management controls applied by agencies.

Our testing was designed to confirm the controls applied over key aspects of the ICT asset management lifecycle. This included scanning a sample of ICT assets connected to agency networks, such as end-user computers, servers and network devices.

Our review did not highlight any major concerns with ICT asset management practices in the agencies we reviewed. We did note that controls varied across agencies and we identified several areas for improvement.

For security reasons we have not identified the individual agencies we reviewed, but we have provided detailed findings to each of them.

Acknowledgements

The audit team for this report was Andrew Corrigan, Tyson Hancock and Abhinav Tomar.

We appreciate the cooperation and assistance given by staff of the agencies we reviewed.

Yours sincerely

Andrew Blaskett
Auditor-General

Contents

Audit snapshot

What we reviewed and why

The increasing complexity of ICT environments and risk of cyber security threats reinforces the need for agencies to have clear visibility and understanding of their ICT assets. To protect these assets and meet the requirements of the South Australian Cyber Security Framework, all agencies need to establish and maintain ICT asset management controls.

We reviewed the ICT asset management controls applied by six SA Government agencies from a variety of sectors.

What we found

We had no major concerns with the ICT asset management practices of the agencies we reviewed. Their controls varied, and we did identify some areas to improve. Our key findings included:

- ICT asset scanning and discovery discrepancies
- gaps in documented ICT asset management procedures
- inconsistent management of ICT assets
- gaps in documented ownership and classification of ICT assets
- a lack of periodic review and monitoring of ICT assets
- gaps in ICT asset sanitisation and disposal.

Good ICT asset management controls

Documented procedures for onboarding, managing and offboarding ICT assets

Vendor service monitoring arrangements

Well maintained centralised ICT asset registers, with owners and classifications listed

Documented procedures for monitoring ICT asset sanitisation and destruction

1 Executive summary

1.1 Introduction

The South Australian Cyber Security Framework (SACSF)[1] describes an information asset as 'any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people and physical documents.'

The increased complexity of ICT environments and risk of cyber security threats is reinforcing the need for agencies to have clear visibility and understanding of their ICT assets. To protect these assets and meet the requirements of the SACSF, all agencies need to establish and maintain ICT asset management controls.

The SACSF requires information assets that support critical processes to be identified and recorded in an information asset register. They should also be formally assigned an owner and processes put in place to label, store, handle and dispose of them in a way that aligns with their classification. A key objective of the SACSF is to maintain the confidentiality, integrity and availability of information assets.

In addition to security risks posed by poor ICT asset management, having weak asset management controls can result in overpaying licencing and support costs and poor performance.

We assessed the ICT asset management controls applied across the SA Government by selecting a sample of six agencies from different sectors. This included identifying the ICT assets connected to agency networks, such as network and server infrastructure and end-user computers. For most agencies, we also used an ICT asset discovery tool.[2] In performing this review we took into account the fact that agencies use different processes, controls and IT systems to track and manage the ICT assets that support their business processes. This includes using a range of different ICT vendor services.

Our testing covered the period from May to September 2023. It was conducted with the assistance of an external specialist firm.

1.2 Conclusion

We did not identify any major concerns with the ICT asset management practices at the agencies we reviewed. Controls varied across these agencies and we identified several areas for improvement.

[1] The SACSF is a risk-based framework developed by the Department of the Premier and Cabinet. It aims to help agencies preserve the confidentiality, integrity and availability of their information by applying appropriate cyber security management processes. It is a mandatory framework for SA Government agencies.

[2] A tool that scans an IT network to detect connected hardware and software assets and returns detailed information about them.

Our ICT asset scanning and discovery exercise identified a risk that assets are not recorded on agency ICT asset registers. Although some agencies provided reasons for these discrepancies, the full extent of the unmatched assets could only be identified through further analysis.

Most agencies need to better define and document their ICT asset management practices, including the allocation of roles and responsibilities between agencies and their ICT vendors. Agencies also needed to strengthen their periodic review processes and confirm asset disposal and monitoring arrangements.

1.3 What we found and recommended

Our key findings and recommendations are summarised in figure 1.1, with more details provided in chapters 4 and 5.

Figure 1.1: Key findings and recommendations

Finding	Recommendation
ICT asset scanning	
ICT asset scanning and discovery discrepancies (section 4.1.1)	Agencies should review the additional ICT assets we identified in our scanning and discovery process and address any issues. Agencies should also consider performing their own periodic network scanning to ensure their ICT asset registers are complete and accurate.
Governance	
Gaps in documented ICT asset management procedures (section 5.1.1)	Agencies should review and update their ICT asset management procedures to reflect their current practices. These procedures should cover the entire ICT asset management lifecycle and the key roles and responsibilities for agencies and their ICT vendors. In addition, internal assurance activities over ICT vendor activities should be documented.
Inconsistent management of ICT assets (section 5.1.2)	Agencies should establish a central record to manage their ICT assets. Agencies should consider implementing automated notifications to all stakeholders when staff movements occur.

Finding	Recommendation
Gaps in documented ownership and classification of ICT assets (section 5.1.3)	Agencies should formally assign ICT information assets to an owner and classify them in their ICT asset registers. For most agencies, we also recommended that they review their ICT asset registers and address the missing or inaccurate information we identified.
Lack of periodic review and monitoring of ICT assets (section 5.1.4)	Agencies should periodically review the ICT assets connected to their networks and update their ICT asset register accordingly. This may require a network discovery tool. Review requirements should be formally documented, including roles and responsibilities for discovering and following up unknown or suspicious devices.
Gaps in ICT asset sanitisation and disposal (section 5.1.5)	Agencies should ensure that ICT assets have been appropriately sanitised on decommissioning.[3]

1.4 Response to our recommendations

Most agencies responded positively to our findings and recommendations with details of their remedial actions and ongoing ICT asset management strategies.

Two agencies raised a concern with our assessment of the level of documentation they maintain to support their ICT asset management (sections 5.1.1 and 5.1.3).

Another agency raised concerns about aspects of our findings and recommendations, particularly the administrative overhead to implement some recommendations and robustness of other mitigating controls.

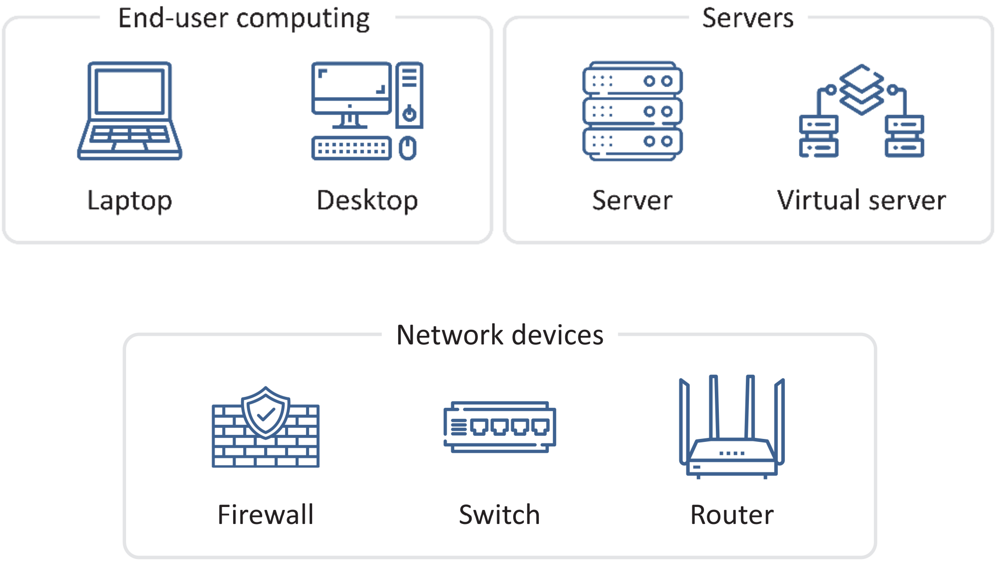
[3] Sanitising an ICT asset before decommissioning is the process of securely removing all sensitive or confidential data from it to prevent unauthorised access or data breaches. It ensures no residual data remains on the asset after it is taken out of service.

2 Background

Agencies provide critical services to the South Australian public and are increasingly becoming targets of malicious cyber attacks. They rely heavily on their ICT assets to support their operations and to store, process and secure agency data.

An ICT asset can be the hardware or software used to process agency information.

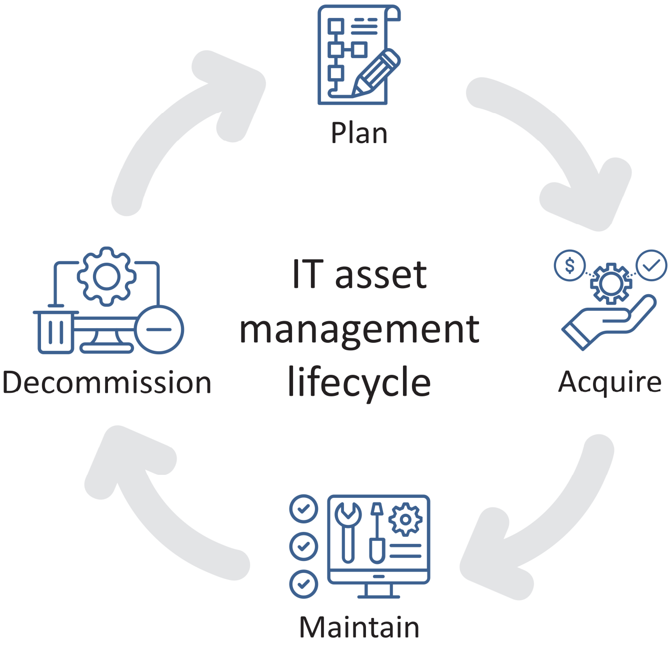
Figure 2.1: Examples of ICT assets



Proper ICT asset management practices are fundamental for agencies to maintain a clear understanding of the ICT assets operating on their networks and any potential security risks. Good governance helps to efficiently apply ICT resources to agency ICT operations, optimises ICT investments and support costs, and helps reduce the risks associated with ICT assets reaching their end of life.

Maintaining an accurate and centralised ICT asset inventory, including tracking ICT assets and the IT asset management lifecycle, helps inform short and long-term decisions to meet agency ICT goals, including modernising and digitising the network. It also allows an agency to improve its maintenance activities and network performance. This includes ensuring assets are appropriately maintained by applying adequate security settings and patches to address security threats.

Figure 2.2: Key phases of the ICT asset management lifecycle



3 Review mandate, objective and scope

3.1 Our mandate

The Auditor-General has authority to conduct this review under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987.*

3.2 Our objective

Our objective was to conclude on the ICT asset management controls applied by SA Government agencies.

Our testing was designed to confirm the controls applied over key aspects of the ICT asset management lifecycle. This included scanning a sample of ICT assets connected to agency networks, such as end-user computers, servers and network devices.

3.3 What we reviewed and how

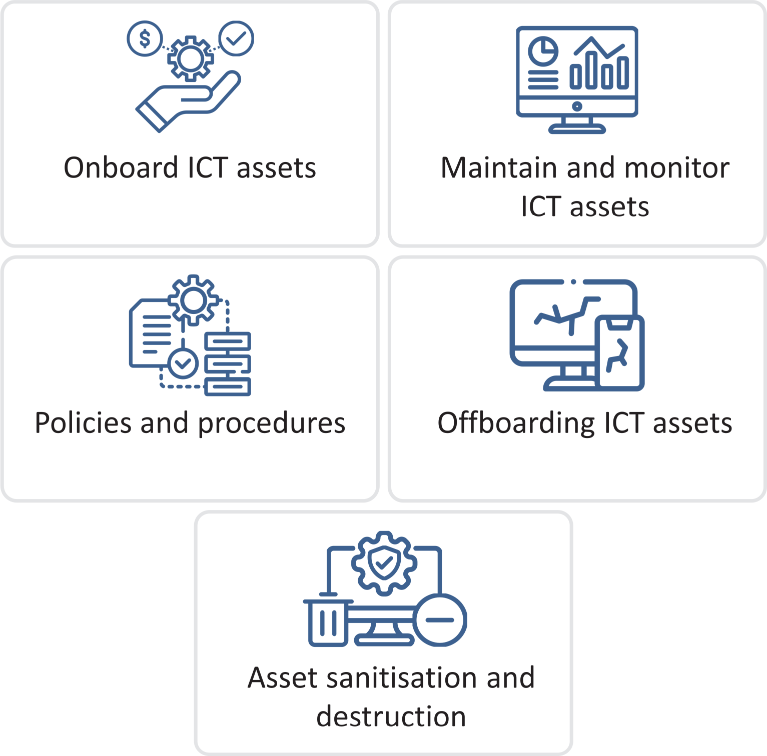
To conduct our testing, we selected a sample of six agencies from a variety of sectors. We reviewed the following areas to determine whether those agencies had established appropriate ICT asset management controls:

- procedures for onboarding, managing and offboarding ICT assets (end-user computers, servers and network devices) and ICT asset monitoring
- ICT asset registers, including asset ownership and classification
- procedures for periodic reviews of ICT assets and their sanitisation and destruction
- vendor service monitoring arrangements.

Our testing involved:

- conducting workshops with key stakeholders to understand current agency ICT asset management processes and the asset lifecycle
- reviewing available documentation
- performing an ICT asset network scanning and discovery exercise
- comparing scanned and provided discovery data against existing agency ICT asset registers and vendor billing data.

Figure 3.1: Elements of the IT asset management lifecycle that we reviewed


Onboard ICT assets
Maintain and monitor ICT assets
Policies and procedures
Offboarding ICT assets
Asset sanitisation and destruction

3.4 What we did not review

Our review had a specific focus on the ICT asset management controls applied by agencies.

We did not test all ICT asset management processes, including all of the processes agencies have established with their ICT vendors.

Agencies did not provide us with a consistent level of detail and format of information in their server and network device registers. As such, we were not able to conduct the same level of testing of these registers as we did for end-user computers (section 5.1.3).

We did not validate the appropriateness of the devices we identified in our ICT asset scanning and discovery exercise.

4 ICT asset scanning

4.1 Detailed findings

4.1.1 ICT asset scanning and discovery discrepancies

Recommendation

We recommended that agencies review the additional ICT assets we identified in our scanning and discovery process and address any issues.

Agencies should also consider performing their own periodic network scanning to ensure ICT asset registers are complete and accurate. This will also help agencies ensure that they are only being billed by ICT vendors for their current operational ICT assets.

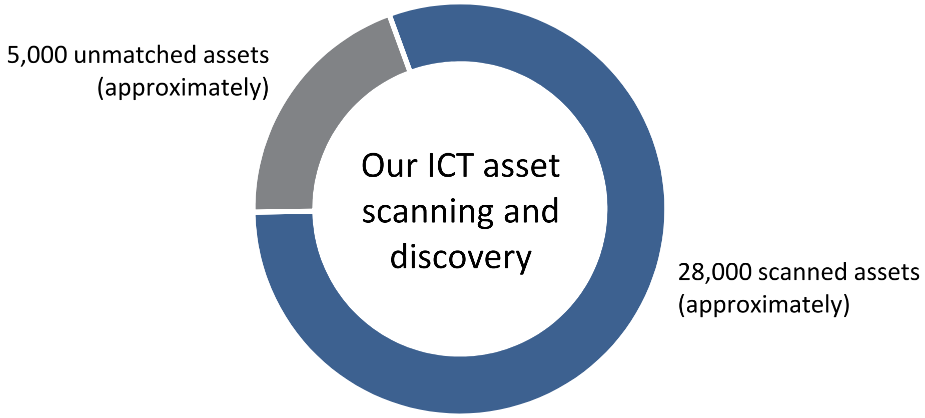
Finding

As part of our testing, we conducted network scanning and discovery exercises to identify the ICT assets running on agency networks (end-user computers, servers and network devices) and compare them to those listed in agency ICT asset registers and ICT vendor billing lists.

Our testing included the use of an ICT discovery tool for some agencies. The data sources available varied between agencies and prevented us from discovering all in-scope ICT assets connected to agency networks.

Figure 4.1 summarises what we found.

Figure 4.1: Summary of ICT asset matching results



Agencies advised us that some of the discrepancies we identified may have been due to:

- timing differences in when the information was obtained
- decommissioned assets not yet removed from asset registers
- devices owned by other agencies or ICT vendors

- subcomponents not considered to be ICT assets
- workforce mobility
- machinery of government changes.

The full extent of the discrepancies could only be identified through further analysis.

We also found that some agencies were being billed for ICT assets that did not appear in their ICT asset register. Two agencies advised us that some ICT components appear on vendor billing lists but are not considered to be ICT assets, such as a subcomponent (module) of a network device.

Why this is important

It is important to periodically use ICT network discovery tools to ensure that only known, approved ICT assets are operating on agency networks. Good asset management requires good asset identification.

Having a clear understanding of ICT assets in operation helps to optimise costs, including vendor billing, appropriately allocate ICT resources and make informed business decisions. It also helps to maintain the performance and security of the network and reduces the risk of unauthorised or inappropriate access to agency data.

5 Governance

5.1 Detailed findings

5.1.1 Gaps in documented ICT asset management procedures

Recommendation

We recommended that agencies review and update their ICT asset management procedures to reflect current practices and provide guidance when onboarding, managing and offboarding ICT assets.

These documented procedures should be endorsed and outline the ICT asset management lifecycle, including key roles and responsibilities for both the agency and ICT vendors. To remain current they should be regularly reviewed to reflect any changes and be communicated to all staff who need them.

To help ensure ICT vendors comply with their responsibilities, vendor performance reporting on ICT asset management should be reviewed. Key outcomes from these reviews and any supporting vendor meetings should be documented.

Finding

We reviewed ICT asset management process documentation covering end-user computers, servers and network devices for the six agencies we selected.

Most agencies had developed some supporting documentation, but we identified the following gaps:

- The ICT asset management procedures for some agencies did not include guidance for the whole ICT asset lifecycle. This included onboarding, managing and offboarding of ICT assets and processes for updating ICT asset registers.
- Some agencies had not reviewed and updated their ICT asset management procedures to reflect current processes.
- Some agencies had not documented procedures for all ICT assets, such as server and network devices.
- Some agencies had not documented all roles and responsibilities for their agency and their ICT vendors.
- One agency had not documented the outcomes of ICT asset vendor performance meetings.
- One agency had not documented the internal assurance activities it performs to confirm the accuracy of what is being reported by its ICT vendors.

We noted that two agencies developed procedures to support their ICT asset management processes after we started our review.

Why this is important

It is important to document procedures associated with the whole ICT asset lifecycle, including planning, acquiring, maintaining and disposing of assets.

Gaps in documented procedures can result in an inconsistent understanding of agency processes to manage ICT assets and inaccuracies in the ICT asset register. This increases the risk of potential billing errors, active devices falling out of warranty, loss or theft of hardware and threats to the security of agency data.

Inadequate review of ICT vendor activities may result in contractual arrangements and expectations for managing ICT assets not being fully met and potential overcharging of services.

5.1.2 Inconsistent management of ICT assets

Recommendation

We recommended that agencies establish central asset registers to manage their ICT assets. Access should be restricted to those responsible for maintaining these registers.

We also recommended that agencies consider implementing automated notifications to all stakeholders when staff movements occur. This includes notifying the ICT team so that ICT asset registers can be kept up to date. We recommended that two agencies review their current notification process.

We also recommended that, where possible, access to make changes to the ICT asset register should be limited and should be periodically reviewed for appropriateness. The ICT team's monitoring processes should be formally documented.

Finding

We reviewed agencies' operational processes to track and manage their ICT assets across business units. In most agency ICT teams, their ICT asset management practices were well understood. Despite this, we identified gaps in some agencies' ongoing management of ICT assets throughout their lifecycle:

- Five agencies rely on business units to inform their ICT team of any asset movement, but this is not consistently performed. One agency said that it did not have a process to consistently track the movement of end-user computers and their owners.
- In two agencies, ICT asset management is segregated and no centralised tool is used to provide an overview of all ICT assets. One agency told us that challenges with its existing tool meant that its various business units used separate processes to track the status of their ICT assets.
- In one agency, several manual processes exist to track and manage ICT asset inventory produced from several sources of information.

- In one agency, many business units have access to make changes to the ICT asset register. The ICT team monitors the changes made, but its monitoring processes are not documented. In addition, there is no periodic review of user accounts with access to the ICT asset register.
- One agency did not have a process to consistently track the movement of end-user computers and their associated owners.

Two agencies told us that they were planning to implement new systems to improve their ICT asset management processes.

Why this is important

Without the proactive notification of changes to the status of ICT assets and consistent management and oversight, there is an increased risk of errors and gaps occurring in agency asset inventory records.

Having a secure, single source of truth for ICT assets, documented in a central record, helps to make accurate and informed business decisions regarding agencies’ ICT environments.

Documenting ICT asset management processes helps to reduce the risk of knowledge loss when staff leave.

5.1.3 Gaps in documented ownership and classification of ICT assets

Recommendation

We recommended that agencies ensure that ICT information asset owners are formally assigned and documented in the agency ICT asset register.

We also recommended that ICT asset classifications be documented.

For most agencies, we recommended that they review their ICT asset registers and address the missing or inaccurate information we identified.

Finding

We asked agencies whether they had formally identified and documented information asset owners and classified their ICT assets as required by the SACSF.[4]

Most agencies understood the criticality of their ICT assets and had assigned information assets to business units and individuals. Despite this, we identified the following gaps:

[4] Policy Statement 2.1:
Information Asset Identification and Classification: Information assets are formally assigned an owner. Information assets are classified by the asset owner in alignment with the South Australian Information Classification System.

- Five agencies had not documented the classification of ICT assets in their ICT asset register. Three agencies had not documented individual asset owners.
- In one agency, there was no documented owner and classifications for end-user computers.

Our review of agency ICT asset registers identified the following missing or inaccurate information for end-user computers:

- Four agencies had not documented serial numbers and/or hardware configurations information.
- Two agencies had duplicate serial numbers recorded.
- Four agencies had not documented warranty or installation dates.
- Five agencies had assets with outdated warranties or retirement dates.

Why this is important

ICT assets may not have the appropriate protective requirements applied in line with the SACSF if they are not classified. ICT asset classification enables agencies to protect their information in a consistent, organised and appropriate way.

Not clearly documenting the ownership of ICT assets may lead to a lack of accountability for monitoring and responding promptly to security concerns, and for performing upgrades and other maintenance tasks.

Not being able to identify ICT assets owners can result in confusion and unsuccessful recovery of agency ICT assets. It could also result in unauthorised access to agency data if valid account credentials were obtained. It is important for asset owners to take responsibility for the strategic planning of their ICT assets to ensure they are meeting business needs.

Having an up-to-date ICT asset register helps to provide an accurate overview of an agency's ICT environments.

5.1.4 Lack of periodic review and monitoring of ICT assets

Recommendation

We recommended that agencies periodically review the ICT assets connected to their networks and update their ICT asset registers accordingly. This process can be supported by the asset discovery tools that agencies have implemented.

End-user computer last location and individual user logins (or custodians) should be obtained where possible to inform periodic reviews and any outcomes should be followed up.

Review requirements should be formally documented in agency ICT asset management policies and procedures. This includes clarifying the roles and responsibilities for discovering and following up unknown or suspicious devices.

Finding

We asked agencies if they perform periodic reviews of the ICT assets operating on their networks.

Some agencies had discovery tools to help track ICT asset movements. Despite this, we identified the following gaps:

- One agency periodically reviewed its server environment but did not review its end-user computers and network devices.
- Two agencies had not reviewed the active server and network devices running on their networks. They advised us that ad hoc reviews of ICT assets are performed, but the outcomes are not documented.
- In one agency, network discovery is not regularly performed to identify any unknown ICT assets connected to the network and ensure that all devices in use are captured in its ICT asset register.
- One agency did not perform periodic reviews of end-user computers operating on its network and had no follow-up processes. It advised us that staff movements make it difficult to track and manage end-user computers. This agency has the technical capabilities to track business unit assignment and individual users. We also noted that its process to perform and outcomes from its periodic reviews of server and network devices were not formally documented.

  This agency has tools available to help identify potentially suspicious activities on its network. However, responsibilities for discovering and following up any unknown ICT assets were not clear.

Why this is important

Periodically reviewing ICT assets helps to ensure that only approved assets are connected to agency networks and reduces the risk of agencies being charged for ICT assets that are not in use.

Unauthorised assets on the network can increase security risks to agency IT environments. Clear responsibilities for the discovery and follow up of unknown ICT assets helps to reduce this risk.

5.1.5 Gaps in ICT asset sanitisation and disposal

Recommendation

We recommended that agencies ensure that their ICT assets have been appropriately sanitised on decommissioning.

We also recommended that agencies ensure their sanitisation and disposal processes are documented. This includes documenting the roles and responsibilities of their ICT vendors and the assurance the agency obtains that its ICT assets have been securely sanitised and disposed of.

Finding

We asked agencies about their processes to sanitise and dispose of their ICT assets when they are no longer required.

While most agencies were able to demonstrate that they had adequate processes for sanitising and disposing of their ICT assets, we identified the following gaps:

- In one agency, ICT vendors are responsible for the secure sanitisation or disposal of the agency’s ICT assets. The agency was not fully aware of the vendors’ sanitisation processes.

  The agency did not receive formal confirmation of the sanitisation of end-user devices. Although the agency advised us that it received sanitisation certificates for server and network devices, we were unable to obtain evidence to confirm this.
- In another agency, ICT vendors are also responsible for sanitising and disposing of the agency’s ICT assets. Sanitisation certificates for end-user computers are not obtained and reports on end-user computers received for decommissioning produced by the vendor do not confirm sanitisation. The agency does not perform any ongoing assurance checks to confirm that appropriate sanitisation is occurring.

  The agency receives reports from a separate ICT vendor for server and network device hard drives received for destruction, but these reports do not confirm destruction. While the agency has documented its decommissioning procedures at a high level for server and network devices, it did not include the ICT vendor’s responsibilities or the agency’s assurance activities.
- One agency did not obtain evidence from its ICT vendor to confirm that its ICT assets had been securely sanitised and destroyed.

Why this is important

There is a risk that decommissioned ICT assets that contain agency sensitive information are not securely sanitised and destroyed. This risk is increased if the asset is purchased by a third party rather than being destroyed.

Appendix – Glossary of abbreviations and terms

Term	Description
ICT	Information and communications technology
IT	Information technology
SACSF	South Australian Cyber Security Framework. A risk-based framework developed by the Department of the Premier and Cabinet. It aims to help agencies preserve the confidentiality, integrity and availability of their information by applying appropriate cyber security management processes. It is a mandatory framework for SA Government agencies
Sanitisation	Sanitising an ICT asset before decommissioning is the process of securely removing all sensitive or confidential data from it to prevent unauthorised access or data breaches. It ensures no residual data remains on the asset after it is taken out of service