Audit Office
of South Australia

Auditor-General's Report 3 of 2026

Review of legacy ICT systems

Government of South Australia

[P.P.4ZP

Auditor-General's Report 3 of 2026

Review of legacy ICT systems

Tabled in the House of Assembly and ordered to be published, 16 June 2026

First Session, Fifty-Sixth Parliament

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

2026

The Audit Office of South Australia 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.

Audit Office
of South Australia

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Audit Office of South Australia
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157

Government of South Australia
Audit Office of South Australia

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

15 June 2026

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 3 of 2026 *Review of legacy ICT systems*

Under the *Public Finance and Audit Act 1987,* I present this report to each of you. It reviews the extent of legacy ICT systems operating across SA Government agencies and the risks they create for service delivery, security, performance and long-term sustainability.

Acknowledgements

The review team for this report was Andrew Corrigan, Tyson Hancock, Abhinav Tomar and Adrian Chong.

We appreciate the cooperation and assistance given by staff of the SA Government agencies involved in our review.

Yours sincerely

Andrew Blaskett
Auditor-General

Contents

Government of South Australia

Audit Office of South Australia

Audit snapshot

Review of legacy ICT systems

What we reviewed and why

We reviewed the extent of legacy ICT systems operating across SA Government agencies and the risks they create for service delivery, security, performance and long-term sustainability. Legacy systems remain in use when ageing, complex or tightly integrated technology is too costly, risky or difficult to replace.

In 2025, we surveyed 18 agencies to gather high-level information about legacy systems in their ICT environments. We then selected 10 agencies to review how they are managing the operational, security and governance risks of legacy applications, operating systems, hardware devices, database management systems and virtualisation platforms.

This review builds on our earlier work over the past decade, and reflects the continuing significance of legacy ICT systems as a whole-of-government issue. It also considers whether agencies are identifying, documenting and reporting legacy system risks to governance committees so they can be prioritised for treatment, upgrade or replacement.

What we concluded

Legacy ICT systems remain common across agencies and continue to present significant operational and security challenges. In many cases, these systems remain in use because agencies do not have sufficient funding, resourcing or replacement pathways to modernise them.

We found weaknesses in how some agencies manage legacy system risks, including incomplete asset inventories, limited formal risk assessments, gaps in risk register documents and inconsistent reporting to governance bodies. These gaps reduce visibility of risks and can delay action to remediate or replace systems.

We concluded that agencies need to adopt a more structured, risk-based approach to managing legacy ICT systems. This includes completing modernisation projects, maintaining better visibility of legacy assets, documenting risks and treatments more clearly, and ensuring governance committees receive regular updates on progress and residual risk.

Key facts

Of the ICT systems we assessed in 2025, these qualified as legacy systems:

195 applications	168 databases	766 operating systems	121 virtualisation platforms	5,736 ICT hardware devices/applications
(24% of 812)	(16% of 1,026)	(24% of 3,181)	(31% of 392)	(49% of 11,602)

1 Executive summary

1.1 Legacy system risks to agencies

A legacy information communication technology (ICT) system is a system that is still used by SA Government agencies, but it is outdated or no longer aligned with current business needs or modern technology standards.[1] These systems can pose significant operational and service delivery risks to the SA Government. Agencies tend to keep legacy ICT systems in operation when ageing, complex or tightly integrated technology becomes too expensive, risky or difficult to replace or upgrade.

Legacy systems can be costly to maintain, difficult to integrate and heavily reliant on limited specialist skills. This can result in increased system outages, slow responses to policy and legislative changes and a reduced ability to deliver digital services to businesses and the public. Over time, agencies can become locked into inflexible processes that limit the ability to implement innovative system changes and increase the total cost of owning the system.

Legacy systems create significant cyber security, privacy and compliance risks. They often lack modern security controls, current vendor support and alignment with current security frameworks and privacy obligations. This increases the risk of cyber incidents, data breaches and service disruptions, particularly as threat actors target public sector systems that hold sensitive personal and operational data.

Reliance on ageing technology also creates strategic and workforce risks. It can limit data sharing, analytics and evidence-based decision-making across the SA Government, which slows public sector reform and digital transformation. It can also make it harder to attract and retain staff with the skills to support outdated technologies, increasing the reliance on contractors to maintain these systems and raising knowledge and succession risks.

1.2 Our review of legacy ICT systems

Over the last 10 years, we reviewed and reported on the extent of legacy ICT systems operating across the SA Government and their risks, replacement programs and mitigation controls. In 2016 we reported on our review of key information security management components, including the use of legacy servers by 10 SA Government agencies.[2] In 2019 we reported on our high-level review of the extent and impact of legacy ICT systems used by 18 major SA Government agencies.[3]

In early 2025, we surveyed 18 major SA Government agencies to gather high-level information about the extent of legacy systems operating in their ICT environments. We then selected 10 agencies to review how they are managing the impacts and risks of using legacy ICT systems, and how these risks are reported through governance arrangements to ensure that they are appropriately managed. This report summarises the results of this review.

---

1 See section 5.3 for more information about what a legacy system is.

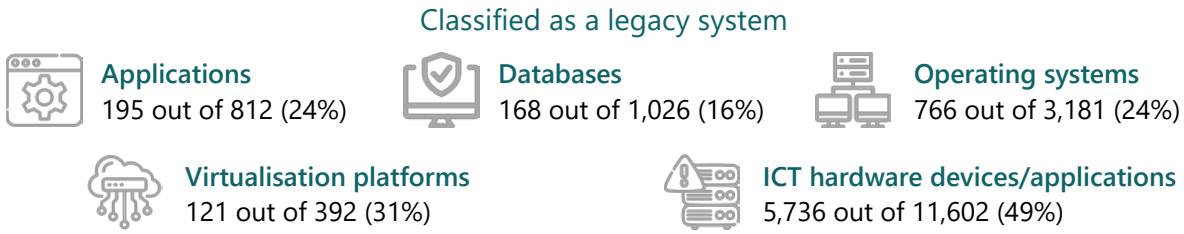
2 Auditor-General's Supplementary Report for the year ended 30 June 2016 *Security management of information systems: November 2016.*

3 Auditor-General's Report 12 of 2020 *Information and communications technology reviews*.

1.3 What we found

We found that legacy ICT systems are common across SA Government agencies. The extent of legacy systems in operation across the 10 agencies we reviewed is shown below.[4]

Figure 1: Extent of legacy systems



We found that legacy ICT systems present operational challenges for agencies. In general, agencies told us that legacy systems remain in use largely because their allocated budgets to upgrade or replace these systems were insufficient and limited agency resourcing has slowed progress on plans to upgrade or replace them.

We found that legacy systems affect agencies in different ways, including:

- limiting operational capability
- reducing the ability to innovate and adapt to change
- reducing operational performance
- increasing security risks.

We noted that the risks and costs related to addressing each legacy system type will vary. We did not raise any key concerns over backup and recovery solutions across the agencies we tested.

Given the above, the SA Government should consider options to strengthen how it collects information and oversees and monitors legacy ICT systems and digital governance across government.

1.4 Conclusion

Agencies need to strengthen their risk management and governance oversight to ensure legacy ICT risks are identified, actively managed and appropriately prioritised for remediation or replacement.

We recommended that agencies adopt a structured, risk-based approach to managing legacy ICT systems, focusing on completing modernisation projects, maintaining visibility of legacy assets and strengthening governance oversight, as shown in figure 2.

[4] Based on information provided by agencies at the time of our review. For SA Health we have not reported on its legacy applications given the high volume of applications across SA Health and the hybrid management and ownership arrangements of applications within the agency.

Figure 2: Recommendation to address legacy risks

See section 4 for more detailed findings and recommendations.

1.5 Response to our recommendations

The agencies we reviewed responded positively to our findings and recommendations and provided details about the actions they would take to address their legacy systems.

At the time of writing this report, one agency was still formulating its responses to our recommendations.

2 Digital Investment Fund

The existence of legacy ICT systems is a well-known issue across the SA Government and presents ongoing challenges for agencies. The SA Government has allocated source funding for agencies to help them replace or upgrade outdated technology and reduce associated risks. It established the Digital Investment Fund (DIF) in the 2023-24 State Budget. It initially allocated $200 million over five years for the purpose of driving strategic investment in cyber security and digital initiatives across the public sector.

The DIF aims to deliver:

- a strategic approach to prioritising digital investment and managing value
- better outcomes for the SA Government through investment in initiatives aligned with whole-of-government digital strategies and technologies
- improved opportunities for the digital sector through a published pipeline of funded digital and artificial intelligence projects
- better value for money outcomes for these digital initiatives.

For an agency's ICT upgrade or replacement project to be considered for funding under the DIF, it must submit a business case outlining that the project relates to a public authority and meets the Fund's investment principles.

The DIF was increased by $126.5 million to $326.5 million across the 2024-25 and 2025-26 State Budgets. The additional funding includes establishing a dedicated artificial intelligence (AI) program to support ongoing future capacity for digital investment initiatives across the SA Government and the development of multiple use cases on trusted foundational technologies.

From January 2026, DIF funding applications will be assessed twice yearly in April and September, in line with the State Budget cycle. The DIF had received 55 applications by the end of April 2026. Of these, 22 applications were approved, with total committed expenditure of $225 million. $113 million of this was spent by the end of April 2026.

The Department of Treasury and Finance advised us that it is taking a more strategic approach to working with agencies to prioritise projects funded by the DIF, focusing on projects for significant agency systems aligned with the SA Government's strategic direction.

3 Agency survey

There are about 170 SA Government entities. In April 2025, we surveyed 18 major SA Government agencies to gather high-level information about the extent of legacy systems operating in their ICT environments. The key responses are summarised below.

- All agencies have legacy systems, most of which support key business applications.
- Agencies identified risks including security vulnerabilities and limited vendor, third-party and internal staff support.
- The current challenges in upgrading or replacing these systems include resource shortages, budget constraints, system complexity and competing agency priorities.
- The total cost of upgrading or replacing legacy systems for 10 of the 18 responding agencies is estimated to be $435 million.[5] 14 agencies indicated that only partial or no funding was secured to replace systems.

While we sought clarification for some agency responses, we did not seek supporting evidence to validate these responses. We relied on the completeness and accuracy of the information the agencies provided.

See section 5.4 for the list of agencies we surveyed and reviewed.

[5] At the time of our review, not all agencies were able to easily quantify upgrade or replacement costs without extensive work.

4 Detailed agency testing findings

4.1 Gaps in managing risks for legacy applications

Recommendation

We recommended that agencies complete their current projects to upgrade or replace their legacy applications.

For legacy applications where no plans are in place, agencies should formally assess and document the risks of their continued operation. This should form the basis for prioritising future upgrade or replacement plans. Agencies should document the outcomes of these assessments in their ICT risk register.

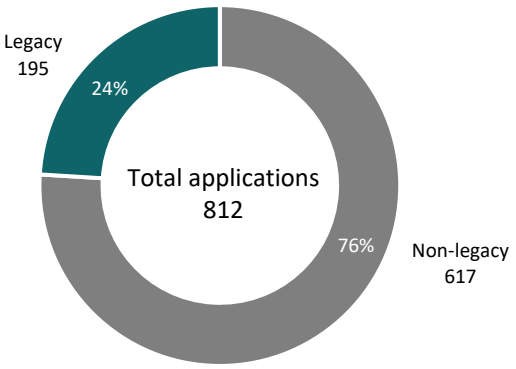
Agencies should regularly assess all their applications against the South Australian Cyber Security Framework (SACSF) legacy criteria.[6] Risk assessments should be performed for those that qualify as legacy.

Agencies should also provide the governance committees with regular updates on actions to address strategic legacy system risks, including updates on ongoing operational treatments and monitoring activities.

Finding

We requested that agencies provide us a list of all applications currently operating in their ICT environments. Across the nine agencies we reviewed,[7] 195 out of 812 applications (24%) qualified as legacy based on the SACSF criteria. Of greater concern is that many of these systems are key business applications that may directly affect service delivery and operational resilience.

Figure 3: Total applications in use across SA Government agencies we reviewed



[6] Government of South Australia 2025, *South Australian Cyber Security Framework (Appendix D)*, version 2, Government of South Australia, Adelaide.

[7] For SA Health we have not reported on their legacy applications given the high volume of applications across SA Health and the hybrid management and ownership arrangements of applications within the agency.

148 out of 195 legacy applications (76%) were identified as key business applications. Three of the nine agencies we reviewed reported that all their key business applications are legacy.

Across the agencies, we found weaknesses in the governance and risk management of legacy applications. For some agencies, these included:

- incomplete or outdated risk registers, with some legacy applications not recorded
- a lack of formal, detailed risk assessments for individual legacy applications and their treatment actions
- high-level risk register entries with a lack of supporting documents
- limited governance oversight, with legacy risks not consistently reported to relevant committees
- incomplete or inaccurate inventories of legacy applications, limiting effective risk management.

Most agencies are planning to upgrade or replace their legacy applications, although progress and certainty vary. Key points include:

- some legacy systems pose service delivery risks if they fail, prompting major replacement programs, some of which are already being implemented
- one agency was transitioning its applications by changing ownership or reassessing them
- several agencies are pursuing modernisation strategies such as retiring legacy systems, adopting software as a service, or consolidating platforms
- in many cases, upgrade or replacement projects are either under way or in planning, with some agencies developing supporting business cases
- agencies are generally taking a mixed approach, with some applications marked for replacement, others under review, and some with no current retirement plans.

A small number of applications were decommissioned during our review, after our initial information requests.

Why this is important

Legacy systems may limit operational capability, reduce an agency's ability to innovate and adapt to change, impair performance and increase security risks. It is therefore important to regularly assess legacy system risks and, where needed, plan to fully replace systems, modernise components or apply additional mitigating controls.

If governance bodies are not aware of legacy system risks and mitigation plans, agencies may not prioritise or allocate the funding and resources needed to address the risks.

The following case study shows how and why the Department for Child Protection started a project to replace its case management system.

Application case study – Department for Child Protection (C3MS)

The Department for Child Protection (DCP) implemented the Connected Client and Case Management System (C3MS) in 2009 to record, manage and share information about vulnerable children and families. At the time, C3MS provided a centralised platform intended to improve consistency in case management and strengthen coordination across the agency.

C3MS is now over 15 years old and lacks the flexibility needed to support modern workflows and integration. DCP advised us that it no longer meets the evolving needs of contemporary child protection service delivery.

C3MS receives limited vendor support as it is beyond its end-of-life support period. While DCP retains internal capability to manage the system, sustaining the required specialist skills remains difficult, particularly during periods of high demand or staff leave. This creates capacity pressures and ongoing operational strain in maintaining system continuity.

DCP advised us that its staff rely on manual workarounds, duplicate data entry and supplementary systems to perform core functions. Frontline workers spend significant time managing system limitations and maintaining records, reducing the time available to support vulnerable children and families. Access to timely, complete and reliable information has become more difficult, affecting the quality and speed of decision-making in high-risk situations.

As a legacy platform, C3MS also presents a range of operational and sustainability challenges, including:

- difficulty aligning with current technology standards and practices
- difficulty keeping pace with evolving organisational and regulatory requirements
- increased risk of poor performance, slower issue resolution and difficulty applying updates or enhancements
- limited flexibility to deliver improvements or respond to incidents, with reliance on a small number of staff with specialised legacy knowledge.

Given these known challenges, DCP started the KidSafe Connect Program to replace C3MS. The new system is expected to provide a modern, fit-for-purpose case management platform that improves the quality, accessibility and timeliness of data needed by staff. It is also expected to be more secure, stable and resilient, while supporting better information sharing and coordination with partner agencies. A core benefit will be reducing the administrative burden created by the current legacy system, allowing staff to focus more on supporting children and families.

4.2 Weaknesses in managing legacy operating systems

Recommendation

Agencies should complete their current plans to upgrade or replace their legacy operating systems.

Agencies should assess and document the risks of upgrading or retaining each legacy operating system to minimise adverse impacts on key system environments. These assessments should inform upgrade priorities.

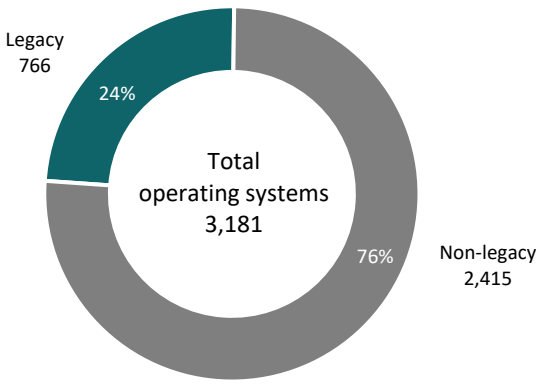
Relevant agency ICT governance committees should receive regular updates on any developments, including ongoing treatments and monitoring activities.

Finding

We requested agencies provide a list of operating systems currently used in their ICT environments. Our review found that agencies continue to use some legacy operating systems. Based on the data provided by agencies, 766 out of 3,181 operating system instances (24%)[8] qualified as legacy, using vendor information to determine the end of life and support status.

One agency reported to us that it had no legacy operating systems as it had recently upgraded all operating systems to supported versions.

Figure 4: Legacy operating systems



Agencies are actively managing legacy operating system risks through remediation, containment and transitional strategies. Several agencies have already decommissioned or upgraded legacy systems, or are planning to remove them, while others are progressing targeted projects to enable replacement or reduce dependencies.

[8] This figure may be higher, as one agency did not provide a complete list of operating systems for our assessment.

Where immediate remediation is constrained, often due to application dependencies, agencies are implementing compensating controls such as network segregation and enhanced security measures. In the interim, half of the agencies we reviewed relied on extended vendor support for critical patching, incurring extra costs alongside regular monitoring, disaster recovery and backup capabilities to mitigate operational risk.

While extended support reduces the risk by providing limited critical patches, it does not address all security issues. Many vulnerabilities remain unpatched, application-level and third-party software may still be unsupported and no new security features are introduced.

Most agencies had recorded legacy operating system risks in their risk registers or strategic plans and provided governance committees with high-level updates on issues. However, several agencies had gaps in this process, including incomplete records of identified legacy operation systems, limited detailed risk assessments and insufficient documentation of remediation actions and treatment plans. In some cases, risks were missing from risk registers or only recorded at a high level without supporting detail. Some agencies relied on project-level tracking or informal processes without formally recording, monitoring or reporting these risks to governance bodies. These gaps reduce visibility, accountability and effective oversight of legacy system risks.

Why this is important

Legacy operating systems expose agencies to significant security vulnerabilities, including unpatched exploits that make them more vulnerable to cyberattacks. Limited vendor support and available internal expertise can increase operational instability and the risk of system failures.

Legacy systems can also cause integration issues with newer software and hardware, often leading to time-consuming workarounds and poorer performance. Modernising legacy operating systems improves security, efficiency and scalability, while reducing support costs and enabling innovation.

Agencies should therefore regularly assess the risks of legacy operating systems still in production and keep governance bodies aware of those risks and the plans in place to manage them.

4.3 Weaknesses in managing legacy hardware devices

Recommendation

We recommend that agencies should finalise business cases and complete projects to upgrade or replace their legacy ICT hardware devices and appliances.

One agency should consider plans for its remaining legacy ICT hardware devices and appliances. Another agency should complete its audit and assessment of its infrastructure assets.

Some agencies should develop a detailed inventory of legacy ICT hardware devices and appliances and assess the risks of each item. This should guide prioritisation of replacement activities. For one agency, we recommended it use a structured, risk-based assessment by type or manufacturer to help prioritise high-risk categories for upgrade.

Relevant agency ICT governance committees should receive regular updates on the progress of developments.

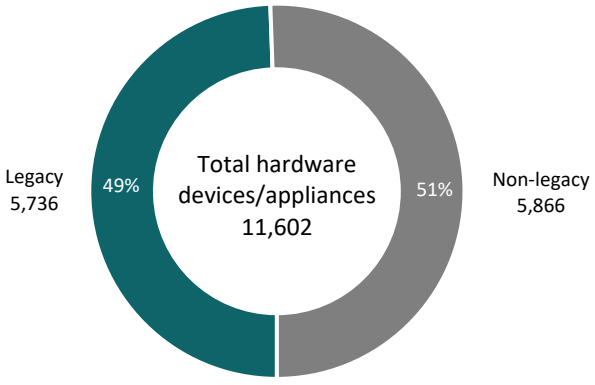
Finding

We requested that agencies provide a list of all ICT hardware devices and appliances in operation. ICT hardware devices and appliances are the physical infrastructure that supports agency business processes. This includes running applications, managing data and enabling communication and connectivity within the agency and with external parties.

We found that 5,736 out of 11,602 ICT hardware devices and appliances (49%) qualified as legacy. Vendor information was used to determine the end of life and extended support status.

One agency reported to us that it did not have any legacy ICT hardware devices and appliances, while two agencies reported only a small number.

Figure 5: Legacy ICT hardware devices/appliances



Most agencies have started initiatives to address legacy hardware and infrastructure, although limited vendor support and budget constraints remain common challenges. Actions under way included:

- upgrades, migrations and capital projects to reduce the legacy footprint
- assessments and business cases to support future upgrades
- use of an updated hardware-as-a-service model to support ongoing refresh cycles.

Agencies advised us of the following activities to reduce the risk of legacy ICT hardware devices and appliances:

- using vendor maintenance and support arrangements to manage legacy hardware risks
- regular patching, monitoring, and reporting practices are in place in some agencies
- maintenance contracts and vendor support to replace faulty devices
- implementing redundancy for critical systems to maintain resilience
- external service providers supporting some legacy infrastructure
- incident response plans and hardware support arrangements to mitigate operational risk.

Most agencies had recorded legacy hardware risks and reported them to governance committees. However, supporting documentation was often incomplete or lacked detail. Common gaps included missing information on support arrangements, upgrade plans and treatment activities. Some agencies did not have detailed inventories of legacy ICT hardware devices and appliances to support reported risks, and had not completed sufficient risk assessments or documented remediation status.

Why this is important

Without reliable ICT hardware, key agency functions such as transaction processing, data storage and communication, may be disrupted, affecting overall operational efficiency. Legacy ICT hardware devices and appliances can increase security vulnerability risks, reduce performance and create operational inefficiencies.

As vendors withdraw support, these devices become harder to maintain and less compatible with modern systems, increasing the risk of failure. Continued reliance on outdated hardware can lead to unplanned downtime, higher operating costs and reduced ability to meet agency ICT strategic goals.

Agencies should therefore regularly assess the risks of legacy hardware devices and, where needed, plan to fully replace systems, modernise components or apply additional mitigating controls.

If governance bodies are not fully informed of legacy hardware risks and mitigation plans, funding and resources may not be prioritised and applied to address them.

4.4 Weaknesses in managing database management systems

Recommendation

We recommend that agencies should complete planned projects to upgrade, migrate or decommission their legacy database management system environments, including working with vendors to complete this process, and considering options to upgrade or replace these systems, where possible.

For one agency, legacy database management systems should remain in scope for removal as part of its upcoming major business transformation project.

Agencies should continue to monitor and assess legacy database management systems for available patches and regularly assess the risks of their continued operation.

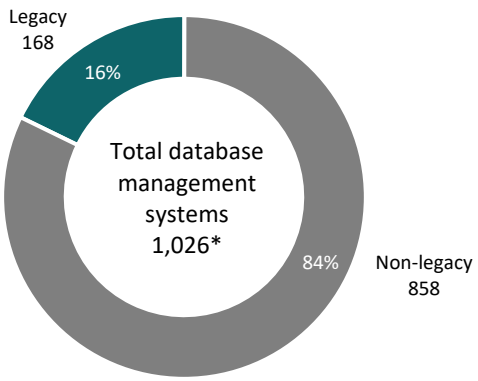
Two agencies should develop a detailed inventory of legacy database management systems and complete formal risk assessments with associated treatments. Strategic plans, mitigating controls and ongoing treatment, and monitoring activities should be documented in agency risk registers. One agency also needs to develop a more detailed ICT risk register to record this information.

ICT governance committees should be kept informed of any changes and receive regular updates.

Finding

We requested agencies provide a list of all current database management systems. We found that 168 out of 1,026 database management systems (16%) qualified as legacy. Vendor information was used to determine the end of life and extended support status. Two agencies reported no legacy database management systems.

Figure 6: Legacy database management systems



* One agency did not provide data on its total database management systems.

Some agencies advised us that these database management systems support key business application and could affect service availability if issues occurred.

Agencies are managing legacy database management system risks, although maturity and timelines vary. Some systems remain constrained by application dependencies and are planned for replacement through broader projects, while others are in planning stages for decommissioning, upgrade or migration. Several agencies have decommissioned, disabled or migrated some legacy database management systems during our review, while others plan staged migrations over the coming years. Overall, these efforts reflect a transition approach that balances immediate risk management with longer-term modernisation.

Agencies are managing legacy database management system risks through operational controls, such as applying patches where possible and maintaining regular monitoring, tracking and reporting processes. One agency was also strengthening resilience through consistent backups, recovery testing and business continuity planning. In addition, agencies are reducing known vulnerabilities, implementing access controls and monitoring audit logs to detect and respond to issues.

Most agencies had recorded legacy database risks at a high level and reported them to governance committees, but supporting documents were often incomplete. Gaps included missing details on maintenance, patching, risks and treatment activities as well as limited inventories of identified legacy database management systems, including end of life and support status. Some agencies had limited or no risk assessments and remediation tracking. In some cases, risks were not formally recorded in active risk registers or supported by adequate evidence, reducing transparency and effective oversight.

Why this is important

Legacy databases increase the risk of cyber threats, compliance failures, operational inefficiencies and reduced ability to innovate. Modernising database platforms improves security, scalability and long-term sustainability while reducing maintenance costs.

Agencies should therefore regularly assess legacy database management system risks and, where needed, plan to fully replace systems, modernise components or apply additional mitigating controls.

If governance bodies are not aware of the risks and mitigation plans, funding and resources may not be prioritised appropriately to address them.

4.5 Weaknesses in managing virtualisation platforms

Recommendation

Affected agencies should complete their planned actions to assess and reduce their current reliance on legacy virtualisation platforms. This includes developing detailed inventory of their environments.

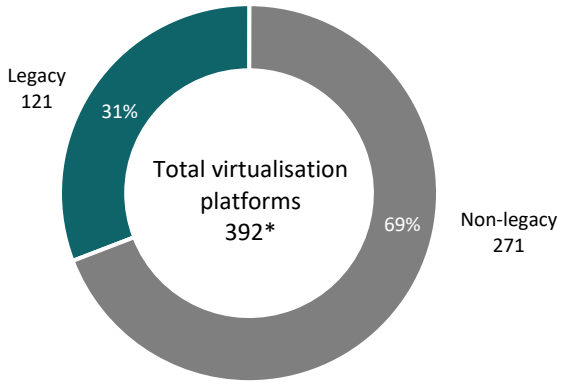
These agencies should also complete formal risk assessments with associated treatments, and keep ICT governance committees informed of progress.

Finding

We requested that agencies provide a list of all current virtualisation platforms. We found that three agencies had legacy virtualisation platforms still in production. The other seven agencies reported no virtualisation platforms that qualified as legacy.

We found that 121 out of 392 virtualisation platforms (31%) qualified as legacy. Vendor information was used to determine the end of life and extended support status.

Figure 7: Legacy virtualisation platforms



* One agency did not provide data on its total virtualisation platforms.

The three affected agencies outlined plans to address these legacy systems, including scheduled upgrades, phased migration as funding allows and broader security strategies. Reported mitigation controls included redundancy, incident management, maintenance contracts and enhanced security controls such as network segmentation.

We found that high-level legacy risks were generally recorded in agency risk registers or strategic plans and reported to relevant governance committees. However, there were gaps in their risk assessments that limit their ability to prioritise upgrades or other mitigation activities effectively.

Why this is important

Unsupported legacy virtualisation platforms expose agencies to unpatched security vulnerabilities. They can also limit scalability, increase operational costs and reduce access to capabilities such as automation, cloud integration and modern disaster recovery. Limited vendor support makes troubleshooting more difficult and reduces compatibility with modern systems.

Agencies should therefore regularly assess the risks of legacy virtualisation platforms and, where needed, plan to fully replace systems, modernise key components or apply additional mitigating controls.

If governance bodies are not aware of legacy virtualisation risks and mitigation plans, funding and resources may not be prioritised appropriately to address them.

5 Review mandate, objective and scope

5.1 Our mandate

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

5.2 Our objective and testing scope

The purpose of our high-level review was to determine the extent and impact of legacy ICT systems within the SA Government and how it is managing these impacts.

For the SA Government agencies reviewed, we assessed:

- the extent of legacy ICT systems[9] operating in the production environment
- strategic, financial, security, operational and functionality impacts and whether mitigation plans have been adopted
- whether plans exist to upgrade or replace these systems, with the estimated costs
- how the associated risks are documented and reported to their applicable governance committees to ensure appropriate attention and oversight.

5.3 Defining a legacy ICT system

The *South Australian Cyber Security Framework* defines that an information technology product (ie hardware, software, services, protocols and/or system)[10] is considered 'legacy' when it meets one or more of the criteria in both Category A and Category B below:

Category A

Considered an end-of-life product, or

Out of support, and extended support from the manufacturer, vendor or developer.

Category B

Impractical to update or support within the entity, or

No longer cost-effective, or

Considered to be above the current acceptable risk threshold, or

Offers diminishing business utility, or

Prevents or obstructs fulfilment of the entity's IT strategies.

[9] Including applications, operating systems, databases, backup recovery solutions, ICT hardware devices and appliances and virtualised platforms.

[10] Government of South Australia 2025, *South Australian Cyber Security Framework (Appendix D)*, version 2, Government of South Australia, Adelaide.

5.4 Agencies we reviewed

To conduct our testing, we surveyed 18 agencies to request high-level information about the extent of legacy systems operating in their ICT environments. The agencies we surveyed were:

- Attorney General's Department
- Courts Administration Authority
- Department for Child Protection
- Department for Correctional Services
- Department for Education
- Department for Environment and Water
- Department for Health and Wellbeing
- Department for Infrastructure and Transport
- Department of Human Services
- Department of Primary Industries and Regions
- Department of State Development
- Department of Treasury and Finance (Corporate and Shared Services SA)
- Legal Services Commission of South Australia
- Public Trustee
- South Australian Water Corporation
- SACE Board
- South Australia Police
- TAFE SA.

We then selected 10 of these agencies to review how they are managing the impacts and risks of using legacy ICT systems. The agencies we reviewed were:

- Department for Child Protection
- Department for Environment and Water
- Department for Health and Wellbeing
- Department for Infrastructure and Transport
- Department of Human Services
- Department of Treasury and Finance (Corporate and Shared Services SA)
- Public Trustee
- South Australia Police
- South Australian Water Corporation
- TAFE SA.

We provided these agencies with a further set of questions seeking information about their legacy applications, operating systems, database management systems, virtualisation platforms, backup and recovery solutions, hardware devices and appliances, and risk management approaches.

5.5 What we did not review

Our review focused on the extent of legacy systems that exist in SA Government agencies.

We did not verify agency survey responses or agency confirmations on the status of ICT assets, including resourcing, vendor support, cost-effectiveness or installation dates.

Where agencies provided us with inconsistent information about ICT assets, we sought clarification to present the most accurate view of their legacy environments.

Appendix 1 – Abbreviations and terms used in this report

Abbreviation/Term	Description
Application	Used to support an agency's operations by helping users perform specific tasks such as finance, human resources or customer management.
Operating system	The core software that manages a computer's hardware and provides services for applications and user interaction.
Database management system	Software that stores and manages data, allowing users and applications to easily access and update it.
Virtualisation platform	Software that allows a single server (or computer) to run multiple virtual machines, each acting like its own independent system.
Legacy system	A system that is still in use by South Australian government agencies but is outdated or no longer aligned with current business needs or modern technology standards.
Software as a service	A cloud-based model where software is delivered over the internet and accessed by a browser, rather than installed locally. The provider manages hosting, maintenance and updates, typically through a subscription-based model.
Hardware as a service	A cloud-like model where organisations lease physical ICT equipment (such as laptops, servers, or networking devices) through a subscription, rather than purchasing it outright. The provider manages the hardware life cycle, including maintenance, upgrades, and replacement, for a recurring fee.
SACSF	South Australian Cyber Security Framework. It is a Cabinet-approved, whole-of-government framework designed to help SA Government agencies safeguard digital assets, information, and ICT infrastructure against cyber threats while maintaining public trust and service reliability. It applies to all SA Government agencies.