Office of the Auditor General
Serving the Public Interest

Report 16: 2023-24 | 27 May 2024

INFORMATION SYSTEMS AUDIT RESULTS

Local Government 2022-23

Office of the Auditor General
for Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Paul Tilbrook
Information Systems Audit team

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

Image credit: shutterstock.com/13_Phunkod

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government 2022-23 – Information Systems Audit Results

Report 16: 2023-24
27 May 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT 2022-23 – INFORMATION SYSTEMS AUDIT RESULTS

This report has been prepared for submission to Parliament under the provisions of section 24 of the *Auditor General Act 2006*.

Our information systems audits focus on the computer environments of entities to determine if their general computer controls effectively support the confidentiality, integrity and availability of information systems and the information they hold.

This is our fifth report on the findings from our audits of local government entities' information technology general computer controls.

I wish to acknowledge the entities' staff for their cooperation with this audit.

Caroline Spencer
Auditor General
27 May 2024

Contents

Auditor General's overview

This report summarises the results of the 2022-23 cycle of local government entities' information systems audits performed between April 2023 and March 2024. As these audits focus on areas that may affect the confidentiality, integrity and availability of the entities' information and systems, they are an essential part of our financial statement audits.

Our audit results show entities have improved the maturity of their control capability since our first information system audits in 2019-20, with the biggest improvements in risk and change management. However, significant improvements are still needed in all other areas.

Information and cyber security remains the highest concern due to the number of weaknesses we continue to identify in the five related categories (access management, endpoint security, human resource security, network security and information security framework). Entities need to better protect themselves against external and internal threats to reduce the risk of security breaches. Internal threats can be notably reduced through fit-for-purpose human resource controls such as screening, onboarding and offboarding procedures, and cyber security education programs.

This year, we reported 473 (58 significant, 328 moderate, 87 minor) issues to 76 entities. Concerningly, a large proportion (45%) of significant issues were unresolved findings from last year.

I encourage all entities to take note of the findings and recommendations in this report and implement fit-for-purpose solutions.

2022-23 at a glance

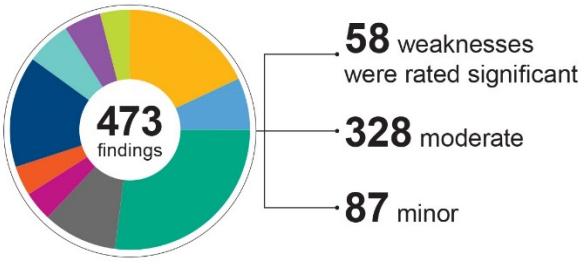
Auditing local government entities

(Prior year shown in brackets)

473 (PY: 324 at 53 entities) general computer controls findings at 76 entities

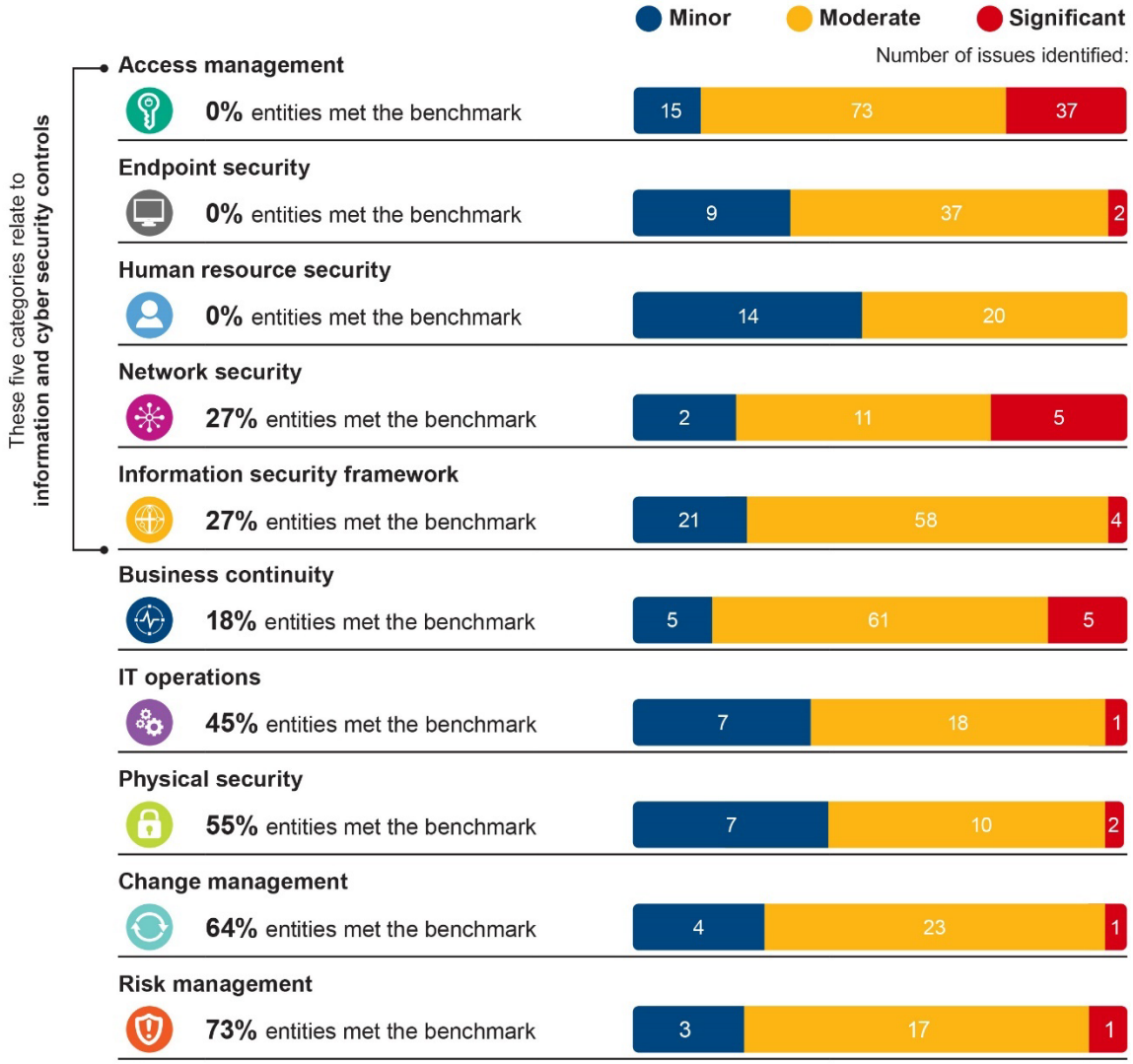
11 (PY: 12) capability maturity assessments

Key insights



45% of the significant findings were unresolved issues from prior year

Snapshot of general computer controls findings and capability maturity assessments



Introduction

This is our fifth report on the findings from our audits of local government entities' information technology general computer controls (GCC)[1]. GCC audits are an essential part of our audits of local government entities' financial statements and are a requirement of the Australian auditing standards[2]. Our GCC audits determine if entities' information technology and related internal controls effectively support the integrity, availability and confidentiality of the information and systems used to prepare the financial statements.

The entities vary in the nature and complexity of the information technology they use to process and maintain their financial information. However, the ever-changing internal and external threat environment exposes all entities to the risk of compromise. Appropriate controls help entities to protect their information and systems.

In 2022-23, we reported GCC findings to 76[3] entities, compared to 53 entities last year[4]. Eleven of these entities were provided with capability maturity assessments. These assessments look at how well-developed and capable entities' established IT controls are. This report summarises the results of our GCC findings and capability maturity assessments.

Our GCC audits incorporate recognised industry better practices and consider various factors, such as:

- business objectives of the entity
- level of entity reliance on IT
- technological sophistication of entity computer systems
- significance of information managed by the entity.

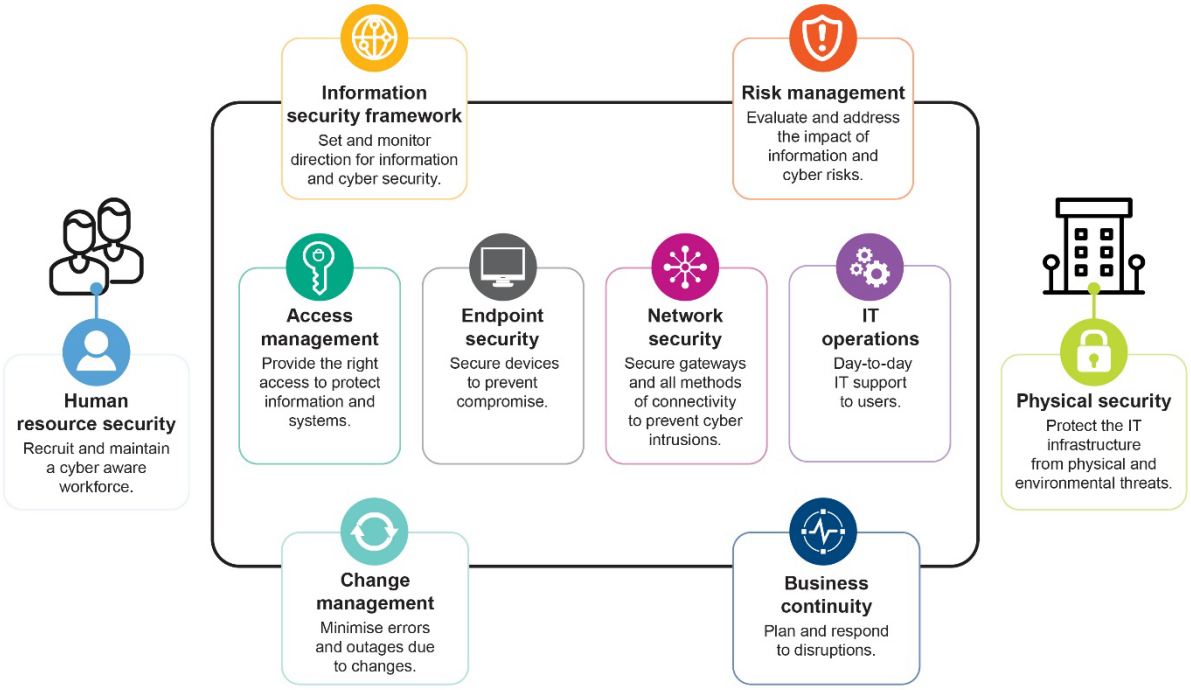
Figure 1 shows the 10 categories covered in our GCC audits.

[1] Our 2018-19 GCC and capability maturity assessments were done to inform our approach to assessing the sector's capability. 2018-19 results are not comparable to subsequent years and are therefore not shown.

[2] Auditing and Assurance Standards Board, *Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement*, AUASB, February 2020.

[3] Entities issued with GCC findings at 29 March 2024. Opinions of 10 local governments are not yet issued and their results are not included in this report. The entities are a mix of regional and metropolitan local governments.

[4] The number of entities issued GCC findings increased as auditing standards now require more consideration of IT and cyber security controls.



Source: OAG

Figure 1: General computer controls categories

Conclusion

In 2022-23, we reported 473 control weaknesses to 76 entities, compared to 324 weaknesses to 53 entities last year. The majority of these weaknesses were in categories that increase information and cyber security risks. Entities need to address these to protect their information and systems from security breaches.

While a number of entities addressed some prior year audit findings, most of the significant control weaknesses were not addressed. Entities should address these weaknesses as a priority and implement compensating[5] controls while progressing long term plans, such as migration to new platforms. Unresolved weaknesses can seriously impact the overall integrity of entities' IT environments and operations.

Our capability maturity assessments at 11 entities show improvement since our first assessments in 2019-20, with more controls meeting the benchmark. The biggest improvements have been in the categories of risk and change management, but significant improvement is still needed in all other categories.

This year's assessments showed some improvement in one of the five categories related to information and cyber security (network security) but only three entities met the benchmark. Categories of highest concern were access management, endpoint security and human resource security with no entities meeting the benchmark.

There was no material change in four categories (information security framework, IT operations, change management and IT risk management) while business continuity and physical security declined slightly.

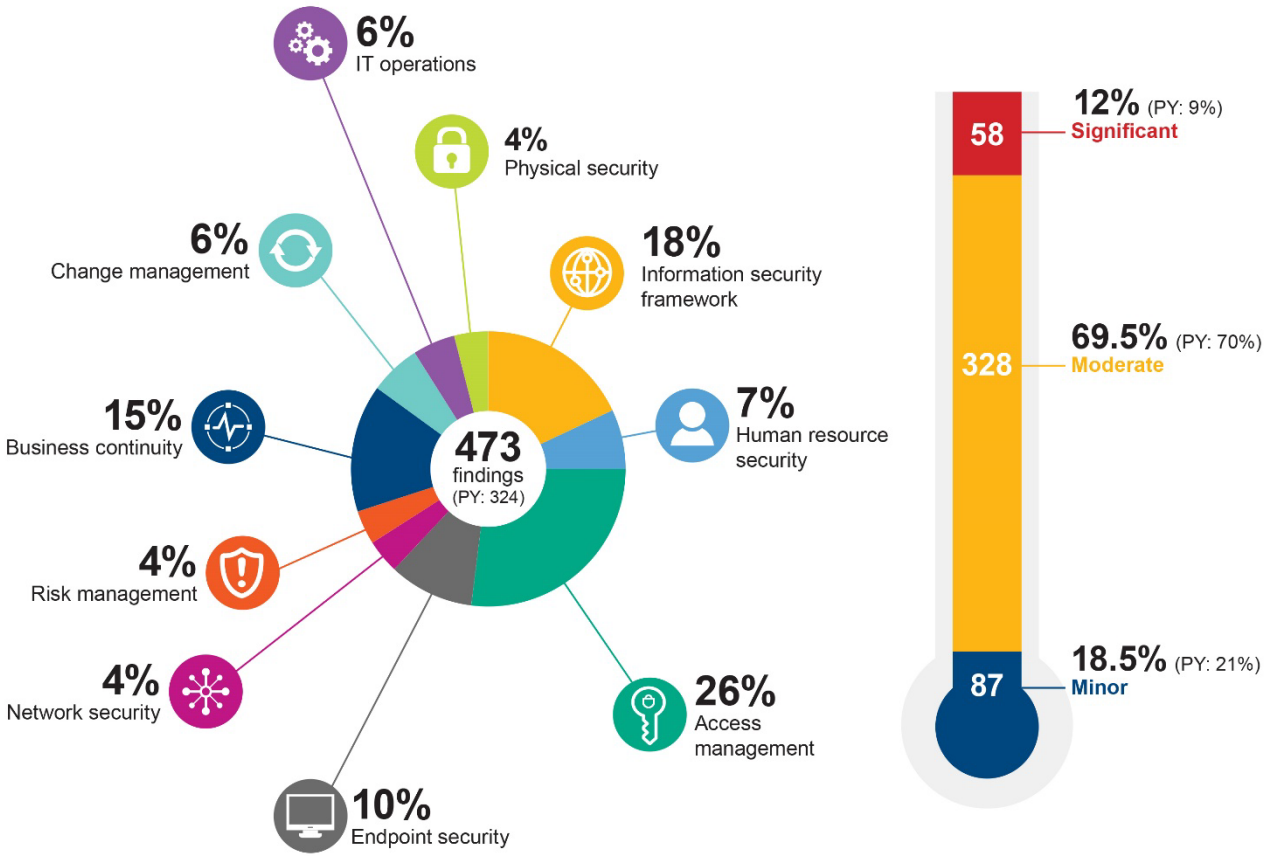
[5] Stop gap measures to address vulnerabilities where primary controls cannot be implemented due to limitations.

What we found: General computer controls

We reported 473 control weaknesses to 76 entities; 58 weaknesses were rated significant, 328 moderate and 87 minor. The increase in the number of entities issued GCC findings reflects changes in auditing standards[6] that require higher consideration of IT and cyber security controls.

There was a 3% increase in the number of significant findings compared to last year (Figure 2), which is mainly due to more entities issued findings this year. Although the majority of control weaknesses were rated moderate, these weaknesses combined significantly increase an entity's overall exposure to cyber threats.

Case studies throughout this report highlight the importance of good controls.



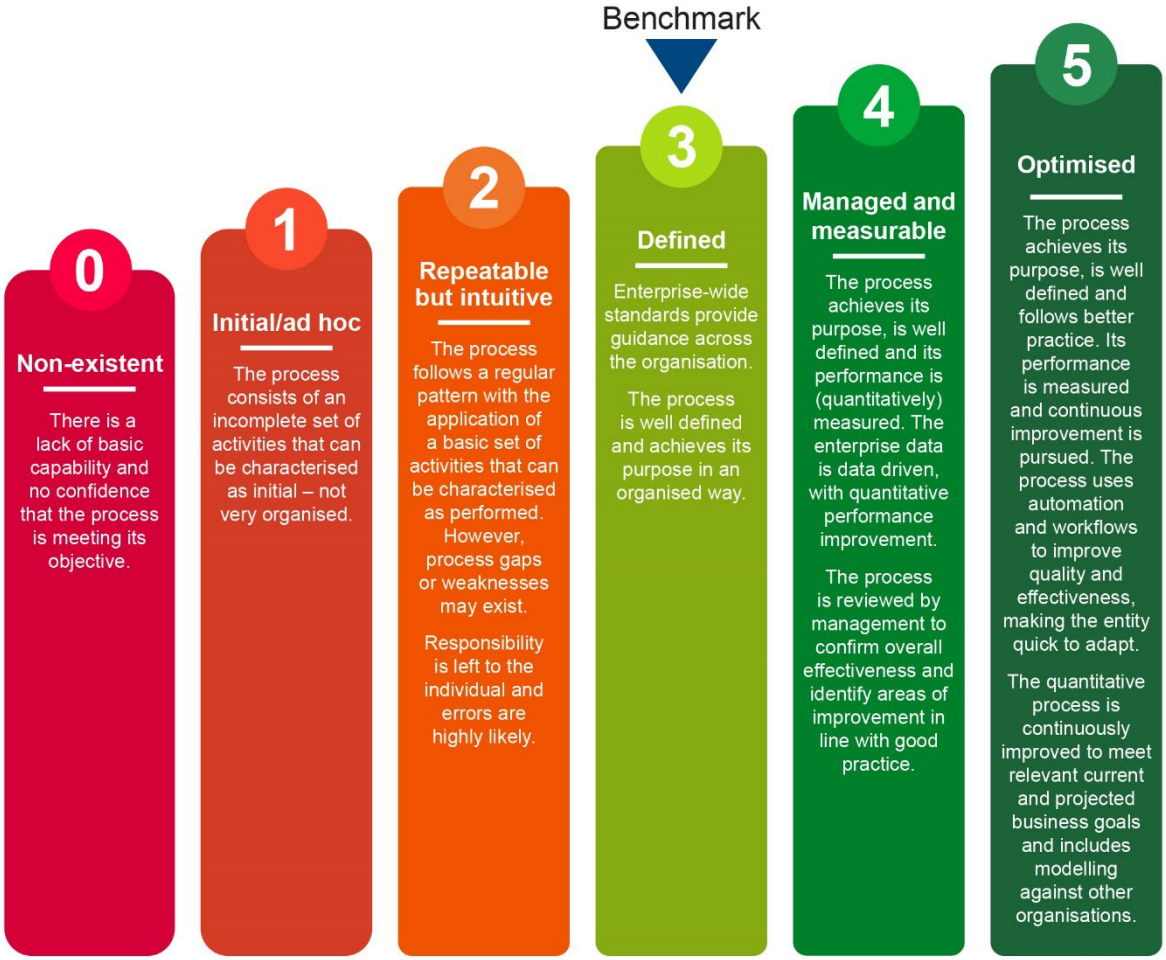
Source: OAG

Figure 2: Ratings and distribution of GCC findings in each control category

[6] Auditing and Assurance Standards Board, *The Consideration of Cyber Security Risks in an Audit of Financial Report*, AUASB, May 2021 *and* Auditing and Assurance Standards Board, *Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement*, AUASB, February 2020.

What we found: Capability assessments

We performed capability maturity assessments at 11 entities compared with 12 last year. This involved assessing the capability maturity level across the 10 GCC categories using a 0-5 rating scale[7] (Figure 3). To meet the benchmark, entities need to achieve a level 3 (Defined) rating or better.

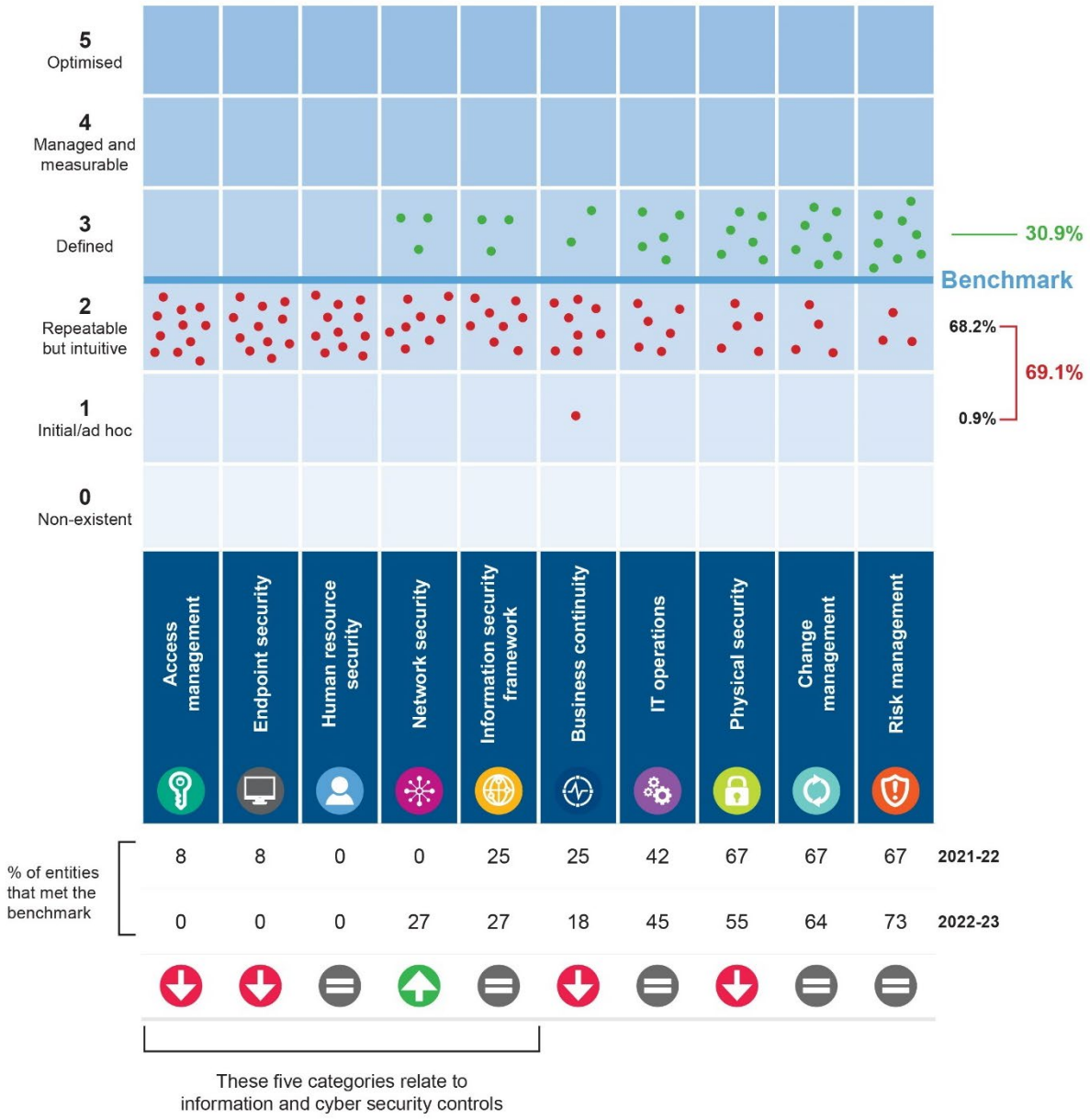


Source: OAG

Figure 3: Capability maturity rating scale and criteria

[7] The information within this maturity model assessment is derived from the criteria defined within the framework Control Objectives for Information Technologies 2019, released in 2018 by ISACA (an international professional association focused on IT governance).

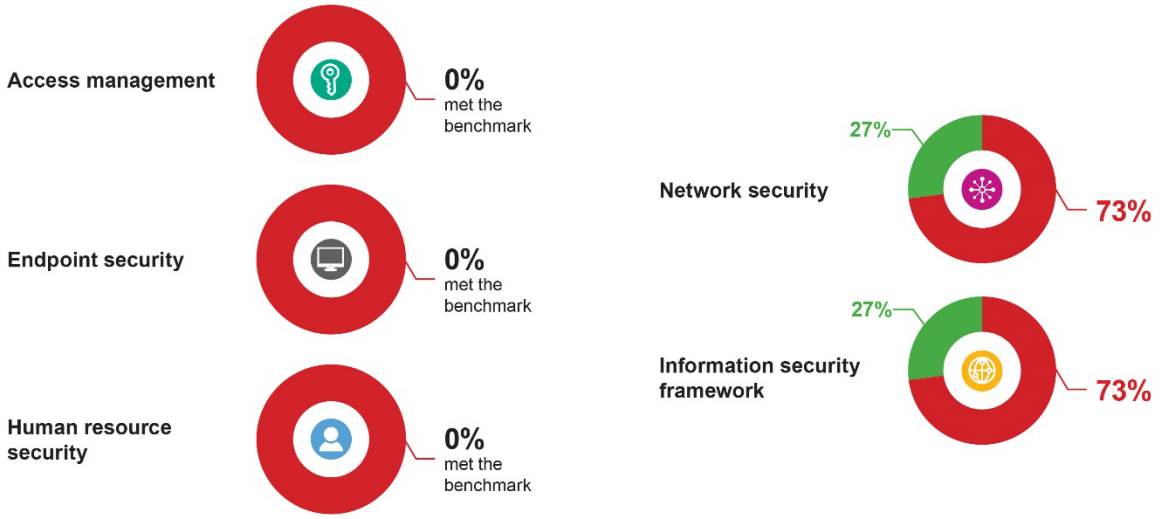
Figure 4 shows the results of our capability maturity assessments.



Source: OAG

Figure 4: Capability maturity assessment results

While there were improvements in network security this year, most entities were still not meeting the benchmark in the five information and cyber security categories (Figure 5). Entities must plan and implement fit-for-purpose controls to protect their operations and information from internal and external threats.



Source: OAG

Figure 5: Percentage of entities that met/did not meet the benchmark in the five information and cyber security categories

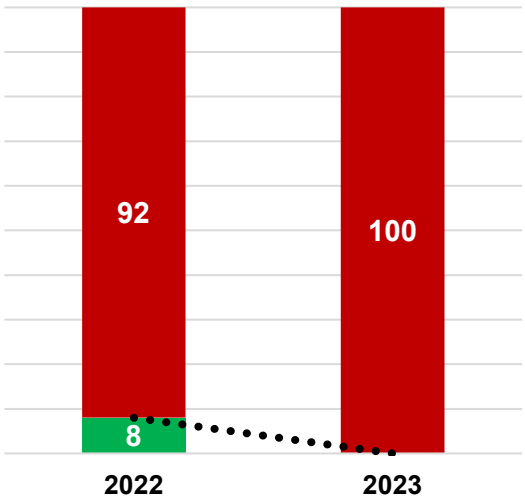
Entities continue to adopt digital technologies to improve engagement with their communities and deliver efficiencies in their service delivery. While there are many benefits to these digital technologies, there remains the ever-present and evolving nature of cyber security threats. Effective cyber security controls help entities manage risks, protect sensitive information and deliver services securely.

Entities are encouraged to implement the Australian Cyber Security Centre's mitigation strategies designed to protect against common cyber threats with a key focus on Essential Eight controls.

1. Access management

None of the 11 entities met the benchmark compared with one of 12 last year. This control category also had the highest number of significant GCC findings this year, mainly due to inappropriate or excessive administrative privileges within the finance systems. Poor access management controls increase the risk of security incidents, financial loss and reputational damage.

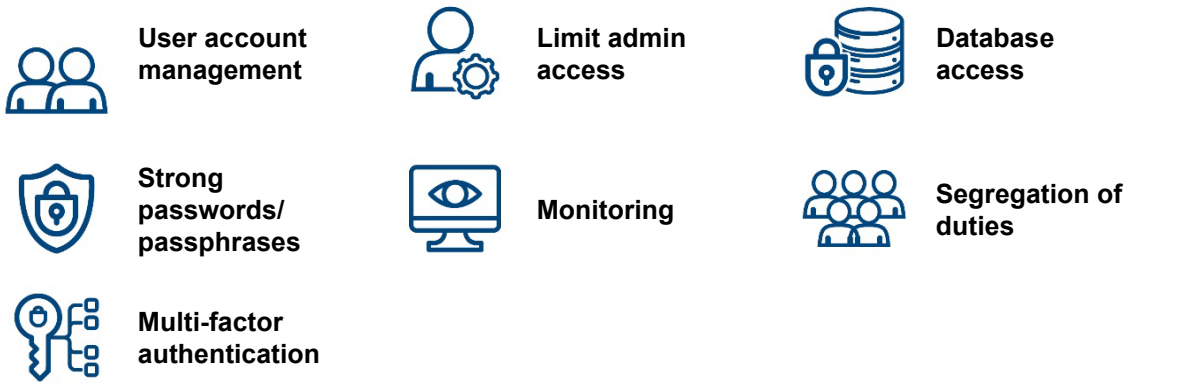
We assessed whether entities use the principle of least privilege to manage access, have strong authentication methods, monitor access and changes to data, and ensure key transactions cannot be performed end to end by the same individual (Figure 7).



Source: OAG

Figure 6: Percentage of entities that met/did not meet the benchmark

We have published a better practice guide[8] to help entities improve access management and protect information assets from unauthorised access. We encourage all public sector entities to adopt the principles in the guide.



Source: OAG

Figure 7: Key access management controls

Common weaknesses included:

- **Administrator privileges were not well managed** – excessive numbers of individuals were given administrator privileges. Administrators did not have separate non-privileged accounts for day-to-day tasks and administrator activity was not logged and monitored. Highly privileged accounts must be well managed as they can change system configurations, access rights and data.
- **Access and activity were not logged and monitored** – application, database and network access and activity were not appropriately logged or monitored to detect malicious activity. Entities should use fit-for-purpose tools to correlate and monitor activity from different systems (e.g. network, applications and databases).
- **Multi-factor authentication (MFA) was not used or not applied to all accounts** – a lack of MFA can increase the likelihood of unauthorised access.
- **Access was not reviewed** – entities did not review accounts to ensure they are required and have least privileges assigned to perform their function. Without a review of accounts (application, network, database, remote access, generic, system and administrator) there is an increased risk of unauthorised access.
- **Access was not appropriately approved** – access to key systems should be appropriately approved to prevent inappropriate access being granted.

The following case studies illustrate a range of control weaknesses in access management.

[8] Office of the Auditor General, *Digital Identity and Access Management – Better Practice Guide*, OAG, Perth, 28 March 2024.

Case study 1: Poor access controls increased the risk of fraud

At one entity, we found receipts had been deleted prior to end-of-day batch processing from the finance system. Poor access controls meant receipts could be deleted by any user without a trace to identify who deleted them. This could compromise the integrity of data and increases the likelihood of fraud.

Case study 2: Excessive superuser access

An entity had granted superuser access to almost all (24 out of 25) of its finance system users. This level of access allows users to inadvertently or maliciously change system configurations and potentially bypass system enforced expenditure authorisation and fraud prevention controls. This type of weakness increases the importance of manual controls as a last line of defence against error and fraud.

Case study 3: Excessive number of domain administrators

An entity granted the highest level of access rights (domain administrator) to 45 accounts, 40 of which also had database administrator rights to the finance and payroll system. Compromise of one account would give an attacker full access to the entity's systems. There is also a risk that unauthorised or unintentional changes of IT systems will occur.

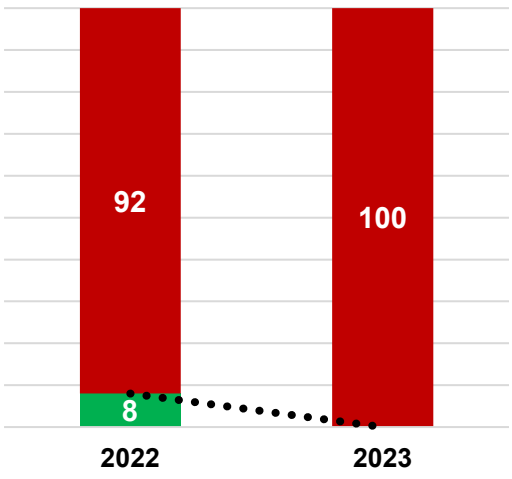
Case study 4: Lack of MFA

An entity is more vulnerable to being compromised through password guessing and phishing attacks, as it does not use MFA and uses single-sign-on for access to its network and finance application. This means a threat actor would gain access to all systems if the entity is compromised. While staff security awareness training can help reduce some risks, entities should prioritise MFA.

2. Endpoint security

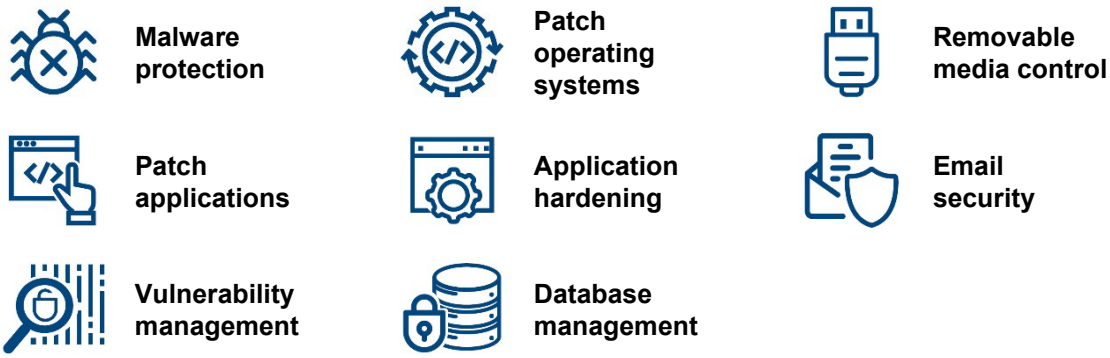
None of the 11 entities met the benchmark, compared with one of 12 last year.

Entities need to implement fit-for-purpose controls to protect endpoints (computers, servers, phones and network devices) from known threats (Figure 9).



Source: OAG

Figure 8: Percentage of entities that met/did not meet the benchmark



Source: OAG

Figure 9: Key endpoint security controls

Common weaknesses included:

- **Unauthorised applications are not prevented** – malicious applications could successfully compromise entities' systems and information.
- **Vulnerability management was ineffective** – systems that are not regularly scanned and patched to fix known vulnerabilities are more susceptible to compromise.
- **Unsupported systems** – key business systems and operating system software were no longer supported by vendors and were therefore not receiving updates designed to fix known vulnerabilities.

The following case study illustrates a common weakness in endpoint security.

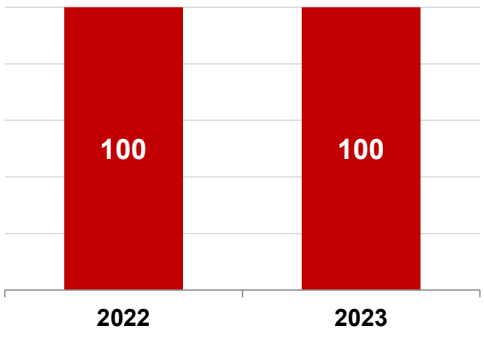
Case study 5: Ineffective application control

An entity only allowed applications and scripts to run from trusted locations. However, all staff could add applications and scripts to these locations to execute them. There is a higher likelihood of malware infections and compromise if unapproved applications are not blocked.

3. Human resource security

Similar to last year, none of the 11 entities met the benchmark in this category. Human resource security ensures employees, contractors and third-party vendors understand their responsibility to protect information during and after engagement.

Fit-for-purpose screening, onboarding and offboarding procedures, and cyber security education are key controls in this category (Figure 11).



Source: OAG

Figure 10: Percentage of entities that did not meet the benchmark

Figure 11: Key human resource security controls

Common weaknesses included:

- **Inadequate background screening** – without fit-for-purpose background screening processes, entities may engage unsuitable individuals (staff or contractors) to positions of trust, increasing insider threat risks.
- **Lack of security awareness training** – regular cyber security education creates a culture of awareness that helps prevent social engineering attacks such as phishing and business email compromise.
- **Exit procedures were not completed** – not completing exit procedures can contribute to unauthorised access to entities' premises, systems and information. This may also increase post-employment integrity risks such as the use or disclosure of confidential information.

The following case study illustrates weaknesses in human resource security.

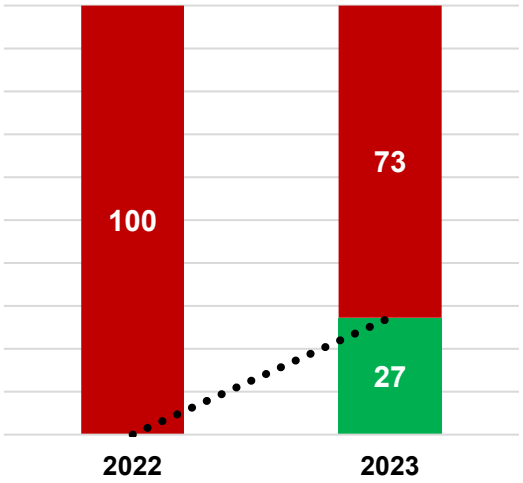
Case study 6: Staff and contractors were not aware of their information security responsibilities

An audited entity did not require its staff and contractors to understand and acknowledge acceptable use of IT resources. Contractors were also not required to sign any confidentiality agreements. There is a higher likelihood that individuals may not understand their information security obligations resulting in data breaches.

4. Network security

There was an improvement this year with three of the 11 entities meeting the benchmark, compared to none last year. The three entities improved their controls to manage and secure network infrastructure, segregated their network and had good monitoring.

Key controls to prevent and limit the extent of cyber attacks include securely configured network devices, network segregation, control over unauthorised connections and regular penetration testing to check that controls are operating as expected (Figure 13).



Source: OAG

Figure 12: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 13: Key network security controls

Common weaknesses included:

- **A lack of controls to block unauthorised devices on the physical network** – unauthorised devices can spread malware or be used to eavesdrop on communications or access sensitive information.
- **Firewall configurations were not reviewed** – reviews help to identify and promptly correct exploitable configuration weaknesses. Firewalls are important security systems that control and protect networks against cyber intrusions.
- **Networks were not segregated** – segregation controls to prevent lateral movement between network segments have not been implemented. Without proper network segregation a cyber breach would be difficult to contain.

The following case study illustrates a common weakness in network security.

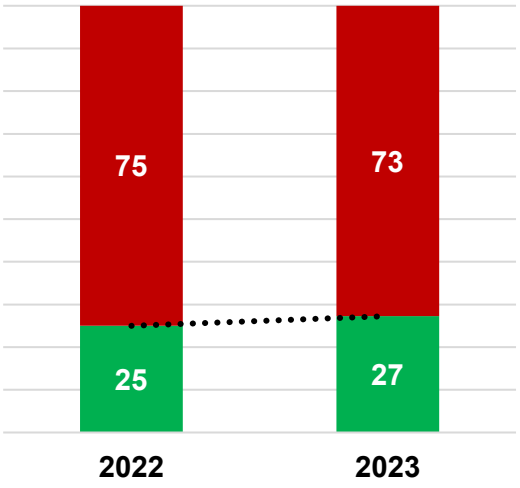
Case study 7: Publicly accessible network port allowed access

An entity did not prevent unauthorised devices from connecting to its physical network and had not segregated its network. We were able to connect a device to the entity's network, view all IT systems and infrastructure and access database, storage and CCTV servers. This entity is at high risk of compromise as unauthorised devices could be used to attack its systems or spread malware.

5. Information security framework

Three of the 11 entities met the benchmark compared with three of 12 last year. A structured approach ensures IT and security initiatives align with business objectives to protect systems and information against emerging threats.

We assessed whether entities had fit-for-purpose information and cyber security policies to govern and mitigate against current and emerging security risks (Figure 15).



Source: OAG

Figure 14: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 15: Key information security framework controls

Common weaknesses included:

- **Information and cyber security policies did not exist or were outdated** – without fit-for-purpose policies, entities' information security objectives are less likely to be achieved.
- **Lack of IT strategy** – an IT strategy is crucial for informing decisions about technology and cyber security investments and implementation. The strategy should align technology and cyber security initiatives with business objectives.

- **Data loss prevention controls were missing or inadequate** – the inadvertent or malicious leakage of information may go undetected and lead to reputational damage.

The following case study illustrates a common information security framework weakness.

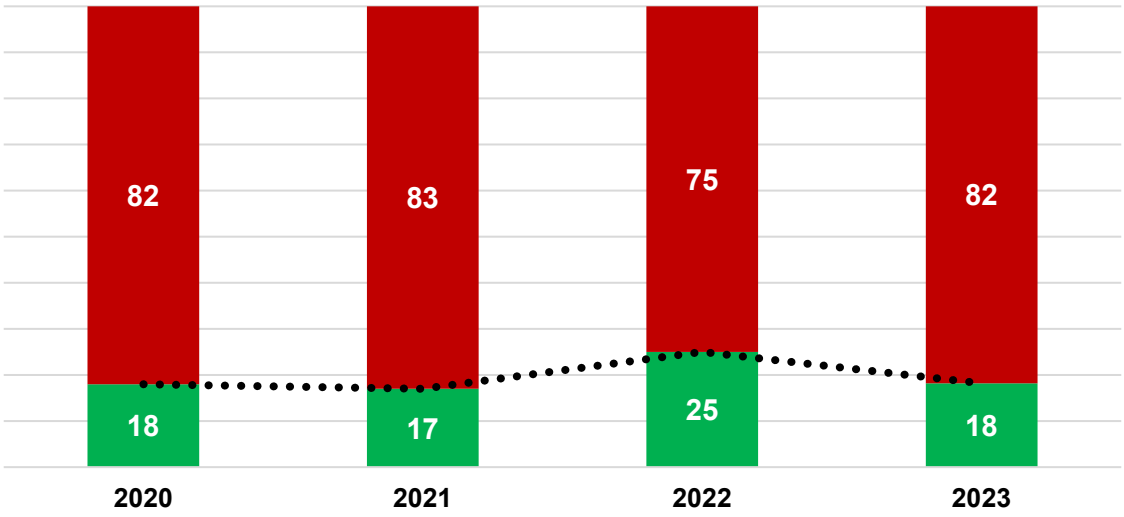
Case study 8: Assurance over cloud based services

An entity did not have a mechanism to know if its vendor's cloud security controls protected its information and systems. When key services are delivered through cloud systems, the cloud vendor must provide important security controls to protect the information and systems. Entities need adequate assurance and visibility that the vendor's controls operate effectively to deliver services in a secure manner.

Independent assurance reports such as a service organisation controls report (SOC2) provide insights into vendor management of cloud infrastructure and systems.

6. Business continuity

We saw a minor decline this year. Only two of the 11 entities met the benchmark in this category, compared with three out of 12 last year. Entities should have fit-for-purpose plans and procedures to guide their response to disruptive events (Figure 17). These should be based on a business impact assessment and agreed recovery objectives.



Source: OAG

Figure 16: Percentage of entities that met/did not meet the benchmark

Source: OAG

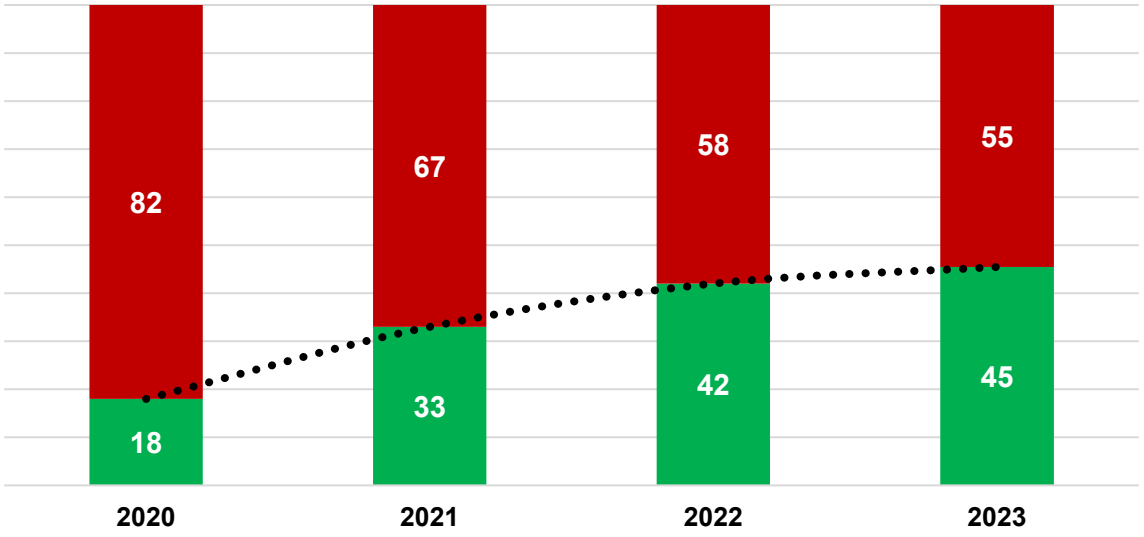
Figure 17: Key business continuity controls

Common weaknesses included:

- **Missing or outdated continuity plans** – delivery of services to the community may experience prolonged outages if adequate continuity plans do not exist.
- **Plans were not tested** – continuity plans must be regularly tested to confirm they can meet recovery expectations.
- **Lack of backup restoration testing** – entities should regularly restore their backups to ensure complete systems can be recovered to a common point. Business-as-usual recovery of files is not sufficient.

7. IT operations

There was no material change in IT operations this year with five of the 11 entities meeting the benchmark. We assessed if the entities had fit-for-purpose service desk processes and appropriately managed IT vendors and IT assets (Figure 19).



Source: OAG

Figure 18: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 19: Key IT operations controls

Common weaknesses included:

- **IT asset registers were poorly maintained and stocktakes not performed** – inadequate management of IT assets can result in loss or theft, leading to financial loss and reputational damage.

- **Service level agreements were not in place or monitored** – a lack of or poorly monitored service level agreements could result in substandard services.

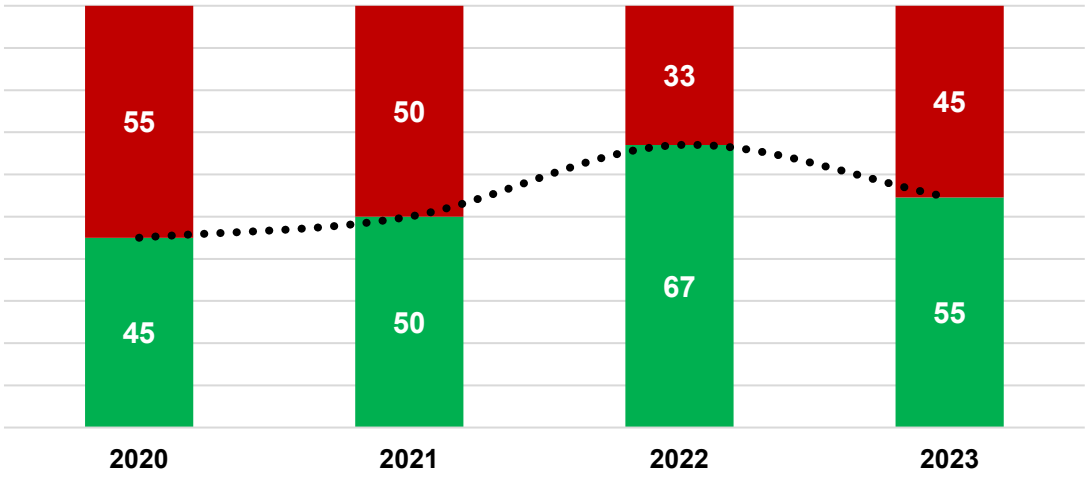
The following case study illustrates a common weakness in IT operations.

Case study 9: Supply chain risks

An entity's service agreement did not include information and cyber security requirements for the vendor to comply. Security expectations should be clearly documented in third-party agreements to reduce supply chain risk. Vendors may not adequately protect entity information and systems if requirements are not clearly documented in the service agreement. Threat actors will often target vendors to indirectly compromise entities, highlighting the importance of vendors' sound security practices.

8. Physical security

Physical security declined this year with only six of the 11 entities meeting the benchmark in this category, compared with eight of the 12 last year. The decline was due to a deterioration in server room access controls. We assessed if entities had controls to protect IT infrastructure from unauthorised access, deliberate damage and environmental hazards such as heat, fire and humidity (Figure 21).



Source: OAG

Figure 20: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 21: Key physical security controls

Common weaknesses included:

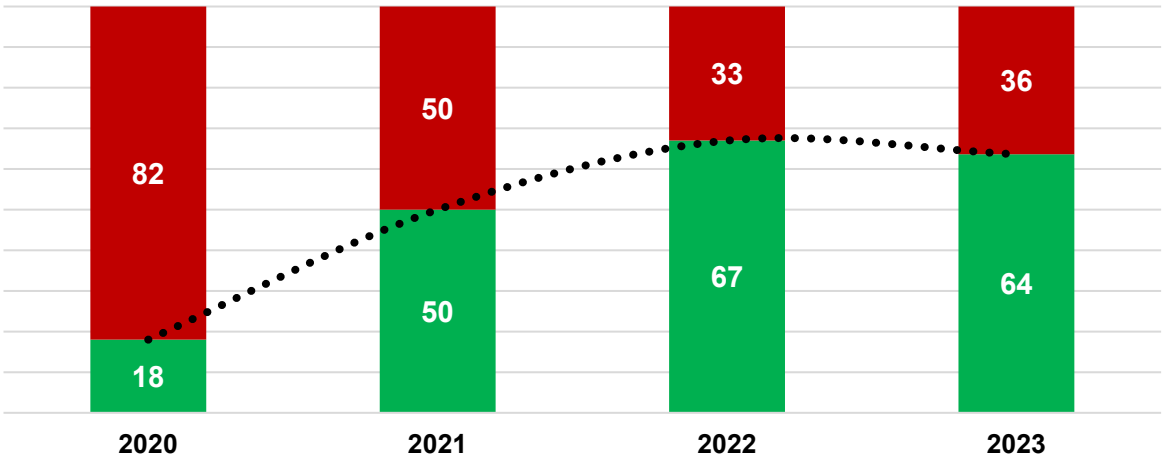
- **Access to equipment enclosures/rooms was not controlled** – access to equipment enclosures should be authorised, recorded and reviewed to reduce malicious or

unintentional damage to IT equipment. Additional controls may include access alarms or CCTV.

- **Dedicated server rooms were not well maintained** – server rooms need to be clear of unwanted material and cabled tidily to reduce the likelihood of damage to infrastructure.

9. Change management

There was no material change this year. Seven of the 11 entities met the benchmark, compared with eight of the 12 last year. Well managed change control processes reduce the likelihood of disruptions (Figure 23).



Source: OAG

Figure 22: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 23: Change management controls

A common weakness was:

- **Change management processes were not documented or not followed** – this increases the chance of errors or delays when implementing changes and the likelihood of disruptions and outages.

The following case study illustrates a common weakness in change management.

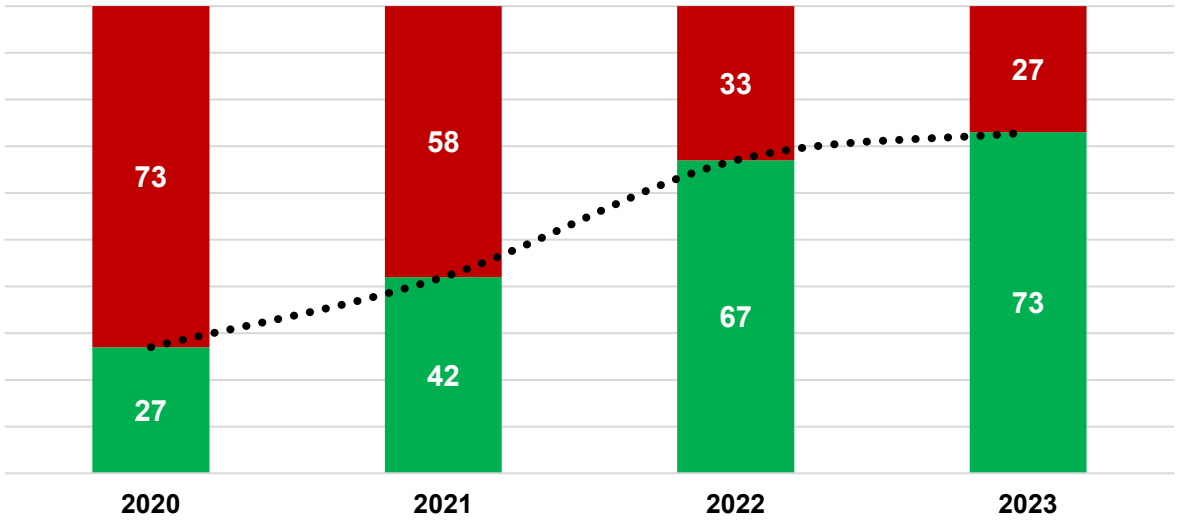
Case study 10: Changes were not appropriately assessed

At one entity, we found staff could approve their own change request. In some instances, the changes were poorly documented and lacked an impact and risk assessment. These

weaknesses increase the likelihood that changes will adversely impact the entity's operations.

10. Risk management

There was no material change this year. Eight of the 11 entities met the benchmark, compared with eight of the 12 last year. A fit-for-purpose risk management process helps entities prioritise information and cyber security risks.



Source: OAG

Figure 24: Percentage of entities that met/did not meet the benchmark

We reviewed risk management policies and processes and if they considered key cyber risks, threats and vulnerabilities (Figure 25).

Source: OAG

Figure 25: Risk management controls

Common weaknesses included:

- **IT risk registers not in place or not maintained** – IT risks may not be effectively managed without adequate documentation.
- **IT risks not reviewed –** timely review of risks is important to ensure mitigation strategies are cost efficient and operate effectively.

Recommendations

1. **Access management**

   To ensure only authorised individuals have access, entities should:

   a. implement effective access management processes

   b. regularly review active user accounts

   c. enforce strong passphrases/passwords and phishing-resistant multi-factor authentication

   d. limit and control administrator privileges

   e. implement automated access monitoring processes to detect malicious activity.

2. **Endpoint security**

   Entities should:

   a. implement effective controls against malware

   b. promptly identify and address known vulnerabilities

   c. control installation of software on workstations, servers and mobile devices

   d. prevent unapproved applications and macros from executing

   e. enforce minimum baseline controls for personal or third-party devices connecting to their systems

   f. implement controls to prevent impersonations and detect/prevent phishing emails

   g. review and harden server and workstation configurations.

3. **Human resources security**

   Entities should ensure that:

   a. pre-employment screening is conducted for key positions

   b. confidentiality/non-disclosure requirements are in place and understood by individuals

   c. termination procedures are in place and followed to ensure timely access cancellation and return of assets

   d. ongoing security awareness training programs are in place and completed by all staff.

4. **Network security**

   Entities should:

   a. implement secure administration processes for network devices

   b. regularly review their network security controls through penetration tests

   c. segregate their network

   d. prevent unauthorised devices from connecting to their network

e. adequately secure wireless networks.

5. Information security framework

Entities should:

a. maintain clear information and cyber security policies and governance structures to oversee and direct IT operations and cyber security

b. conduct regular assessments or gain comfort through assurance reports

c. obtain and review service organisation controls (SOC2) report or equivalent when they use software-as-a-service (SaaS) application for key systems including payroll and finance

d. classify information and implement data loss prevention controls.

6. Business continuity

Entities should maintain up-to-date business continuity, disaster recovery and incident response plans and regularly test them.

7. IT operations

Entities should:

a. implement appropriate IT incident management processes

b. regularly monitor supplier performance

c. perform regular reviews of inventory assets

d. have formal service level agreements with suppliers.

8. Physical security

Entities should:

a. implement effective physical access controls to prevent unauthorised access

b. maintain environmental controls to prevent damage to IT infrastructure arising from heat, moisture, fire and other hazards

c. gain assurance that third-party providers manage their data centres appropriately.

9. Change management

Entities should:

a. consistently apply change control processes when making changes to their IT systems

b. assess and test changes before implementation to minimise errors

c. maintain change control documentation

d. implement controls to detect unauthorised changes.

10. Risk management

Entities should:

a. understand their information assets and apply controls based on their value

b. ensure IT, information and cyber security risks are identified, assessed and treated within appropriate timeframes

c. provide executive oversight and remain vigilant against the risks of internal and external threats.

In accordance with section 7.12A of the *Local Government Act 1995*, local government entities should prepare a report on any matters identified as significant in the local government's audit report[9]. The report should be given to the Minister for Local Government within three months of the local government receiving the audit report and published on the local government's website.

[9] An audit report includes the independent auditor's opinion and the auditor's management report (interim and final management letters) as described in regulation 10 of Local Government (Audit) Regulations 1996. Further information on what is an audit report is available on our website (https://audit.wa.gov.au/resources/local-government/faqs/#faq-21828).

Auditor General's 2023-24 reports

Number	Title	Date tabled
16	Local Government 2022-23 – Information Systems Audit Results	27 May 2024
15	State Government Advertising	15 May 2024
14	State Government 2022-23 – Information Systems Audit	12 April 2024
13	Provision of Supplementary Information to the Standing Committee on Estimates and Financial Operations – Opinions on Ministerial Notifications	5 April 2024
12	Digital Identity and Access Management – Better Practice Guide	28 March 2024
11	Funding for Community Sport and Recreation	21 March 2024
10	State Government 2022-23 – Financial Audit Results	20 December 2023
9	Implementation of the Essential Eight Cyber Security Controls	6 December 2023
8	Electricity Generation and Retail Corporation (Synergy)	8 November 2023
7	Management of the Road Trauma Trust Account	17 October 2023
6	2023 Transparency Report: Major Projects	2 October 2023
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Local Government 2021-22 – Financial Audit Results	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

Office of the Auditor General
for Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General
for Western Australia