



Report 14: 2023-24 | 12 April 2024

INFORMATION SYSTEMS AUDIT

State Government 2022-23



Office of the Auditor General for Western Australia

Audit team:

Aloha Morrissey
Kamran Aslam
Svetla Alphonso
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.

© 2024 Office of the Auditor General Western Australia.
All rights reserved. If acknowledged, this material may be reproduced in whole or in part.

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.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**State Government 2022-23 – Information
Systems Audit**

Report 14: 2023-24
12 April 2024

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

STATE GOVERNMENT 2022-23 – INFORMATION SYSTEMS AUDIT

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 the 16th year we have reported on State government entities' general computer controls.

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

A handwritten signature in grey ink that reads "S. Labuschagne".

Sandra Labuschagne
Acting Auditor General
12 April 2024

Contents

- Auditor General’s overview..... 5
- 2022-23 at a glance 6
 - Introduction8
 - Conclusion10
- What we found: General computer controls..... 11
- What we found: Capability assessments 12
 - Information and cyber security14
 - 1. Endpoint security15
 - 2. Access management.....17
 - 3. Human resource security19
 - 4. Network security20
 - 5. Information security framework21
 - 6. Business continuity21
 - 7. IT operations23
 - 8. Physical security24
 - 9. Risk management25
 - 10. Change management26
- Recommendations..... 28

Auditor General's overview

This report summarises the results of the 2022-23 annual cycle of information systems audits for Western Australian State government entities and tertiary institutions. These audits were conducted between February 2023 and March 2024.



WA public sector entities continue to transform and innovate their information systems to better deliver important services to the public. In doing so entities face many challenges, in particular a shortage of skilled cyber security professionals, and the need to ensure systems remain secure while being improved. Our general computer controls (GCC) audits assess if entities have appropriate controls to protect the confidentiality, integrity and availability of key business systems.

I am pleased to report a decrease in qualified financial audit controls opinions related to GCC weaknesses. While this is a commendable effort, entities need to act more quickly to address known issues. Over half of this year's audit findings were unresolved from the prior year. It is crucial that entities address these long-standing audit findings to improve their information and cyber security controls.

This report is the second with our updated capability maturity model, which provides Parliament with a more detailed view of information and cyber control areas. Our assessments found these areas need the most work, with the poorest results found in endpoint security, access management and human resource security.

To help the sector, my Office has recently published a better practice guide¹ to improve digital identity and access management practices. In 2022-23, we also published our assessment of 10 State entities' progress towards implementing the Essential Eight² cyber security controls, a requirement of the *WA Government Cyber Security Policy*. Effective implementation of these controls will strengthen entities' general computer controls and help them address audit findings.

Common to the entities we recognise as better performing is the constant executive level vigilance and focus required to address cyber risks. This focus is achievable by many more entities.

¹ Office of the Auditor General, [Digital Identity and Access Management – Better Practice Guide](#), OAG, Perth, 28 March 2024.

² Office of the Auditor General, [Implementation of the Essential Eight Cyber Security Controls](#), OAG, Perth, 6 December 2023.

2022-23 at a glance

Auditing State government entities

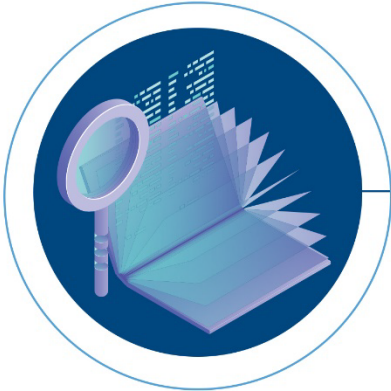


560
general computer
controls findings at
58 entities



39
capability maturity
assessments

Key insights: improvements needed



55% of weaknesses
were unresolved issues from
previous years



8 entities received a
qualified financial audit controls
opinion for significant and
pervasive control weaknesses



Key insights: good practice entities



9 entities
met benchmark in 8 out of 10 categories

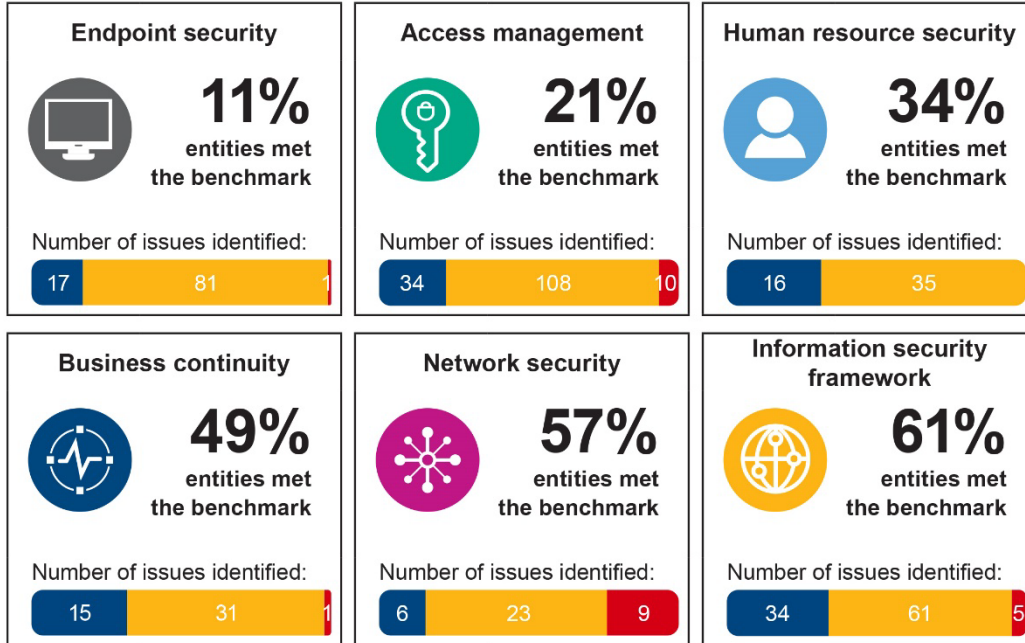
Capability maturity assessments

Need improvement

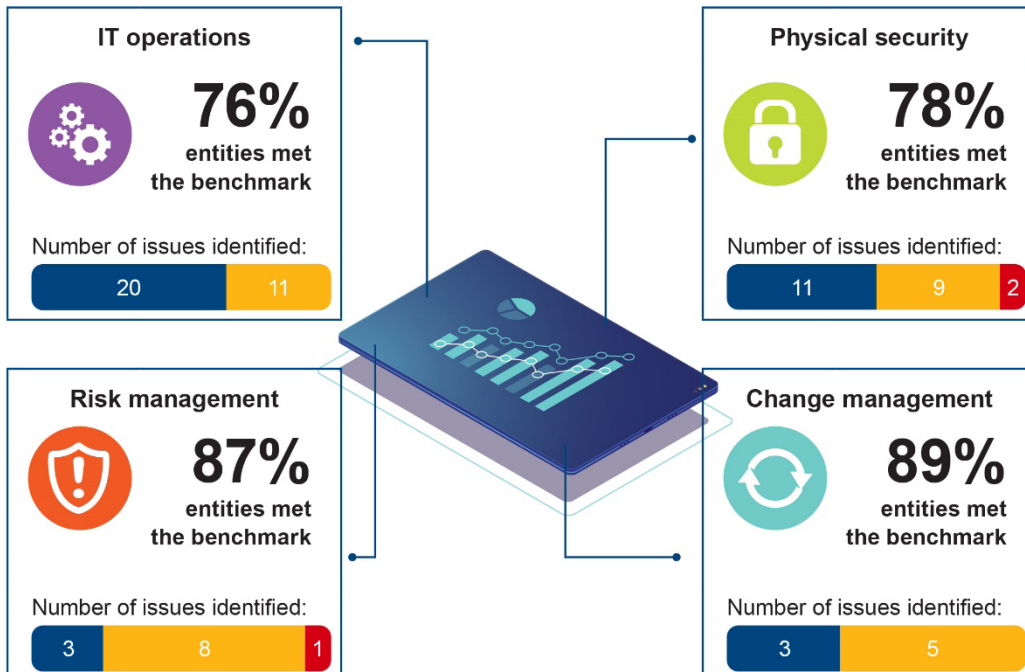
● Minor

● Moderate

● Significant



Better performing



Introduction

This is our 16th report on audits of State government entities' general computer controls (GCC). The objective of our GCC audits is to determine if entities' computer controls effectively support financial processes, delivery of key services, and the confidentiality, integrity and availability of information systems. Strong and well operating controls are a crucial defence to ever increasing cyber threats, enabling entities to safeguard their data, systems and information technology (IT) environments from potential security breaches.

We reported GCC findings to 58 State government entities (Table 1) in 2022-23, and also provided 39 of these 58 entities with capability maturity self-assessments. These assessments look at how well-developed and capable entities' established IT controls are. We then compared entity self-assessments with results from our GCC audits.

Generally, smaller entities or entities audited by our contract audit firms were not provided a capability self-assessment.

39 entities issued with GCC findings and capability assessments		
<ul style="list-style-type: none"> • Central Regional TAFE • Child and Adolescent Health Services • Commissioner of Main Roads • Corruption and Crime Commission • Curtin University • Department of Biodiversity, Conservation and Attractions • Department of Communities • Department of Education • Department of Finance • Department of Justice • Department of Local Government, Sport and Cultural Industries • Department of Planning, Lands and Heritage • Department of Primary Industries and Regional Development 	<ul style="list-style-type: none"> • Department of the Premier and Cabinet • Department of Training and Workforce Development • Department of Transport • Department of Treasury • Department of Water and Environmental Regulation • Disability Services Commission • East Metropolitan Health Service • Edith Cowan University • Health Support Services • Housing Authority • Lotteries Commission (Lotterywest) • Murdoch University • North Metropolitan Health Service 	<ul style="list-style-type: none"> • North Metropolitan TAFE • North Regional TAFE • PathWest Laboratory Medicine WA • Racing and Wagering Western Australia • Rottnest Island Authority • South Metropolitan Health Service • South Metropolitan TAFE • South Regional TAFE • Southern Ports Authority • University of Western Australia • WA Country Health Service • WA Police Service • Western Australian Land Information Authority (Landgate)
19 entities issued with GCC findings only		
<ul style="list-style-type: none"> • Building and Construction Industry Training Board • Botanic Gardens and Parks Authority 	<ul style="list-style-type: none"> • Forest Products Commission • Fremantle Port Authority • Gold Corporation • Mental Health Commission 	<ul style="list-style-type: none"> • Regional Power Corporation (Horizon Power) • Water Corporation

<ul style="list-style-type: none"> • Department of Fire and Emergency Services • Department of Jobs, Tourism, Science and Innovation • Electricity Generation and Retail Corporation (Synergy) • Electricity Networks Corporation (Western Power) 	<ul style="list-style-type: none"> • Office of the Information Commissioner • Parliamentary Services Department • Pilbara Ports Authority • Public Transport Authority of Western Australia 	<ul style="list-style-type: none"> • WA Greyhound Racing Association • Western Australian Land Authority • Zoological Parks Authority
---	---	--

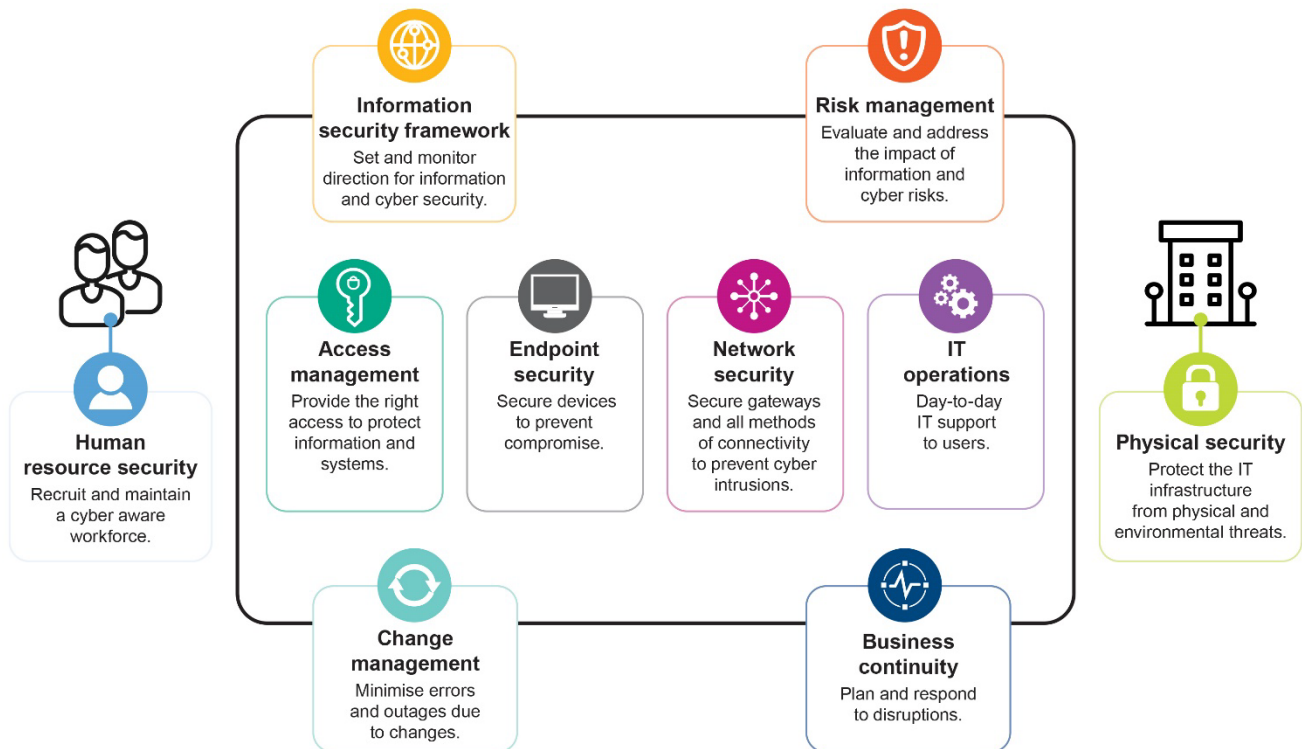
Source: OAG

Table 1: State government entities issued GCC findings

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

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

We focused on the following 10 categories:



Source: OAG

Figure 1: GCC categories

Conclusion

We issued 560 GCC findings to 58 entities this year, compared to 566 findings to 61 entities last year. Entities need to actively address these findings in a climate of increasing cyber-attacks, breaches and information system related outages.

Pleasingly, a number of entities had addressed significant GCC audit findings from prior years resulting in a decreased number of qualified financial audit controls opinions³ related to GCC, down to eight from 13. While this is positive, entities need to do more as over half of this year's findings (55%) were issues still unresolved from the prior year. Not addressing weaknesses in a timely manner leaves entities vulnerable to compromise and data breaches.

The results of our capability maturity assessments show endpoint security was the weakest area, with only 11% of the entities meeting the benchmark. This was followed by access management (21%), human resource security (34%), and business continuity (49%). While more than half of the entities met the benchmark for network security, 24% of the findings in this category were significant and pervasive, a 3% increase compared to last year.

There was a minor decline in the areas of information security framework and IT operations, while results for IT risk management remained the same. Physical security and change management saw improvements this year.

³ Office of the Auditor General, [State Government 2022-23 – Financial Audit Results](#), OAG, Perth, 20 December 2023.

What we found: General computer controls

In 2022-23, we alerted 58 entities to 560 information system weaknesses: 29 were rated significant, 372 moderate and 159 minor.

Significant findings were mainly in the areas of access management and network security. The majority of the weaknesses were rated moderate (Figure 2), which require entities to take action as soon as possible. Combinations of moderate findings can expose entities to more serious risks, so it is important to address the issues promptly.

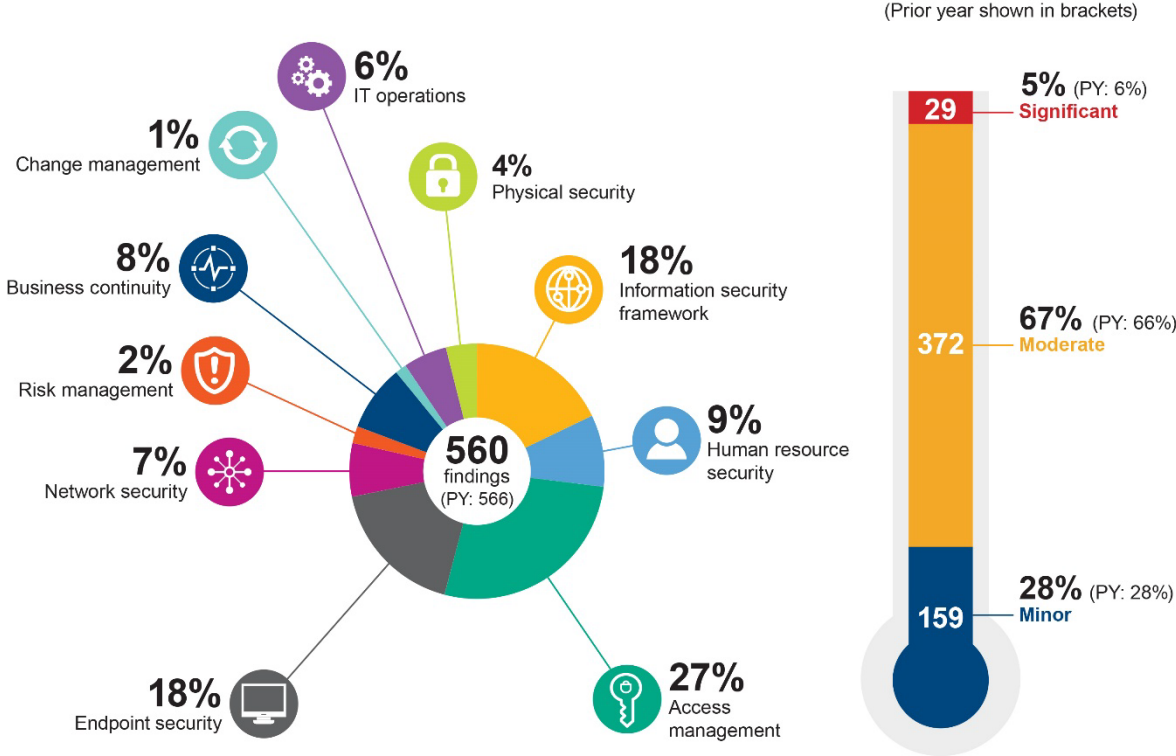
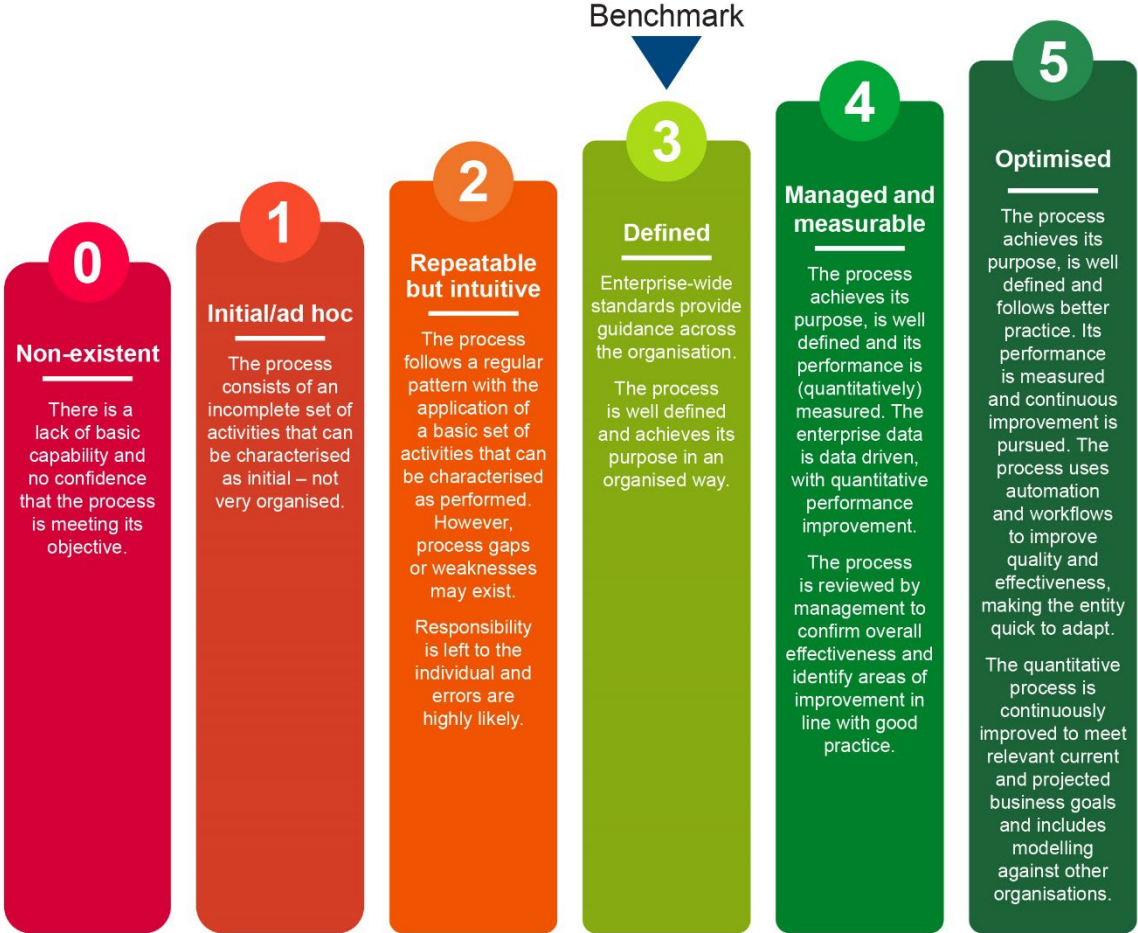


Figure 2: GCC findings and ratings in each control category

Source: OAG

What we found: Capability assessments

We conducted capability assessments at 39 State government entities. The assessments evaluated each entity’s capability maturity level across the 10 GCC categories using a 0-5 rating scale⁴ (Figure 3). Entities need to achieve a level 3 (Defined) rating or better in each category to reach benchmark.

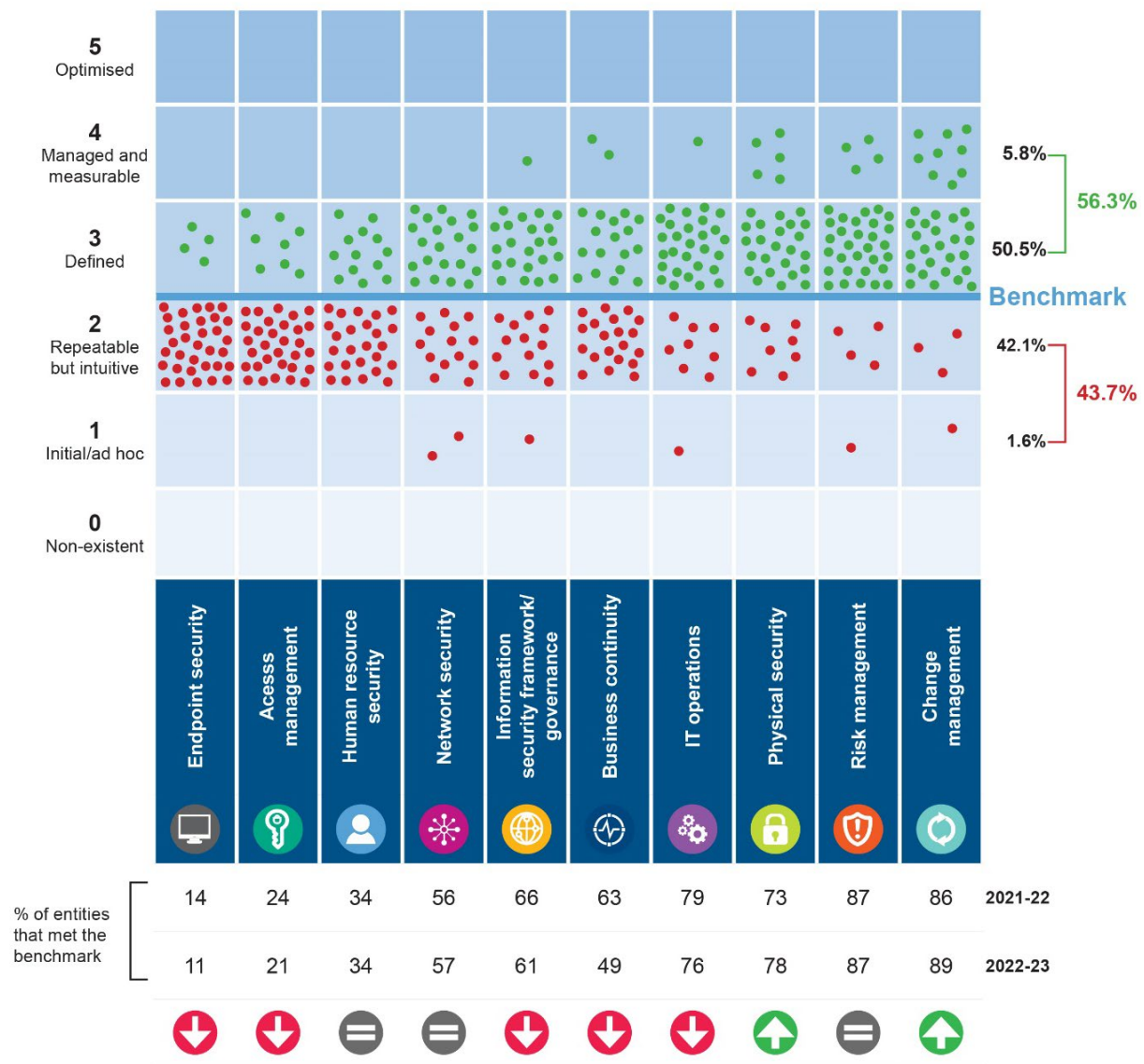


Source: OAG

Figure 3: Rating scale and criteria

⁴ 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 assessments across the 10 control categories. Not all entities were assessed across all 10 categories.



Source: OAG

Figure 4: Capability maturity model assessment results

Endpoint security, access management and human resource security continue to be areas requiring the most attention. There was a decline in the maturity of business continuity processes due to a number of entities failing to test and keep up-to-date their continuity plans, backup procedures, and incident response plans. In addition, while more than half of the entities met the benchmark for network security, 24% of weaknesses in this area were rated as significant and high risk.

The remaining categories did not see a material change. Risk management remained the same, change management and physical security improved slightly and information security framework and IT operations saw a marginal decline.

Over the last five years, four entities issued with capability assessment have consistently met the benchmark in a majority of categories:

- Department of Training and Workforce Development

- North Metropolitan TAFE
- Racing and Wagering Western Australia
- Western Australian Land Information Authority (Landgate).

In addition, the following entities met the benchmark in at least eight of the 10 categories in 2022-23:

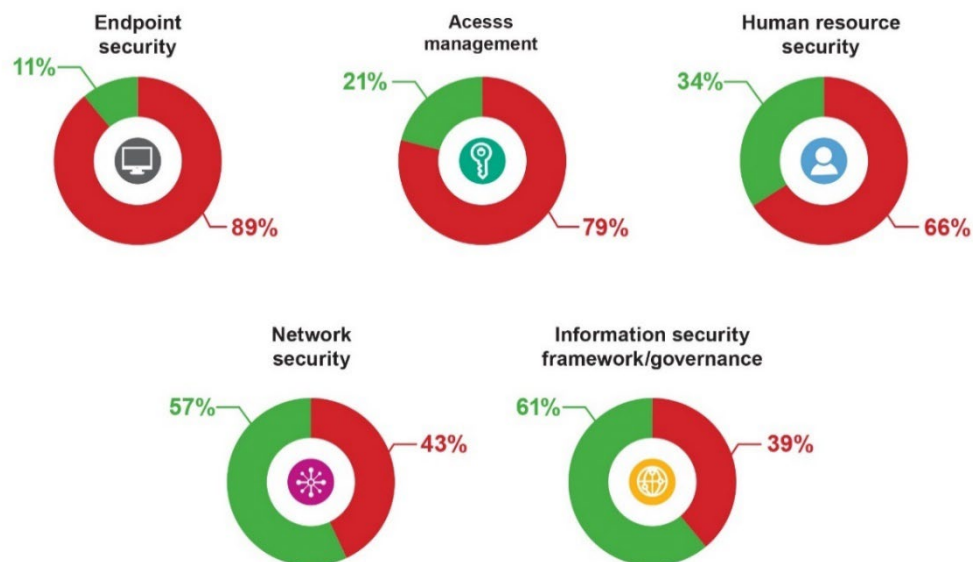
- Department of Biodiversity, Conservation and Attractions
- Department of Planning, Lands and Heritage
- Lotteries Commission
- South Metropolitan TAFE
- Department of Water and Environmental Regulation.

Information and cyber security

In 2021-22, significant information and cyber security weaknesses resulted in 13 entities receiving qualified financial audit controls opinions. In 2022-23 we found a number of those entities had addressed significant issues, resulting in fewer qualified controls opinions.⁵

While this shows positive results, our 2022-23 findings continue to highlight information and cyber security as a heightened area of focus (Figure 5). Entities need to take proactive measures to address weaknesses in these areas.

Information and cyber security controls testing are essential to our GCC audits. We assess whether entities have effective controls to protect their information systems and IT environments from internal and external threats. These control categories include endpoint security, access management, human resource security, network security and information security frameworks. Results for these categories only include two years of data, as they were reported separately for the first-time in 2021-22.



Source: OAG

Figure 5: Percentage of entities that met/did not meet the benchmark in the five categories for information and cyber security in 2022-23

⁵ Office of the Auditor General, [State Government 2022-23 – Financial Audit Results](#), OAG, Perth, 20 December 2023.

As part of our GCC audits, we also assessed controls of 10 entities against the Australian Signals Directorate’s Essential Eight criteria.⁶ We found entities did not have an adequate understanding of their controls and needed more work to achieve the level one maturity required by the *WA Government Cyber Security Policy*.⁷

Implementing Essential Eight controls effectively will also help address shortcomings identified in GCC audits in the information and cyber security area. Essential Eight controls are designed to help entities manage and address common cyber security risks and improve their information and cyber security posture.

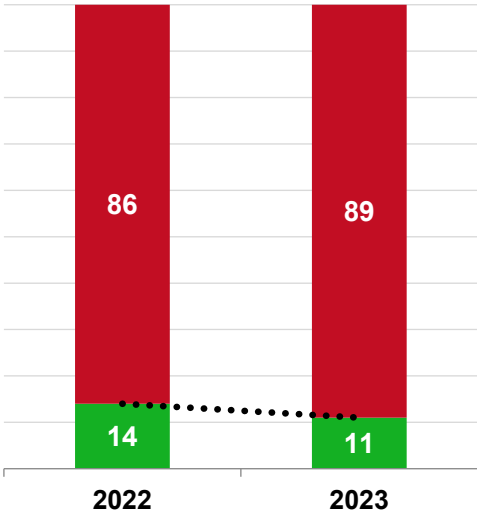
1. Endpoint security

Like last year, results for the endpoint security category continue to be the weakest. Only 11% of entities met the benchmark, down from 14% last year (Figure 6). Weaknesses in endpoint security leave entities more exposed to potential attacks that could compromise their information and operations.

Endpoint security plays a crucial role in ensuring devices (e.g. computers, servers, phones) accessing network and business applications are protected.









We reviewed if entities had anti-malware controls including application and macro controls to prevent the execution of unauthorised applications and code.

Our testing also covered email authentication controls, and whether entities promptly identified and patched vulnerabilities. Where entities allow remote access through personal devices, we examined if they assessed the security posture of these devices before allowing access.



Source: OAG

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

	Malware protection		Patch operating systems		Removable media control
	Patch applications		Application hardening		Email security
	Vulnerability management		Database management		

Source: OAG

Figure 7: Endpoint security controls included in our GCC audits

⁶ Office of the Auditor General, [Implementation of the Essential Eight Cyber Security Controls](#), OAG, Perth, 6 December 2023.

⁷ Department of the Premier and Cabinet, [WA Government Cyber Security Policy](#), DPC, Perth, October 2021.

Common weaknesses included:

- **Ineffective vulnerability management processes** – instances where vulnerability scanning is either not in place or not adequately configured. A high number of vulnerabilities were also present due to unsupported or unpatched systems.
- **Applications controls were not in place** – if unapproved applications are not blocked, malware infections can compromise an entity's network and systems.
- **Untrusted code was not blocked** – malicious code can spread malware infections leading to security breaches.
- **Email systems were not adequately configured** – lack of controls or misconfigurations can result in impersonation and data breaches. Domain-based Message Authentication Reporting and Conformance (DMARC) is not fully enabled to prevent impersonation.
- **Missing or out-of-date anti-malware software** – malware can spread without adequate controls.

The following case studies illustrate the common weaknesses we found in endpoint security.

Case study 1: Ineffective application control

An entity was unaware it had poorly configured its application control software, which rendered the control ineffective, as it had not reviewed the control in the last five years. As a result, we identified a significant number of unapproved applications installed on the entity's network.

Case study 2: Entity did not understand extent of vulnerabilities

An entity did not have a full understanding of vulnerabilities affecting its systems and network. While it performed regular vulnerability scans, these were misconfigured and did not identify all weaknesses. Without being fully informed, the entity cannot address the weaknesses.

Entities need an effective process for identifying, assessing and addressing relevant vulnerabilities in a timely manner, to adequately protect systems against potential threats.

2. Access management

Access management remains an area of concern with only 21% of entities meeting the benchmark compared to 24% in 2021-22 (Figure 8). Inadequate access controls can result in security incidents, financial loss and reputational damage.

In this area, we assess controls such as access rights, active user accounts, generic/shared credentials, privileged access, password policies and multi-factor authentication.

To help the sector improve access management, we have developed and published a better practice guide⁸ focusing on principles to protect information assets from unauthorised access. We encourage all public sector entities to adopt the principles in this guide.



User account management



Limit admin access



Database access



Strong passwords/passphrases



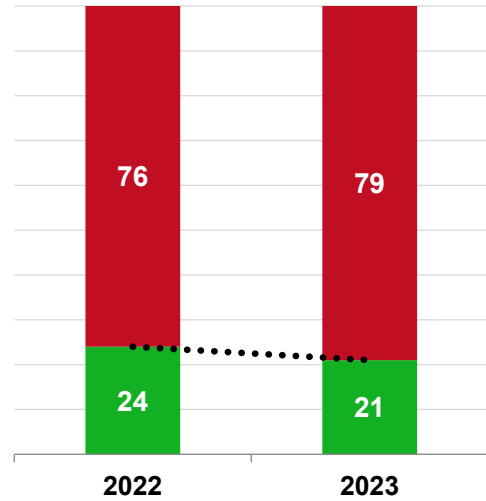
Monitoring



Segregation of duties



Multi-factor authentication



Source: OAG

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

Source: OAG

Figure 9: Access management controls included in our GCC audits

Common weaknesses included:

- **Multi-factor authentication (MFA) was not used or was not adequate** – a lack of phishing resistant MFA can lead to unauthorised access.
- **Access termination process was inadequate** – if access of former staff is not disabled in a timely fashion it could be used for unauthorised or inappropriate access.
- **Access privileges were not regularly reviewed** – appropriately managed access privileges reduce the risk of unintentional or intentional misuse of access.
- **Ineffective system logging and monitoring** – malicious activity may go unnoticed if system access monitoring is not effective.
- **Inadequate access provisioning process** – if access is granted without following a formal process, there is a heightened risk of unauthorised access and individuals accumulating unnecessary privileges.

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

These common weaknesses are further highlighted in the following case studies.

Case study 3: Managing privileged system accounts for data protection

An entity relies on a third-party vendor to maintain its key application, which stores personal and sensitive information. The third-party vendor received highly privileged access to the application through a generic account, which could also be used to view sensitive information. Despite the vendor's highly privileged access, the entity did not monitor the vendor's activity and use of the generic account to identify any inappropriate access to personal and sensitive information.

It is also difficult to determine accountability if generic accounts are misused.

Case study 4: Neglecting good password practices

An entity stores the credentials of a highly privileged generic account in clear text in a user manual. Additionally, the password was short, simple and easy to guess.

Poor password management practices could result in account compromise and unauthorised access.

Case study 5: Excessive users given administrator rights

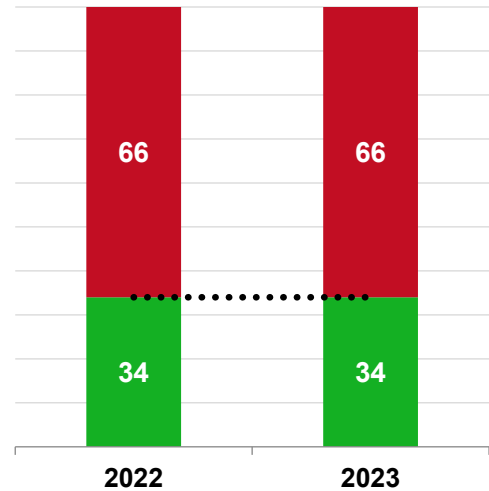
At an entity, all users were automatically granted local administrator privileges to all workstations and could install software at their own discretion. We identified a number of potentially unwanted applications, including games, installed on the devices.

Excessive privileges and a lack of controls to prevent unwanted software installation may introduce malware to the entity's network.

3. Human resource security

Similar to last year, only 34% of the entities met the benchmark in human resource (HR) security (Figure 10). Staff and contractors may not fully understand their information security responsibilities, and insider threats may go undetected, leading to information theft and other security incidents.

Appropriate procedures for onboarding and offboarding, pre-employment screening, ongoing security awareness training, proper disciplinary processes and adequate termination procedures can protect against insider threats and security breaches.



Source: OAG

Figure 10: Percentage of entities that met/did not meet the benchmark for human resource security



Background checks



Acceptable use policies



Confidentiality agreements



Security awareness programs

Source: OAG

Figure 11: Human resource security controls included in our GCC audits

Common weaknesses included:

- **Background screening not performed** – if background checks are not performed, there is an increased risk of fraud and malicious activities occurring.
- **Onboarding processes lacked IT acceptable use and non-disclosure agreements** – there is a heightened risk of misuse and inappropriate actions when individuals are not made aware of their responsibilities.
- **Information security awareness training was not provided or not completed** – training helps individuals understand the risks to the entity and their personal responsibilities for information and cyber security.
- **No visibility of contractors** – insufficient visibility over contractors through a central record can lead to undetected unauthorised activities, posing significant security risk.
- **Employee termination processes not consistently followed** – this may result in delays to disabling access resulting in unauthorised access to entity premises, information and systems, and potentially financial loss.

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

Case study 6: Insufficient cyber security awareness

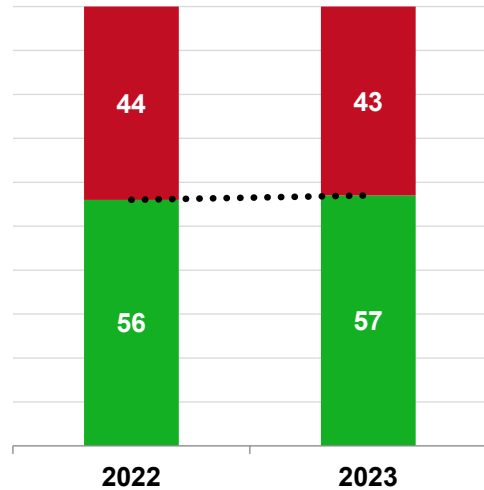
At an entity, under 10% of staff completed cyber security training.

With limited access to training and completion of training resources, not all staff are sufficiently trained in basic cyber security. This may result in inappropriate actions, which can affect the confidentiality, integrity and availability of information.

4. Network security

There was no material change in this area with 57% percent of the entities meeting the benchmark (Figure 12). Twenty-four percent (21% in 2022) of network security weaknesses were rated as significant. Network security controls play a pivotal role in safeguarding networks and critical systems against cyber intrusions.

We review if entities have secure network administration processes and segregation, prevent unauthorised devices from connecting to the network and performed regular penetration tests.



Source: OAG

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



Source: OAG

Figure 13: Network security controls included in our GCC audits

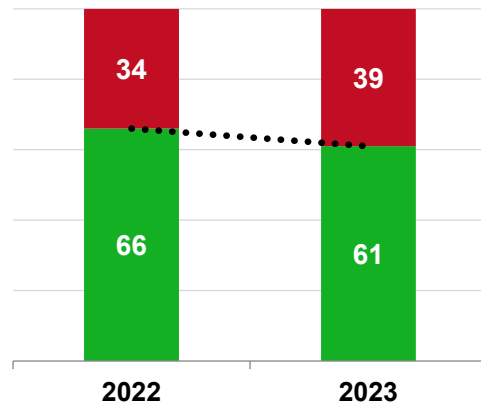
Common weaknesses included:

- **Firewall rules are not reviewed** – outdated firewall rules can increase the risk of compromises.
- **Lack of network segregation** – cyber incidents may spread and be difficult to contain when networks are not segregated. This also isolates and protects critical operational technology assets.
- **Unauthorised devices were not blocked** – unauthorised devices could be used as an attack vector to spread malware or eavesdrop on communications.

5. Information security framework

More than half of the audited entities (61%) met the benchmark in this category, which is slightly fewer than the prior year (Figure 14). Adequate governance and oversight ensure entities mitigate security risks and safeguard sensitive information and key systems.

We assessed whether entities have suitable information security policies and roles, including information classification procedures, as well as established governing committees and communication processes with security groups. We also looked at entities' controls to prevent data loss and security risk assessments for cloud service providers.



Source: OAG

Figure 14: Percentage of entities that met/did not meet the benchmark for information security framework



Source: OAG

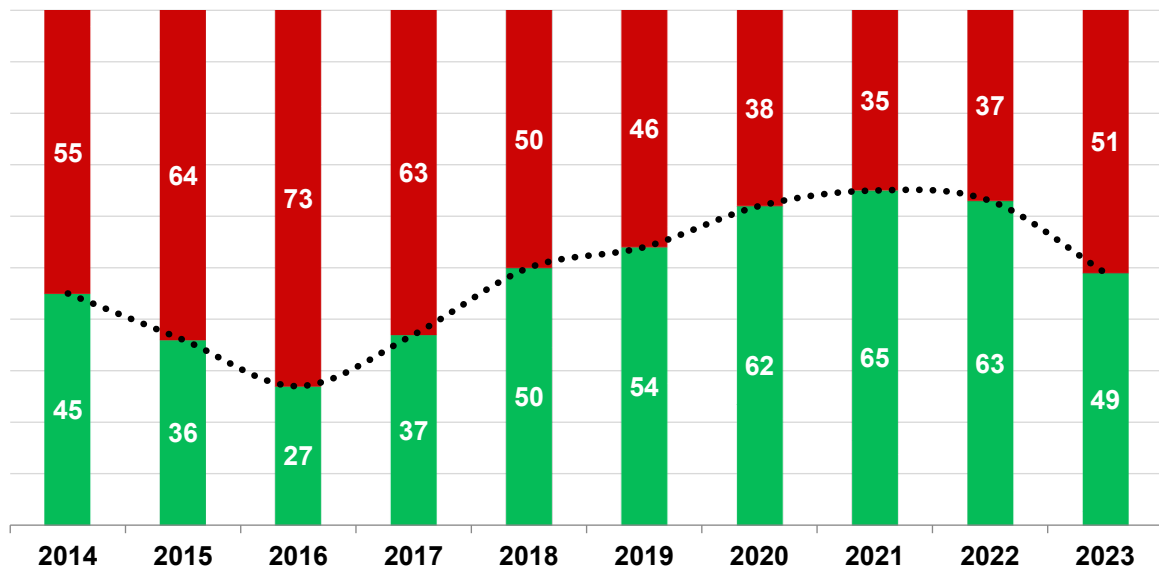
Figure 15: Information security framework controls included in our GCC audits

Common weaknesses included:

- **Information security policies were missing or outdated** – outdated policies, standards and procedures means entities may not be able to achieve their information security objectives.
- **Ineffective cloud security assurance** – services may fail to meet an entity's expectations, rendering the entity vulnerable to security, financial and reputational risks.
- **Data loss prevention controls were insufficient or absent** – data loss may go undetected, potentially resulting in sensitive information leakage and reputational harm.

6. Business continuity

This year, only 49% of entities met the benchmark for business continuity, a substantial decline from last year's 63% and the progress made over the last five years (Figure 16). This is due to entities not maintaining and testing their continuity plans or not taking prompt action to address existing weaknesses. Interruptions to business can seriously impact the delivery of important services to the public. Effective business continuity processes focus on strategies, procedures and plans that help entities operate or quickly resume operations, when a disruption or disaster event occurs.



Source: OAG

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

We assessed if entities have plans for business continuity, disaster recovery, backups and incidents response and if the effectiveness of the plans are regularly tested.



Source: OAG

Figure 17: Business continuity controls included in our GCC audits

Common weaknesses included:

- **Lack of regular backup testing** – insufficient testing of backups could delay restoration of data.
- **Business continuity and disaster recovery plans are not up-to-date** – entities may face longer than expected outages of important services if adequate recovery and continuity plans are not in place and effective.
- **Plans are not tested** – plans may not be fit for purpose unless testing ensures they can be relied upon in emergency. Testing can also identify gaps in recovery plans.

The following case study illustrates a common weakness in continuity planning.

Case study 7: Business continuity management

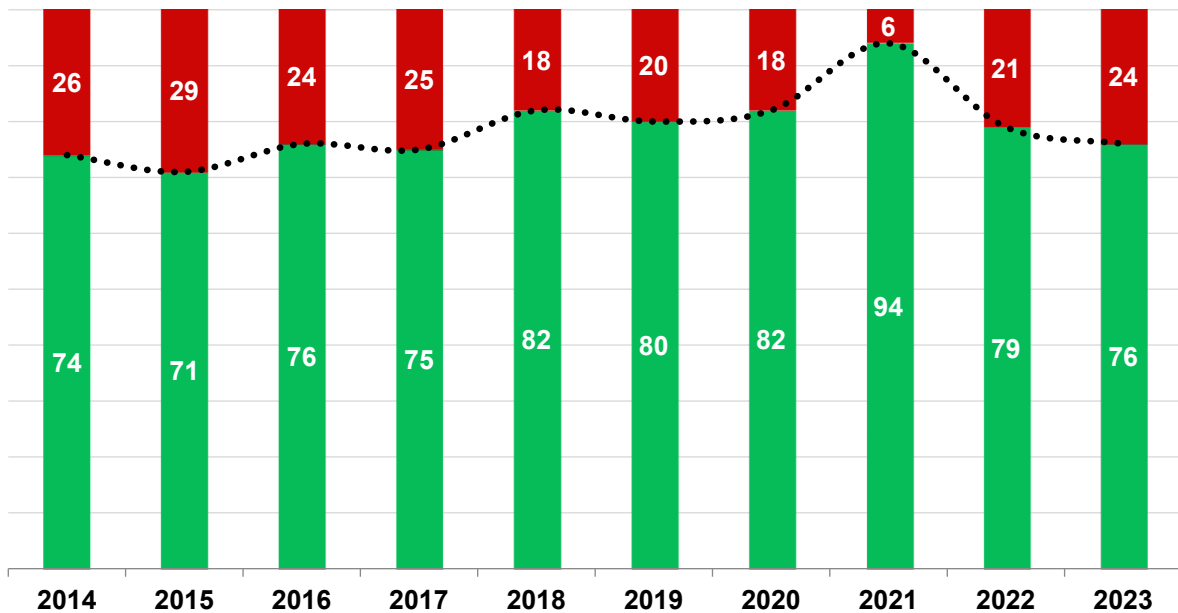
An entity was only backing up its data every 24 hours, with some systems not backed up at all. This was contrary to its recovery requirements defined in the business continuity plan, which allowed a maximum data loss between one to eight hours for critical information.

The entity was also not adequately testing its backups to ensure they can be relied upon for emergency use when necessary.

Without appropriate backup procedures and testing, data may be lost or recovery may take longer than expected.

7. IT operations

Generally, entities perform well in this category, with 76% of entities meeting the benchmark this year (Figure 18). Effective management of IT operations is important to resolve incidents and problems, and maintain IT infrastructure. IT operations is the most customer-centric of the GCC controls, a breakdown in these controls is quickly noticed by entity staff.



Source: OAG

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

We assessed if entities had formal incident management processes, managed supplier contracts and performance, and IT assets.



IT assets lifecycle management



Supplier performance management



Incident and problem management

Source: OAG

Figure 19: IT operational controls included in our GCC audits

Common weaknesses included:

- **IT asset management records are not appropriately maintained** – inadequate IT asset management procedures could result in misplaced, lost or stolen IT assets, potentially resulting in financial losses and reputational damage.
- **Missing or inadequate supplier performance monitoring** – lack of supplier monitoring may lead to substandard services, potentially compromising systems integrity and impacting service delivery.
- **Service level agreements not in place** – service delivery may not be delivered as per expectations if entities and vendors do not have a clear understanding of their obligations.

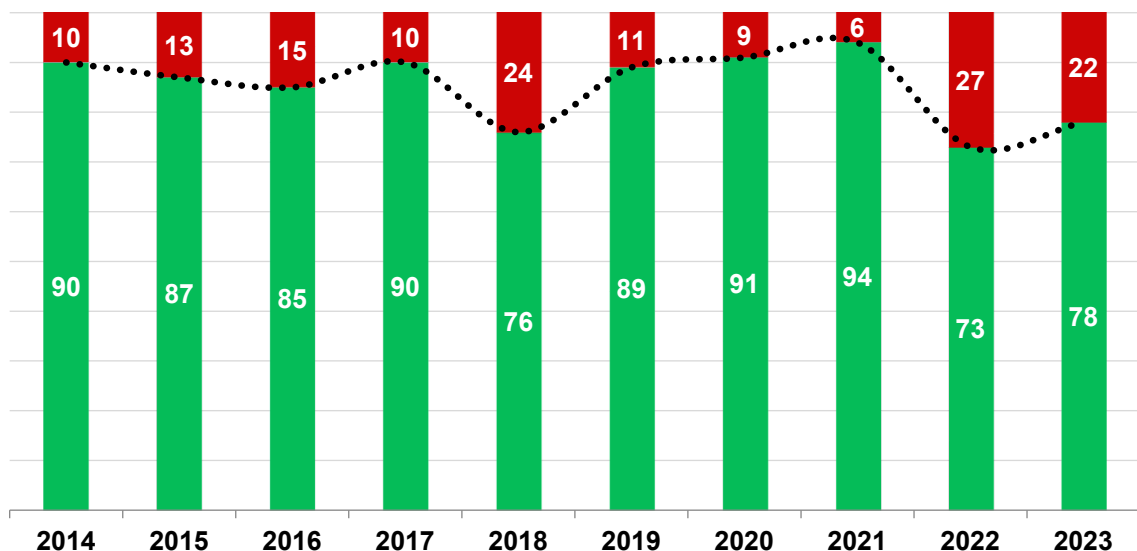
Case study 8: IT assets were not accurately recorded

At one entity, we found hundreds of unused devices awaiting secure destruction as the disposal process had not taken place in over two years.

There is an increased risk that IT assets will be lost or stolen resulting in financial, informational and reputational loss.

8. Physical security

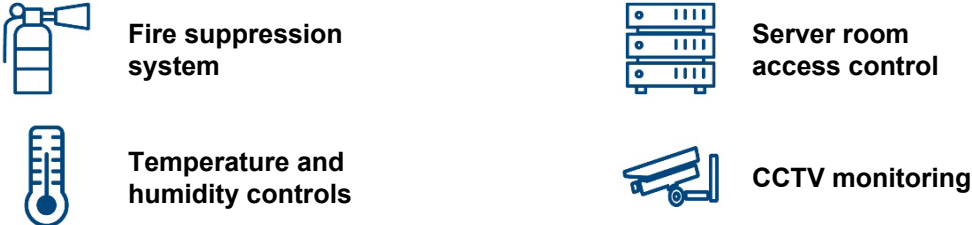
There was a slight improvement in this area, with 78% of entities meeting the benchmark in 2022-23 compared to 73% in 2021-22. However, these results are still lower than many in the recent years (Figure 20). Whether server rooms are on-premises or managed through a third-party vendor, it is important to maintain secure access and environmental controls to prevent accidental damage, mitigate intentional harm, safeguard equipment and protect sensitive data. Well-designed server rooms with appropriate environmental controls ensure availability of IT infrastructure and systems.



Source: OAG

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

We assessed how entities manage physical access controls, power, fire hazards, and temperature and humidity controls in server rooms. We tested whether entities obtain performance and security reports from third-party vendors managing server rooms or delivering infrastructure as a service.



Source: OAG

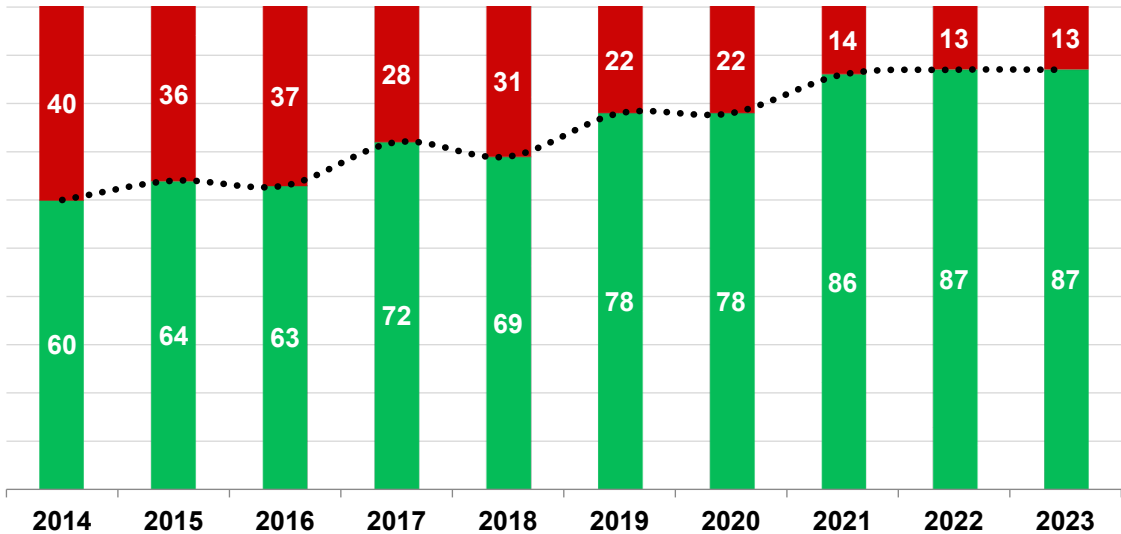
Figure 21: Physical security controls included in our GCC audits

Common weaknesses included:

- **Former staff still had access to server rooms and data centres** – failure to adequately control and restrict access can result in unauthorised or inappropriate entry to key systems and damage to infrastructure.
- **Inadequate data centre management** – storing combustible materials and poor maintenance increase the likelihood of unplanned downtime and can be a health and safety risk.
- **Unsuitable temperature, humidity and fire detection controls** – this can lead to equipment failures, system downtime and reduced performance, affecting service continuity and financial stability.

9. Risk management

Risk management continues to show a consistent positive trend with 87% of entities meeting the benchmark in 2022-23 (Figure 22). A robust risk management process reduces the likelihood and impact of potential threats and enhances overall decision-making.



Source: OAG

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

We reviewed entities' information risk management policies and processes, and if they considered key cyber risks, threats and vulnerabilities.



Source: OAG

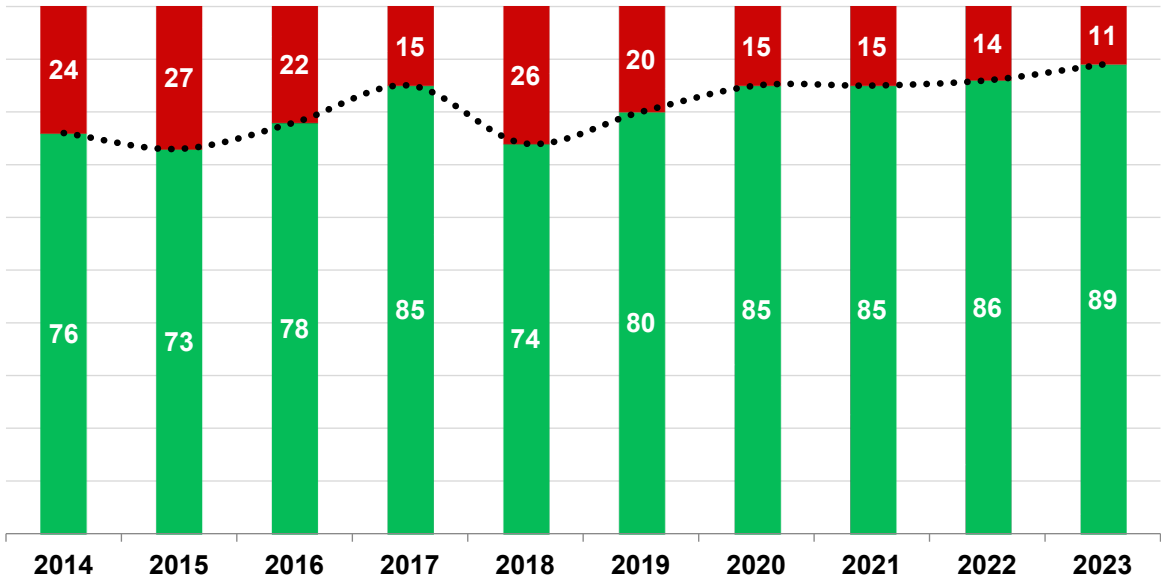
Figure 23: Risk management control included in our GCC audits

Common weaknesses included:

- **Risk management policies not up-to-date** – obsolete policies and procedures could fail to address emerging risks, leaving an entity vulnerable to potential harm.
- **Risk registers are not maintained** – it is crucial to identify and document all relevant risks, including those related to information and cyber security.
- **Inadequate risk management process** - this could lead to incomplete risk analysis and weaken overall risk assessment effectiveness.

10. Change management

There has been continuous improvement in the change management category area over recent years, and we found 89% entities met the benchmark this year (Figure 24).



Source: OAG

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

We examine if entities have processes to authorise and test changes before releasing them to production systems and infrastructure.



Source: OAG

Figure 25: Change management controls included in our GCC audits

Common weaknesses we found included:

- **Change management procedures are not up-to-date or not followed** – errors, delays and failures in implementing changes could occur.
- **Procedures do not cover emergency changes** – emergency changes made to IT systems may result in downtime.

Recommendations

1. Endpoint security

To ensure workstations, servers and mobile devices are protected, 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.

2. Access management

To ensure only authorised individuals and digital identities have access, entities should:

- a. strive for password-less authentication. Where this is not possible, enforce strong passphrases/passwords
- b. implement phishing resistant multi-factor authentication
- c. implement effective access management processes
- d. regularly review active user accounts
- e. limit and control administrator privileges
- f. implement automated access monitoring processes to detect malicious activity.

3. Human resource security

Entities should ensure:

- a. pre-employment screening is conducted for key positions
- b. confidentiality/non-disclosure requirements are in place and understood by individuals
- c. effective termination procedures exist and are 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 perform independent penetration tests to test network security controls
- c. segregate their network, particularly for IT and operational technology systems
- d. prevent unauthorised devices from connecting to their corporate network
- e. adequately secure wireless networks.

5. Information security framework

Entities should:

- a. maintain clear information and cyber security policies and roles in line with the *WA Government Cyber Security Policy*
- b. conduct regular assessments to ensure their IT supply chain is secure
- c. classify information and implement data loss prevention controls
- d. obtain and review service organisation controls (SOC) type 2 or equivalent assurance reports when they use software-as-a service (SaaS) applications for key systems including payroll and finance.

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 and problem management processes
- b. have formal service level agreements with suppliers and regularly monitor supplier performance
- c. perform regular reviews of inventory assets.

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 data centres appropriately.

9. 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.

10. 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 problems
- c. maintain change control documentation
- d. implement controls to detect unauthorised changes.

Auditor General's 2023-24 reports

Number	Title	Date tabled
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