

Report 12 of 2020

Information and communications
technology reviews



Report of the Auditor-General

Report 12 of 2020

Information and communications
technology reviews

Tabled in the House of Assembly and ordered to be published, 8 September 2020

Second Session, Fifty-Fourth Parliament

By authority: S. Smith, Government Printer, South Australia



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



7 September 2020

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

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 12 of 2020 *Information and communications technology reviews***

As required by the *Public Finance and Audit Act 1987*, I present to each of you Report 12 of 2020 *Information and communications technology reviews*.

Content of the Report

Each year we review SA Government agency security controls over IT systems and the status of selected IT projects.

This report communicates the results of the following key IT reviews we conducted in 2019-20:

- information technology general controls
- legacy system review.

Information technology general controls

Most of the control deficiencies identified in the 2019-20 information technology general controls reviews included in this report related to the management of user access, passwords and audit logging. It is disappointing that our reviews regularly highlight these types of control deficiencies. I would again encourage all agencies to be more diligent in addressing these control weaknesses as part of their routine security housekeeping.

Legacy system review

The SA Government has a challenge in managing the large number of legacy systems currently being used by various government agencies.

We acknowledge the difficulties agencies have when accurately assessing the costs and benefits associated with upgrading or replacing their legacy systems. In some cases, replacing them will require significant funding and resourcing.

Despite these costs, agencies must be proactive in managing legacy systems and manage the risks arising from them. They should prepare business cases to help evaluate the feasibility of replacing these systems against other agency priorities. We note that legacy systems are impacting current business operations and strategic objectives within agencies. They are also potentially increasing operational costs and exposing agencies to additional security risks.

Acknowledgements

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

We appreciate the cooperation and assistance given by staff of the agencies involved in these reviews.

Yours sincerely

A handwritten signature in black ink, appearing to read "Richardson", with a long horizontal flourish extending to the right.

Andrew Richardson
Auditor-General

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 2 | Information technology general controls | 1 |
| 2.1 | Executive summary | 1 |
| 2.1.1 | Introduction | 1 |
| 2.1.2 | Conclusion | 1 |
| 2.1.3 | What we found | 2 |
| 2.1.4 | What we recommended | 3 |
| 2.2 | Review objective, scope and approach | 3 |
| 2.2.1 | Audit mandate | 3 |
| 2.2.2 | Agencies tested | 4 |
| 2.2.3 | Summary of information technology general controls tested | 5 |
| 2.3 | Details of findings | 6 |
| 2.3.1 | User access management | 6 |
| 2.3.2 | Change management | 7 |
| 2.3.3 | Password management | 7 |
| 2.3.4 | Audit log management | 8 |
| 2.3.5 | Disaster recovery | 9 |
| 2.3.6 | Patch management | 10 |
| 2.3.7 | Other ICT related testing performed | 10 |
| 2.4 | What we recommended and agency responses | 11 |
| 3 | Legacy system review | 13 |
| 3.1 | Executive summary | 13 |
| 3.1.1 | Introduction | 13 |
| 3.1.2 | Conclusion | 13 |
| 3.1.3 | What we found | 14 |
| 3.2 | Review objective, scope and approach | 14 |
| 3.3 | Details of findings | 15 |
| 3.3.1 | Vendor costs for legacy system maintenance and support | 15 |
| 3.3.2 | Legacy applications | 16 |
| 3.3.3 | Legacy operating systems | 21 |
| 3.3.4 | Legacy databases | 22 |
| 3.3.5 | Legacy network devices | 23 |

1 Introduction

Each year we review SA Government agency security controls over IT systems and the status of selected IT projects.

This report communicates the results of the following key IT reviews we conducted in 2019-20:

- information technology general controls (ITGCs)
- legacy system review.

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

2 Information technology general controls

2.1 Executive summary

2.1.1 Introduction

ITGCs are policies, procedures and system settings that support the effective functioning of operating system, database and application controls. They help agencies maintain the confidentiality, integrity and availability of their data.

Each year we conduct selected ITGC testing over key agency financial systems. Our testing takes into consideration the SA Government's Cyber Security Management Framework and associated agency IT security guidelines.

This Report summarises the 2019-20 ITGC testing we conducted over 10 agencies and 13 key agency financial systems. Our testing also assessed the remediation of ITGC related issues we raised in prior years.

Although this summary does not include all agency ITGC testing that we conducted in 2019-20, it does provide an indication of the general themes where control weaknesses exist. It also provides agencies with information they can use to make informed decisions to improve the management of their overall control environments.

2.1.2 Conclusion

Most of the control deficiencies identified in the 2019-20 ITGC reviews included in this Report related to the management of user access, passwords and audit logging. These deficiencies accounted for 64% of the total findings.

While most findings were low¹ and medium² rated, two findings relating to segregation of

¹ Low rated is a minor control weakness with minimal but reportable impact on the ability to achieve process objectives.

² Medium rated is a control weakness that could have or is having a moderate adverse effect on the ability to achieve process objectives.

duties conflicts and insufficient access to application source code were rated as high.³

It is disappointing that our ITGC reviews regularly highlight these types of control deficiencies. I would again encourage all agencies to be more diligent in addressing these control weaknesses as part of their routine security housekeeping.

2.1.3 What we found

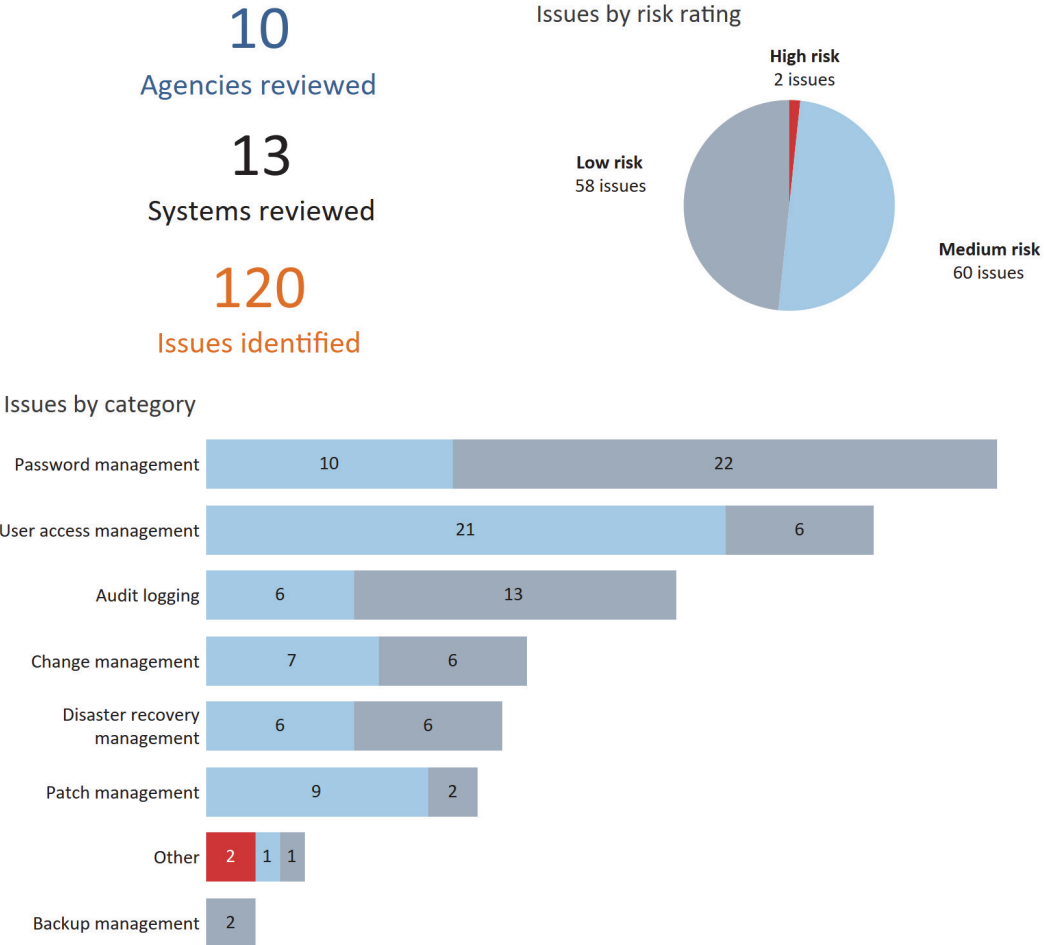
Based on our testing in 2019-20, figure 2.1 shows the key control areas that could be strengthened.

The rating we give the audit issues reflects our assessment of both the likelihood and consequence of each issue in terms of its impact on:

- the effectiveness and efficiency of operations, including probity and compliance with applicable laws
- the reliability, accuracy and timeliness of financial reporting.

The rating also helps agencies to prioritise any remedial action.

Figure 2.1: Summary of our findings



³ High rated is a control weakness that could have or is having a major adverse effect on the ability to achieve process objectives.

2.1.4 What we recommended

Our recommendations to agencies include strengthening the following controls:

- **user access management** – promptly removing inappropriate user access, performing regular user access reviews and maintaining evidence of user access changes
- **change management** – improving policies and procedures, maintaining documented evidence supporting change activities and post-implementation testing, and applying appropriate segregation of duties throughout the change management process
- **password management** – strengthening password configuration settings, improving policies and procedures, and conducting regular reviews of password setting policies
- **audit logging** – implementing and reviewing audit logging and improving policies and procedures
- **disaster recovery** – developing and regularly reviewing formal disaster recovery plans and associated procedures and conducting disaster recovery tests
- **patch management** – developing and improving policies and procedures to ensure patches are appropriately applied
- **other matters** – ensuring that application source code arrangements are regularly reviewed, updated and retained. Also ensuring that remediation of prior internal security and penetration testing reviews is timely, and suitable documentation of this is maintained.

2.2 Review objective, scope and approach

2.2.1 Audit mandate

The *Public Finance and Audit Act 1987* requires the Auditor-General to form an opinion on agency financial reports. In forming an opinion on whether a financial report is free from material misstatement, the auditor must consider the entity's internal control environment. Internal controls are systems, policies and procedures that help an agency reliably and cost effectively meet its objectives. For the agencies we audit, we consider ITGCs to varying degrees, depending on the nature of the agency's operations and the way it uses IT.

Auditing Standard ASA 315 *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment* advises that ITGCs commonly include controls over:

- data centre and network operations
- system software acquisition, change and maintenance
- program change
- access security
- application system acquisition, development and maintenance.

Therefore, we seek to understand how agencies respond to risks arising from their IT environments and assess any controls applied. Ultimately, this will inform my opinion as to whether the information in the financial report is free from material misstatement. This work

also has the significant benefit of informing how well agencies maintain the confidentiality, integrity and availability of data.

2.2.2 Agencies tested

In 2019-20 we tested ITGCs for a range of agencies and their IT systems.

Figure 2.2: Summary of agencies and systems tested








| Agency | System | Description |
|---|---|--|
| Attorney-General's Department | Births, Deaths and Marriages | Records the birth, death and marriage records for life events. |
| Department for Health and Wellbeing | Oracle Corporate System | Used for accounts payable, accounts receivable, general ledger and fixed assets. |
| Department of Human Services | Funding and Grants Management System | Used to track funding arrangements and the payment of grant funding to other entities. |
| Department of Planning, Transport and Infrastructure | TRUMPS | Used for collecting revenue, mainly related to driver's licences and motor registration. |
| Department of Treasury and Finance | Basware, Masterpiece, CommBiz and Chris21 | Shared Services SA uses several central systems to process transactions on behalf of agencies. These include: <ul style="list-style-type: none"> • Basware to process accounts payable transactions • Masterpiece for accounts payable, accounts receivable, general ledger and fixed assets • CommBiz banking for disbursing payroll and third-party payments • Chris21 for agency payroll processes. |
| Independent Gaming Corporation Limited | Scientific Games Video System | Used to monitor and manage existing gaming machine systems. |
| Local Government Finance Authority of South Australia | Quantum | Used for treasury management. |
| Public Trustee | HiPortfolio | Accounting and asset management software. |
| South Australian Government Financing Authority | Findur | Used for treasury management and accounting. |

| Agency | System | Description |
|------------------------------------|---------|--|
| South Australian Water Corporation | Ellipse | Expenditure payment system that includes the agency general ledger module. |

In testing these systems, we examined the ITGCs shown in figure 2.3 at the operating system, application and database level.

2.2.3 Summary of information technology general controls tested

Figure 2.3: Summary of ITGCs tested

| | | |
|---|-------------------------------|---|
|  | User access management | User access management relates to the process of managing access to applications and data, including how access is approved, revoked and periodically reviewed. This helps to ensure that access is aligned with staff roles and responsibilities and prevents unauthorised access to information systems. It includes appropriately restricting and monitoring privileged access permissions, which have a heightened level of access to alter user access profiles and make system changes. |
|  | Change management | Change management is a systematic and standardised approach to ensuring all changes to the IT environment are appropriate, authorised and preserve the integrity of the underlying programs and data. |
|  | Password management | Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorisation. |
|  | Audit log management | Audit logging and monitoring of the ICT environment involves the recording and analysing of system and user activities to detect and respond to unusual events within the IT system. |
|  | Disaster recovery | Disaster recovery is a documented process, or set of procedures, to assist in the recovery of an organisation's ICT infrastructure in the event of a disaster. |
|  | Patch management | Patch management is the process of updating (acquiring, testing and installing) a set of changes or upgrades to support software, application and technology enhancements and to fix defects and vulnerabilities to an information system. |
|  | Backup management | Backup management refers to the process of managing the copying of computer data to an archive file. This copy can then be used to restore the original data in the event of data corruption or data loss event. |

2.3 Details of findings

Our testing involved performing system walkthroughs with agency representatives and reviewing policies and procedures. The walkthrough helps us to get a better understanding of the agency’s IT environment and to evaluate the design of controls and whether they can be tested for effectiveness. For example, the control exists and evidence can be obtained to test its effectiveness.

2.3.1 User access management

Why we reviewed it

Weaknesses in user access management controls can result in inappropriate and unauthorised access to business systems. This can impact the completeness and accuracy of financial information through the destruction of data, improper changes to data or inaccurate recording of transactions.

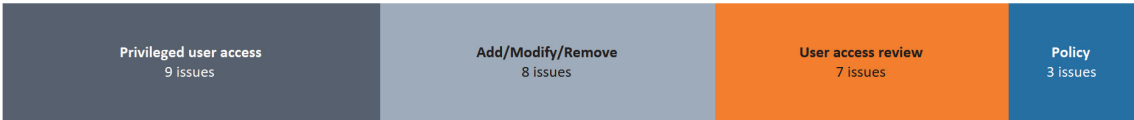
What we reviewed

We reviewed the user access management policies and procedures that apply to key financial systems. This includes assessing processes applied for user access changes, user roles and responsibilities and profile configurations. For example, assessing whether a new user requires a user access form to be completed and approved before the account is created.

Our testing involved selecting a sample of user accounts and obtaining evidence of the addition, modification and removal of these user accounts and profiles. We also confirmed the appropriateness of privileged user accounts⁴ and obtained evidence of recent internal user access reviews and their outcomes.

What we found

Figure 2.4: Summary of user access management findings



Most findings within these categories related to:

- inappropriate assignment of privileged user access
- internal user access reviews either not performed or not promptly actioned
- insufficient evidence of user access changes (add and modify) and failure to promptly remove user access.

⁴ A heightened level of access that provides the ability to manage user access profiles and make changes to critical files and functions at the application, database and operating system level.

2.3.2 Change management

Why we reviewed it

Weaknesses in change management controls can result in poorly tested, inappropriate or unauthorised changes to business systems. This can impact the completeness and accuracy of financial data and the correct functioning of the system.

What we reviewed

We reviewed the policies and procedures that apply to making system changes to the financial system environments. We did this to understand the process applied to making system changes, including where change requests originate from, oversight and approval mechanisms, whether changes can be made within the business or require the assistance of an external vendor, and the roles and responsibilities of each party in the process.

Our testing also involved selecting a sample of system changes and obtaining evidence to determine whether they were appropriately tested, approved and migrated into the production environment.

What we found

Figure 2.5: Summary of change management findings



Most findings within these categories related to:

- lack of segregation of duties throughout the change management process
- inadequate change management policy and/or procedure documents
- inadequate evidencing of documentation supporting change activities and post-implementation testing.

2.3.3 Password management

Why we reviewed it

Weaknesses in password configuration settings may make it easier for a user account to be maliciously compromised, allowing unauthorised access to business systems and data.

Examples of weak password configuration settings include:

- not forcing users to regularly change their password
- not forcing users to change their password to something not previously used

- minimum password length being too short
- not forcing users to add a number, letter or special character to their password
- not setting a limit on how many times a user can enter an incorrect account password before access is denied.

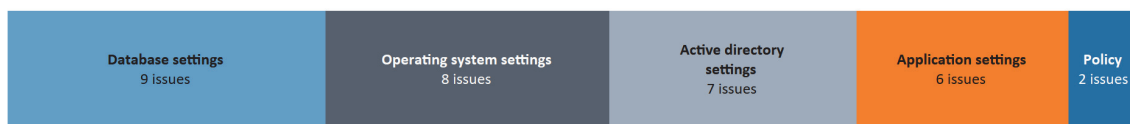
What we reviewed

Our testing involved reviewing the agency’s password management policies and procedures. We did this to determine whether agencies had specified minimum password standards that their system owners must apply when configuring the password settings for their IT systems.

We compared the password settings of each tested system applied at the application, operating system and database level for in-scope financial systems against the configuration settings suggested in the Australian Government Information Security Manual⁵ and the agency’s password standards (if specified).

What we found

Figure 2.6: Summary of password management findings



Most findings within these categories related to:

- weaknesses or inconsistencies in password configuration settings across various agency active directory networks, applications, databases and operating systems
- the absence of a general password policy or insufficient detail in the password policy
- inadequate regular review of the agency’s password policy.

2.3.4 Audit log management

Why we reviewed it

Weaknesses in system audit logging and monitoring increase the risk of inappropriate and unauthorised activities within the system going undetected. Not having an effective audit trail reduces the likelihood that inappropriate activity can be traced back to an individual.

What we reviewed

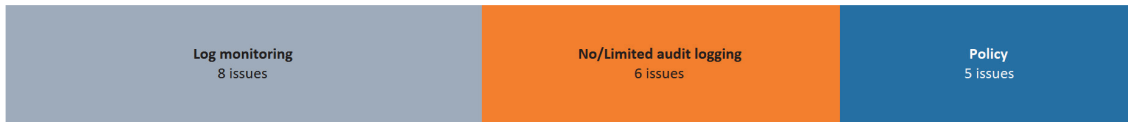
We reviewed the agency’s policies and procedures for audit logging to confirm the approach and extent of audit logging being performed.

⁵ Australian Government Information Security Manual. Refer to www.cyber.gov.au, viewed 24 August 2020. Although we acknowledge that agencies are not required to comply with this manual, we consider the settings recommended in it represent better practice.

Our testing then involved obtaining evidence that audit logs, primarily for privileged user account activities, are maintained, restricted and periodically reviewed.

What we found

Figure 2.7: Summary of audit logging findings



Most findings within these categories related to:

- no or limited audit logging conducted across the application, database, operating system and infrastructure
- no regular review of audit logs
- instances where no formal audit logging policy and procedures were maintained.

2.3.5 Disaster recovery

Why we reviewed it

IT disaster recovery weaknesses may result in agencies not being able to recover key business systems within maximum allowable outage times,⁶ in the event of a disaster or system failure. In addition, the completeness and accuracy of financial data is at risk when a financial system experiences an interruption.

What we reviewed

Our testing involved establishing whether a disaster recovery plan and associated recovery procedures were in place and adequately tested.

What we found

Figure 2.8: Summary of disaster recovery findings



Most findings within these categories related to:

- no formal disaster recovery plan or associated procedures being developed
- insufficient disaster recovery testing conducted across the application and database
- no regular review of the disaster recovery plan.

⁶ The maximum allowable outage time is the maximum time that an agency can tolerate the disruption of an important business function before there is a significant impact on its operations.

2.3.6 Patch management

Why we reviewed it

Not patching IT systems at the operating system, database and application level increases the opportunity for attackers to exploit known vulnerabilities. Patching is also used to provide system functionality updates and fix defects.

What we reviewed

We reviewed the policies and procedures for patch management. Where appropriate, we selected a sample of patches applied to the application, database and operating system. Our testing involved obtaining evidence of a recent patching assessment and reviewing whether patches were subject to a formal risk assessment before being implemented.

What we found

Figure 2.9: Summary of patch management findings



Most findings within these categories related to:

- inadequate patch management processes for specific application, database and operating systems
- instances where no formal patch management policy and procedures were developed.

2.3.7 Other ICT related testing performed

Why we reviewed it

We identified the following other matters at specific agencies that we considered were important to investigate during our ITGC testing:

- Agencies periodically perform security reviews across their key business systems. As part of that process, they may perform certain penetration testing.⁷ These types of tests are used to provide a level of assurance over the adequacy of security controls. This is to help minimise exposure to several threats experienced by the State each year. For example, an SA Government cyber intelligence report has noted a trend of increased cyber security activity since the introduction of mandatory cyber security reporting. In 2019 the number of reports submitted to the watch desk⁸ increased by more than 25% in comparison to 2018.

⁷ Penetration testing seeks to identify weaknesses and vulnerabilities that may have the potential to allow inappropriate and unauthorised access to the application functionality and data.

⁸ The SA Government's Office for Cyber Security Watch Desk is a function of the Department of the Premier and Cabinet.

- Agencies are required, in certain situations, to maintain copies of their application source code⁹ where the application is being provided through an ongoing external service arrangement. This is so that if the arrangement between the government and service provider ends the agency could still potentially maintain and update the application if required.
- Agencies are required to ensure appropriate user profiles to systems are applied, with adequate segregation of duties.

What we reviewed

In addition to our standard ITGC testing we conducted the following testing at selected agencies:

- assessing the remediation status of issues identified as part of prior penetration testing performed across agency infrastructure
- reviewing application source code arrangements, including its retention
- assessing the adequacy of segregation of duties across application user roles.

What we found

For the selected agencies tested we noted:

- delays in remediating findings from an internal security and penetration testing review
- insufficient access to application source code
- segregation of duty conflicts.

The findings relating to segregation of duties conflicts and insufficient access to application source code were rated high.

2.4 What we recommended and agency responses

Our recommendations to agencies include strengthening the following controls:

- **user access management** – prompt removal of inappropriate user access, performing regular user access reviews and maintaining evidence of user access changes
- **change management** – improving policies and procedures, maintaining documented evidence supporting change activities and post-implementation testing, and applying appropriate segregation of duties throughout the change management process
- **password management** – strengthening password configuration settings, improving policies and procedures and conducting regular reviews of password setting policies

⁹ Source code is the foundation of a computer program and contains instructions, functions and other statements that provide guidance as to how the application software performs.

- **audit logging** – implementing and reviewing audit logging and improving policies and procedures
- **disaster recovery** – developing and regularly reviewing formal disaster recovery plans and associated procedures and conducting disaster recovery tests
- **patch management** – developing and improving policies and procedures to ensure patches are appropriately applied
- **other matters** – ensuring that application source code arrangements are regularly reviewed, updated and retained. Also ensuring that remediation of prior internal security and penetration testing reviews is timely, and suitable documentation of this is maintained.

Agencies generally responded positively to our findings with details of their remediation time frames.

3 Legacy system review

3.1 Executive summary

3.1.1 Introduction

A legacy ICT system is either:

- outdated
- unable to be upgraded
- in need of modernisation (eg it is unable to be interfaced with other business systems)
- no longer supported by the vendor, including security updates, or support is limited.

Many SA Government agencies are using legacy ICT systems to store, process, modify and transmit operational and financial data. In some cases legacy systems are delivering core services. These systems may continue to provide their original intended services but may also present ongoing agency risks and challenges.

Risks of using legacy systems potentially include increased ongoing maintenance costs, higher risk of system failure, increased susceptibility to security vulnerabilities, inability to integrate with other key systems and insufficient access to personnel who have adequate support expertise.

Maintaining existing business operations using legacy systems may also reduce an agency's ability to evolve and meet its future business objectives, including modernising the way it interacts and servicing the needs of its internal and external clients.

Given their risks and challenges, we have previously reported on legacy systems within government, including the status of various ICT replacement projects. For example, in 2015-16 we reported that eight of the 10 agencies we reviewed were operating unsupported legacy servers, with several not implementing sufficient mitigating controls.¹⁰

This year we surveyed a number of agencies to check the status of their legacy systems. This Report summaries our observation on what they told us.

3.1.2 Conclusion

The SA Government has a challenge in managing the large number of legacy systems currently being used by various agencies.

We acknowledge the difficulties agencies have when accurately assessing the costs and benefits associated with upgrading or replacing their legacy systems. In some cases, replacing them will require significant funding and resourcing.

¹⁰ Auditor-General's Supplementary Report for the year ended 30 June 2016 *Security management of information systems: November 2016*.

Despite these costs, agencies must be proactive in managing legacy systems and report and highlight the risks arising from them. They should prepare business cases to help evaluate the feasibility of replacing these systems against other agency priorities. We note that legacy systems are impacting current business operations and strategic objectives within agencies. They are also potentially increasing operational costs and exposing agencies to additional security risks.

3.1.3 What we found

We provided a questionnaire to the 18 sampled agencies (refer to section 3.2 for sample details). Their responses noted the following impacts, risks and challenges in maintaining legacy systems:

- Agencies are experiencing additional vendor costs to maintain legacy systems. Although the exact cost is difficult to quantify, the amount totalled at least \$20 million for the sampled agencies.
- There were 215 legacy applications in operation at the sampled agencies. Many of them were over 10 years old, only 59% of them were under vendor support arrangements and agencies considered many of them to be key business applications.
- Some agencies did not have plans to replace some legacy applications for a range of reasons. This included budget constraints, no vendor upgrade being available, other agency priorities, resource limitations or the agency was still assessing future options.
- Most of the sampled agencies did not have enough internal resources and expertise to support some of their legacy applications.
- Some legacy applications were difficult to change to meet future business workflow needs. Some also had performance issues or were at increased risk of failure and some were impacting current business workflows. Other concerns included security vulnerabilities, compatibility and integration issues. In many cases these legacy systems were impacting their current business operations and strategic objectives.
- The sampled agencies provided full listings of their operating systems and databases. We considered 1266 of the total 5602 operating systems and 219 of the total 1928 databases to be legacy.
- The sampled agencies provided details of the legacy network devices¹¹ in their environments. Due to the large number of network devices in operation we limited this request to firewalls, routers and switches. We identified that 13 of the sampled agencies had legacy network devices and many were unsupported.

3.2 Review objective, scope and approach

The purpose of our high-level review was to determine the extent and impact of legacy ICT systems within the SA Government. To conduct this review we gathered high-level information

¹¹ Electronic devices used to help connect equipment such as computers, printers and servers in a computer network.

from a sample of 18 agencies:

- Attorney-General's Department
- Courts Administration Authority
- Department for Correctional Services
- Department for Education
- Department for Environment and Water
- Department for Health and Wellbeing
- Department of Human Services
- Department of Innovation and Skills
- Department of Planning, Transport and Infrastructure
- Department of Primary Industries and Regions
- Department of the Premier and Cabinet
- Department of Treasury and Finance (Corporate and Shared Services SA)¹²
- Legal Services Commission
- Public Trustee
- SACE Board of South Australia
- South Australia Police
- South Australian Fire and Emergency Services Commission
- South Australian Water Corporation.

We provided these agencies with a questionnaire seeking information about their legacy applications, operating systems, databases and certain network devices. The questionnaire sought details on:

- the costs of operating and maintaining legacy environments
- plans for decommissioning or replacement
- impacts of legacy systems on agency workflows
- impacts of legacy systems on ICT strategies
- security issues and risks associated with legacy systems
- resourcing and support arrangements to manage legacy systems.

Our analysis of agency responses to our questionnaires is summarised below. We did not seek supporting evidence to validate these responses and have relied on the completeness and accuracy of the information the agencies provided.

3.3 Details of findings

3.3.1 Vendor costs for legacy system maintenance and support

We asked agencies about the vendor maintenance and support costs associated with managing their legacy systems. This includes their legacy applications, operating systems and databases. For the 18 sampled agencies, vendor support costs totalled around \$20 million¹³ p.a.

¹² The Corporate and Shared Services SA business units are both managed by the Department of Treasury and Finance. For this Report we provided separate questionnaires to these two business units and treated each business unit as a separate entity.

¹³ These figures were provided by the agencies and were not audited.

Figure 3.1: Total vendor costs for legacy system maintenance and support

| Legacy system type | Vendor cost \$'000 |
|------------------------------------|-----------------------|
| Applications | 18 879 |
| Operating systems extended support | 1 049 |
| Databases extended support | 79 |
| Total | 20 007 |

We note this amount did not include legacy systems where agencies:

- did not engage additional vendor support, which equated to over 40% of all legacy applications, 49% of operating systems and 99% of databases
- have only in-house support using internal resources. These additional costs are not included in this total as it was difficult for agencies to accurately allocate the costs to maintain each system.

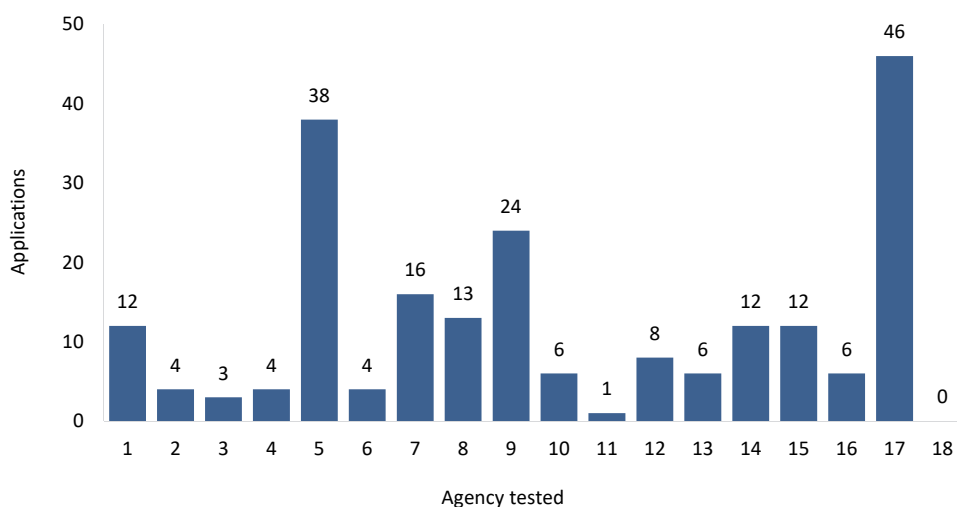
We do acknowledge the difficulties agencies have when accurately assessing the costs and benefits associated with upgrading or replacing these legacy systems. We also acknowledge that while any improved solution may create efficiencies and address current security concerns, it might also require significant funding and resourcing, and that replacing systems in turn can create various project risks that need to be mitigated.

3.3.2 Legacy applications

Extent of legacy applications across SA Government agencies

There were 215 legacy applications in operation at the 18 agencies we sampled. The extent of legacy applications varied between agencies, with two agencies maintaining significantly more than others.

Figure 3.2: Total legacy applications across agencies tested

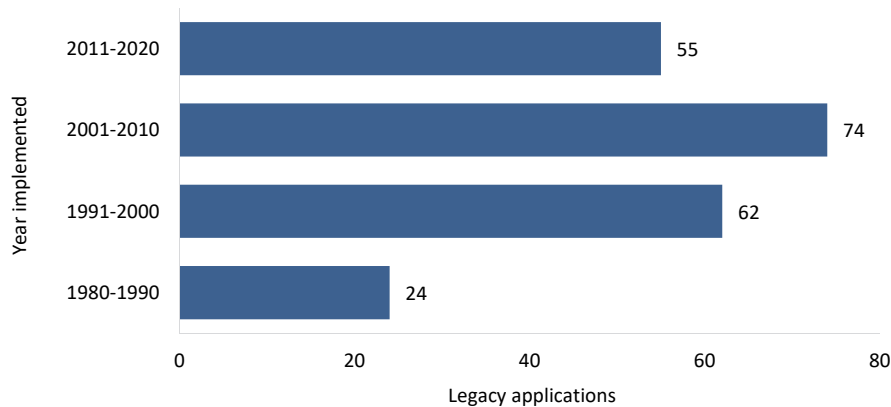


One agency we sampled did not have any legacy applications in operation.

Age of legacy applications

We noted that of the 215 legacy applications reported by the sampled agencies, 55 (26%) were under 10 years old. The remaining 160 (74%) applications ranged from 10 to over 26 years old.

Figure 3.3: Legacy applications – year implemented



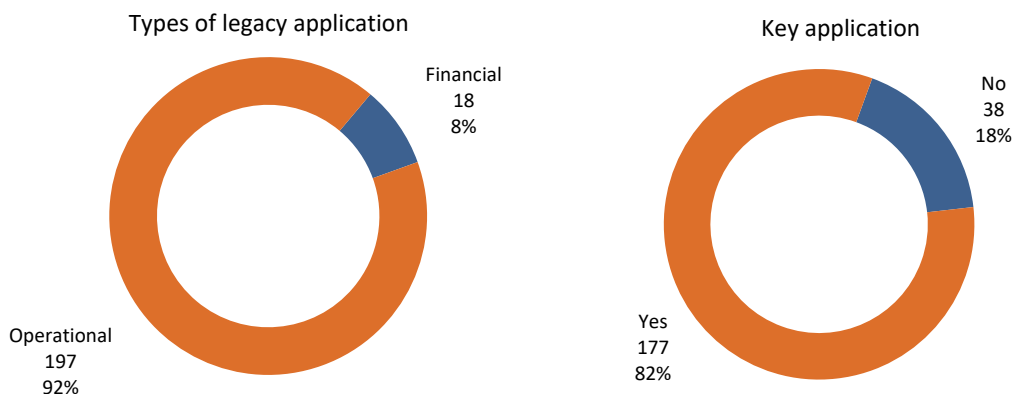
While we acknowledge that some legacy applications are meeting current business needs, they may present agencies with other risks and challenges. These include security vulnerabilities, the inability to integrate with other business applications, potential system performance issues, and the inability to meet current business workflows and agency strategic objectives.

Types of legacy applications

Of the 215 legacy applications, the sampled agencies identified 177 (82%) as key business applications. Further, a large proportion (197 or 92%) were identified as operational applications with only 18 (8%) being financial.

Overall, agencies appear to be taking appropriate action to update or replace their financial applications, but a large number of operational applications remain. Agencies advised that there were plans to enhance or replace over half of these operational applications.

Figure 3.4: Types of business legacy applications



Last time legacy applications were upgraded

Of the legacy applications reported, the sampled agencies advised that 60% had been upgraded in the last five years, with 49% upgraded in the last two years. It is positive that agencies are implementing vendor upgrades for most applications as they become available.

Our testing indicated that of the remaining applications not upgraded in the past five years, 48% of them were unsupported by the application vendor. Further, 66% of these unsupported applications were key business applications.

In addition, five agencies did not maintain records of when their legacy applications were last upgraded. Two applications implemented in 2007 and 2008, at separate agencies, have not been upgraded during their operational life.

Figure 3.5: Legacy applications – years since last upgrade

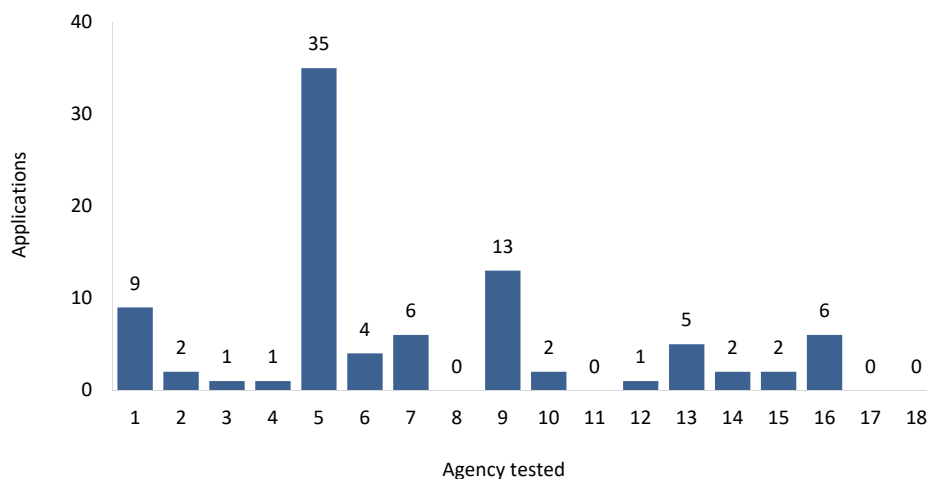
| Year of last upgrade | Applications | Percentage of total legacy applications |
|----------------------|--------------|---|
| 1 to 5 years | 130 | 60% |
| 6 to 10 years | 36 | 17% |
| 11 to 15 years | 20 | 9% |
| 16 to 20 years | 6 | 3% |
| 21 to 25 years | 6 | 3% |
| Over 26 years | 4 | 2% |
| Unknown | 13 | 6% |
| Total | 215 | 100% |

Legacy application vendor support arrangements

Responses from the sampled agencies indicated that 59% of applications were under vendor support arrangements, with 41% unsupported. We note that 34% of the unsupported applications were key business applications.

As shown in figure 3.6 only three agencies had all their legacy applications under vendor support arrangements. One agency responded that they did not have any legacy applications in operation.

Figure 3.6: Applications not under vendor support arrangements



We also sought to understand if agencies intend to continue using their legacy applications and whether they expected to receive future vendor support.

Figure 3.7: Future vendor support arrangements

| Future vendor support arrangements | Legacy application | Percentage of total legacy applications | Key business applications |
|---|--------------------|---|---------------------------|
| In-house support until archived or replaced | 41 | 19% | 41 |
| Intend to use and DO NOT expect the vendor to provide support | 41 | 19% | 27 |
| Intend to use and expect the vendor to provide support | 90 | 42% | 81 |
| DO NOT intend to use | 43 | 20% | 28 |

Plans to upgrade or replace legacy applications

We sought to understand how many legacy applications the sampled agencies intended to upgrade or replace. Agencies advised us that they intended to upgrade or replace 162 (75%). 55 of these were to be enhanced to meet business requirements and 107 were to be replaced.

Agencies did not have any plans to upgrade or replace the remaining 53 legacy applications. Agencies considered 39 of these to be key business applications. Figure 3.8 provides the agencies' reasons for not intending to upgrade or replace them.

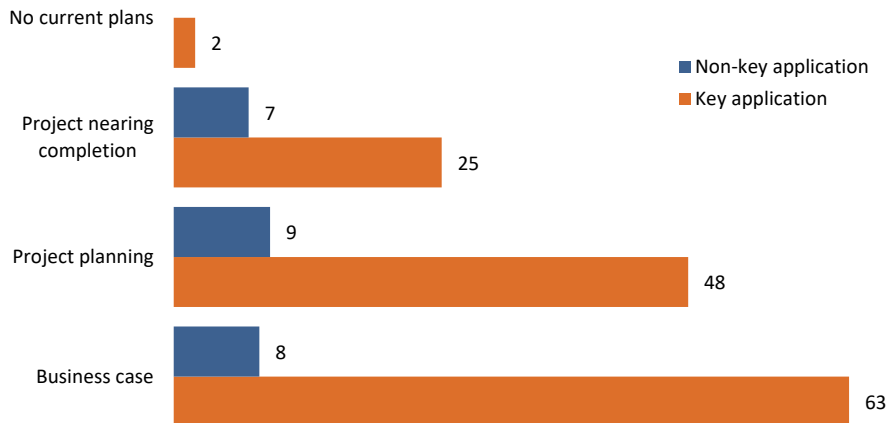
Figure 3.8: Reasons for not upgrading or replacing

| Agency reasons | Legacy application | Key application |
|---------------------------------------|--------------------|-----------------|
| Due to budget constraints | 3 | 1 |
| Due to no vendor upgrade availability | 6 | 4 |
| Due to other agency priorities | 27 | 20 |
| Other | 17 | 14 |
| Total | 53 | 39 |

'Other' related to resource deficiencies or the agency was still assessing future options.

For the agencies that indicated they were planning to upgrade or replace their legacy applications, we sought to understand the status of their plans. These plans are shown in figure 3.9.

Figure 3.9: Status of current plans to upgrade or replace

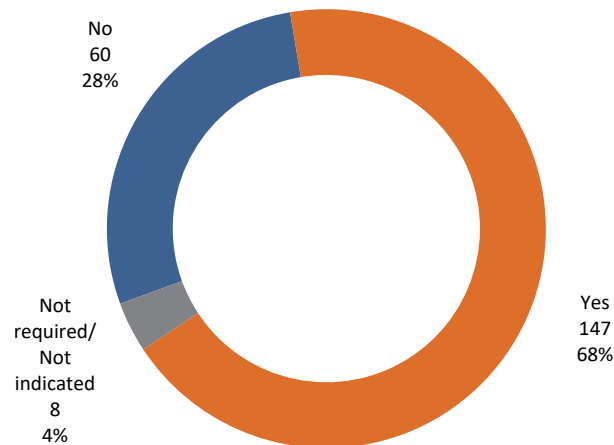


Extent of internal resources and expertise to support legacy applications

Responses from the 18 sampled agencies indicated that 13 of them did not have enough internal resources and expertise to support some of their legacy applications.

Of the 215 legacy applications identified, the 18 sampled agencies indicated that they have the required support to maintain 147 (68%) of them. Despite this, the 13 agencies advised they did not have enough support to maintain 60 legacy applications, of which 49 were considered key business applications.

Figure 3.10: Internal resources and expertise to support legacy application systems



Of the eight applications shown as ‘not required/not indicated’, agencies advised they either no longer required active support or were being decommissioned, or did not indicate whether support was required.

Business impacts and strategic objectives

We asked agencies to advise the business impacts of using their legacy applications. Of the 217 legacy applications identified, agencies indicated that:

- 69 applications (32%) had no current business impacts. 52 of these were key business applications.
- 64 applications (30%) were difficult to change to meet future business workflow needs, and 51 of these were key business applications
- 55 applications (26%) had performance issues or were at increased risk of failure. 51 of these were key business applications
- the remaining 27 applications (13%), 23 of which are key business applications, were impacting current business workflows.

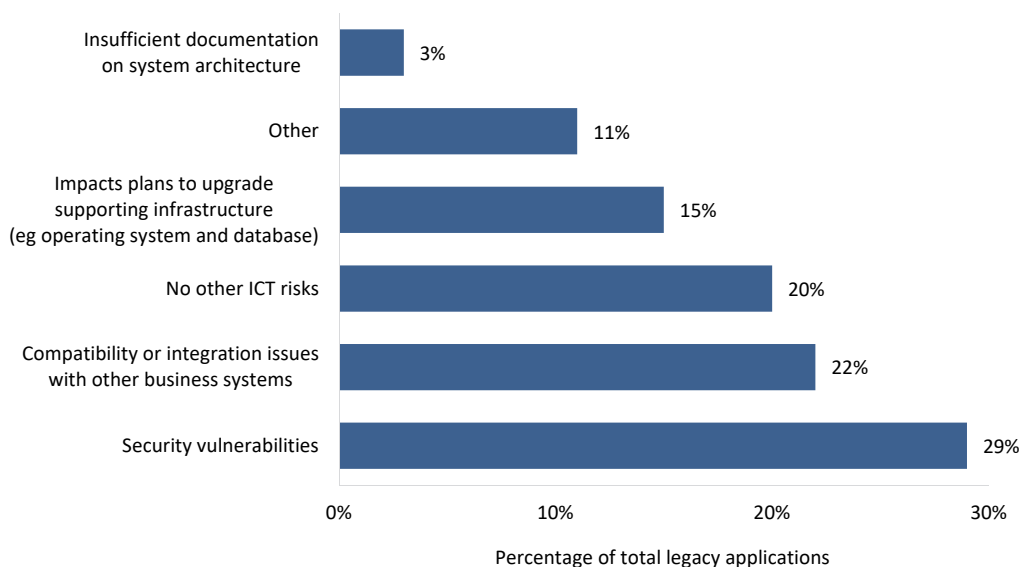
Overall, agencies noted that 58% of key business applications were having some impact on their current business operations.

Further, 73 legacy applications (34%) are currently impacting 15 agencies' strategic objectives. Agencies considered 70 of them to be key business applications.

Other key ICT risks of using legacy applications

We asked the sampled agencies to advise of any further key ICT risks associated with operating their legacy applications, other than the impacts mentioned in section 3.4.8. They considered security vulnerabilities, compatibility and integration issues as their main concerns.

Figure 3.11: Other key ICT risks of using legacy applications



The 11% of ICT risks noted as 'other' include legacy business rules, architecture constraints, lack of redundancy and diminishing resource availability.

3.3.3 Legacy operating systems

We sought full operating system listings from each agency to determine the extent of legacy operating systems in use. We were provided with a list of 5602 operating systems, 1239 of which we considered to be legacy. All agencies, except for one, maintained some legacy operating systems.

Figure 3.12: Extent of legacy operating systems

| Type of operating system | Total instances ¹⁴ | Instances of legacy operating systems | Legacy operating systems under extended support arrangements | Unsupported legacy operating systems |
|--------------------------|-------------------------------|---------------------------------------|--|--------------------------------------|
| Windows | 4 752 | 1 060 | 540 | 520 |
| Solaris | 149 | 26 | 19 | 7 |
| Linux | 367 | 42 | 7 | 35 |
| Vmware | 154 | 32 | 5 | 27 |
| Other | 180 | 79 | 50 | 29 |
| Total | 5 602 | 1 239 | 621 | 618 |

We acknowledge that agencies have reduced the impact of standard support arrangements ending by implementing extended support arrangements at an additional cost, but that does not mean, in our opinion, that they are not legacy systems.

In addition, extended support arrangements may not address all agency concerns with their environments. For example, some vendor extended security updates under an extended support contract may not include new features, customer-requested non-security hotfixes and design change requests. Extended support may also only be available for a certain period.

3.3.4 Legacy databases

We also sought full database listings from each sampled agency to determine the extent of legacy databases in use. Agencies identified 1928 databases, of which only 219 were legacy. All agencies, except for one, maintained some legacy databases.

Figure 3.13: Extent of legacy databases

| Type of operating system | Total instances ¹⁵ | Instances of legacy databases | Percentage of legacy databases |
|--------------------------|-------------------------------|-------------------------------|--------------------------------|
| Microsoft | 1 203 | 158 | 13% |
| Oracle | 699 | 50 | 7% |
| Other | 23 | 8 | 35% |
| Total | 1 925 | 216 | 11% |

We note that there were no Microsoft databases under extended support arrangements. Only five Oracle and two 'other' instances were under extended support arrangements.¹⁶

¹⁴ For some agencies, the total operating system figures changed between the time they were originally provided and, when they confirmed the extent of legacy instances.




¹⁵ For some agencies, the total operating system figures changed between the time they were originally provided and their confirmation of the extent of legacy instances.

¹⁶ 'Other' includes a range of types of databases, such as MySQL, SybaseSQL, OpenEdge and Integrated Database Management System.

3.3.5 Legacy network devices

We asked the sampled agencies to provide details of the legacy network devices in their environments. Due to the large number of network device types in use we limited this request to firewalls, switches and routers. We note that agencies also maintain several other network device types.

Figure 3.14: Description of firewalls, switches and routers

| | | |
|---|-----------------|---|
|  | Firewall | Is a network security device that monitors incoming and outgoing network traffic. Using a defined set of security rules, a firewall will decide whether to allow or block specific traffic to the intended destination. |
|  | Switch | Connects computer devices (such as computers and printers) in a network to each other. Devices are then allowed to ‘talk’ to each other by the switch receiving incoming data packets and redirecting them to their destination on a single computer network. |
|  | Router | Similar to a switch, a router redirects or routes data packets between computer devices. A router is a more sophisticated device than a switch, with a traditional router designed to connect or join multiple area networks to form an even larger network. |

We found that 13 of the 18 agencies sampled maintained some legacy network devices. Further, 24% of the network devices identified had reached their last day of support.¹⁷ Of these devices, 56% were under extended support arrangements,¹⁸ leaving 44% unsupported.

Figure 3.15: Extent of legacy network devices and extended support arrangements

| Network devices | Total devices | Legacy devices (reached last day of support) | Legacy devices under extended support arrangements | Unsupported legacy devices |
|-----------------|---------------|--|--|----------------------------|
| Firewalls | 89 | 38 | 23 | 15 |
| Routers | 3 191 | 723 | 512 | 211 |
| Switches | 2 387 | 601 | 224 | 377 |
| Total | 5 667 | 1 362 | 759 | 603 |

We asked agencies to advise their plans to replace the legacy network devices currently in use. We found that of the 18 sampled agencies:

- four maintain legacy firewalls. All have plans to replace these devices

¹⁷ The last date to receive applicable service and support as entitled by active service contracts for covered products. After this date, the service is no longer available.

¹⁸ Extended Support provides support for Cisco Hardware and On-Premise, perpetual Application Software that are beyond the Last Date of Support (LDoS). Refer to <https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/cisco_extended_support_service.pdf>, viewed 17 July 2020.

- 10 maintain legacy routers, of which:
 - two of these agencies advised they did not intend to replace these devices within two years
 - five agencies advised they intended to replace up to half of these devices within two years
 - three agencies advised they would replace between 51% and 100% of these devices within two years
- 14 maintain legacy switches of which:
 - one agency advised they did not intend to replace these devices within two years
 - four agencies advised they intended to replace up to half of these devices within two years
 - nine agencies advised they would replace between 51% and 100% of these devices within two years.

