Office of the Auditor General
Serving the Public Interest

Report 17: 2022-23 | 22 March 2023

INFORMATION SYSTEMS AUDIT

State Government 2021-22

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Svetla Alphonso
Information Systems Audit team
Financial Audit teams

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: SquareMotion/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit – State Government 2021-22

Report 17: 2022-23
22 March 2023

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT – STATE GOVERNMENT 2021-22

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 15th year we have separately reported on State government entities' general computer controls.

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

CAROLINE SPENCER
AUDITOR GENERAL
22 March 2023

Contents

Auditor General's overview

This report summarises the results of the 2021-22 annual cycle of information systems audits for Western Australian State government entities (including tertiary institutions). These audits were performed between February 2022 and March 2023.

Last year's significant data breaches across sectors and jurisdictions impacted many Australians and highlighted the critical importance of good information and cyber security controls. Along with the many benefits for the public sector that come from the convergence of IT and operational technology, an increasingly mobile workforce and the use of cloud and IT supply chains, is the ever present and evolving nature of cyber security threats. Our IS audits are designed to help entities remain vigilant in their identification, detection and mitigation of cyber risks. The State Government's $500 million Digital Capability Fund[1] provides further support for entities to upgrade their legacy systems and invest in digital transformation. While the full value of this investment will take many years to realise, the enhancements are essential and it is pleasing that a number of entities have already accessed funding to address some audit findings.

We reported 566 general computer control findings to 61 entities for 2021-22. Concerningly, and similar to last year, half of the audit findings (282) were unresolved issues from 2020-21. At 13 entities, control weaknesses were so pervasive they resulted in qualified audit opinions – a serious matter – due to weak system access management, and network security controls. These findings, if not addressed, could result in data breaches, system outages and financial loss to the State and its citizens.

In recognition of growing cyber security threats, during this audit cycle we introduced an updated capability maturity model. The updated model expands the number of control categories to 10, five of which now relate to information and cyber security controls. The model provides more information to entities and the Parliament on the discrete state of system, information and cyber security in the State public sector, and what needs to be done to improve it.

In 2021-22 over half of the entities failed to meet the benchmark for endpoint security, access management and human resource security. In the category of network security more than half the entities met the benchmark, but a number of findings were significant and high risk. We also saw a drop in physical security after a 10-year period of increased stability.

As always, I am grateful to my skilled and dedicated Information Systems Audit team. I also acknowledge the hard work being done by staff and leaders across State government, including the Office of Digital Government, to ensure the delivery of public services is supported by efficient, effective, reliable and secure information systems.

[1] Department of the Premier and Cabinet, 'The Digital Capability Fund', *WA.gov.au*, 29 September 2022, accessed 20 March 2023.

2021-22 information systems audits at a glance

Auditing State government entities

61 entities' general computer control findings are included in this report

39 audits included capability maturity assessments.

10 control categories assessed in the updated capability maturity model

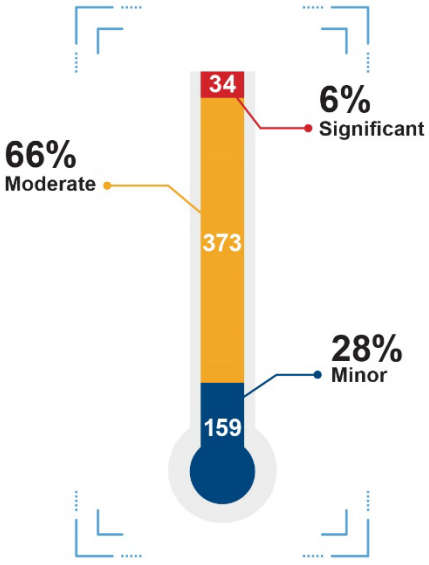
15th year reporting on the results of State government entities' general computer controls

Audit results

566 **information systems control weaknesses** (page 11)

282 (50%) weaknesses were unresolved issues from previous years

13 entities had control weaknesses that were so significant and pervasive they received a qualified financial audit controls opinion



Information security framework

66%

entities met the benchmark
(page 22)

Number of issues identified:

Risk management

87%

entities met the benchmark
(page 28)

Number of issues identified:

Human resource security

34%

entities met the benchmark
(page 19)

Number of issues identified:

Business continuity

63%

entities met the benchmark
(page 23)

Number of issues identified:

Access management

24%

entities met the benchmark
(page 17)

Number of issues identified:

Change management

86%

entities met the benchmark
(page 27)

Number of issues identified:

Endpoint security

14%

entities met the benchmark
(page 16)

Number of issues identified:

IT operations

79%

entities met the benchmark
(page 26)

Number of issues identified:

Network security

56%

entities met the benchmark
(page 20)

Number of issues identified:

Physical security

73%

entities met the benchmark
(page 24)

Number of issues identified:

Minor Moderate Significant

Introduction

This is our 15th report on the audits of State government entities' general computer controls (GCC). The objective of our GCC audits is to determine if entities' computer controls effectively support preparation of financial statements, delivery of key services and the confidentiality, integrity and availability of information systems. Cyber criminals target organisations of all sizes and nature. Well operating controls help entities protect their information systems and IT environments from data breaches and cyber security threats.

For 2021-22, we reported GCC findings to 61 State government entities (Table 1) and provided 39 of the 61 entities with capability maturity assessments. These assessments look at how well-developed and capable entities' established IT controls are and compare their self-assessments with our audit results.

39 entities issued GCC findings and capability assessments			
Central Regional TAFE	Commissioner of Main Roads	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	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	Government Employees Superannuation Board
Health Support Services	Housing Authority	Lotteries Commission (Lotterywest)	Mental Health Commission
Murdoch University	North Metropolitan Health Service	North Metropolitan TAFE	North Regional TAFE
Office of the Information Commissioner	PathWest Laboratory Medicine WA	Racing and Wagering Western Australia	Rottnest Island Authority
South Metropolitan Health Service	South Metropolitan TAFE	South Regional TAFE	University of Western Australia
WA Country Health Service	WA Police Service	Western Australian Land Information Authority (Landgate)	
22 entities issued GCC findings only			
Building and Construction Industry Training Board	Botanic Gardens and Parks Authority	Corruption and Crime Commission	Department of Fire and Emergency Services
Department of Health	Department of Jobs, Tourism, Science and Innovation	Electricity Generation and Retail Corporation (Synergy)	Electricity Networks Corporation (Western Power)

Forest Products Commission	Fremantle Port Authority	Gold Corporation	Kimberley Ports Authority
Parliamentary Services Department	Pilbara Ports Authority	Public Transport Authority of Western Australia	Regional Power Corporation (Horizon Power)
Water Corporation	Western Australian Health Promotion Foundation	Western Australian Land Authority (LandCorp)	Western Australian Sports Centre Trust (VenuesWest)
Western Australian Tourism Commission	Zoological Parks Authority		

Source: OAG

Table 1: State government entities issued GCC findings and assessments

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 sophistication of entity computer systems
- significance of information managed by the entity.

As signalled in our previous information systems report[2], we have modernised and updated our capability maturity model for the 2021-22 audits to increase understanding, transparency and guidance to entities in the area of information and cyber security. It builds on our previous model, increasing the control categories from six to 10, by breaking down the category of information security into the following five categories:

- information security framework
- human resource security
- manage access
- endpoint security
- network security.

[2] Office of the Auditor General, *Information Systems Audit Report 2022 – State Government Entities*, OAG, Perth, 2022.

Our 2021-22 audits, focused on these 10 categories:

Source: OAG

Figure 1: GCC categories for 2021-22

Conclusion

We reported 566 general computer control findings to 61 entities this year, compared to 526 findings to 54 entities last year. These findings, if not addressed, could result in data breaches, system outages and financial loss. Recent cyber security incidents both in Australia and globally highlight the ever present risk of cyber attacks and the need for entities to manage and secure their information system environments.

Concerningly, half of this year's audit findings (282) were unresolved issues from the previous year. Similar to last year it highlights a tendency for entities not to resolve weaknesses from one year to the next. It is crucial entities prioritise addressing audit findings to safeguard their information systems against constantly evolving and increasingly sophisticated threats.

Our updated capability maturity model now includes 10 control categories, five of which relate broadly to information and cyber security, areas of significant concern to us. Over half of the entities failed to meet the benchmark in three of these categories: endpoint security was the weakest, followed by access management and human resource security. Although more than half of the entities met the benchmark for network security, 21% of findings in this category were significant and high-risk. There was no material change in IT risk management, change management and business continuity however, a noticeable decline in physical security this year.

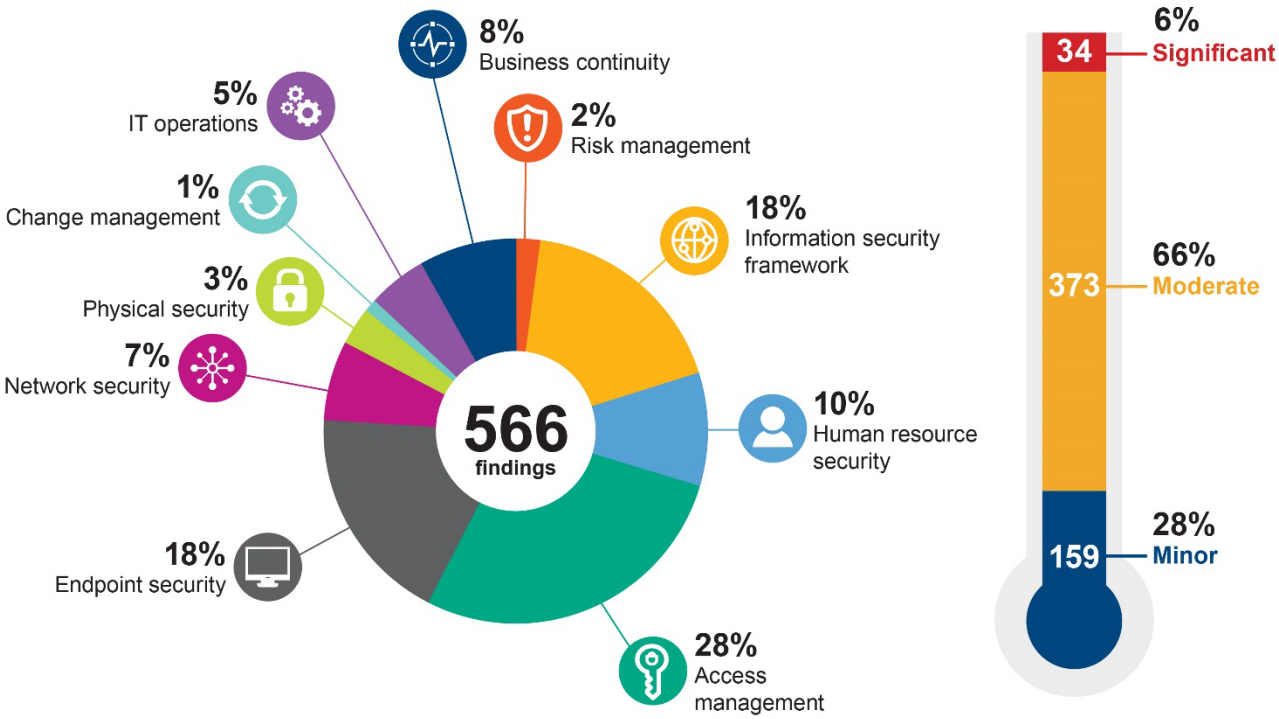
One entity met the benchmark in all 10 control categories. A small number of other entities met the benchmark in at least seven of the 10 categories and have showed consistent performance in our prior reports.

At 13 entities[3], their access management and network security control weaknesses were so significant and pervasive that their financial audit controls opinion was qualified.

[3] Office of the Auditor General, *Financial Audit Results – State Government 2021-22*, OAG, Perth, 2022, pp. 76–81.

What we found: General computer controls

In 2021-22, we alerted 61 entities to 566 information system weaknesses: 34 were rated significant, 373 moderate and 159 minor.



Source: OAG

Figure 2: Ratings for GCC findings in each control category

What we found: Capability assessments

We provided capability maturity assessments covering 10 GCC categories to 39 State government entities.

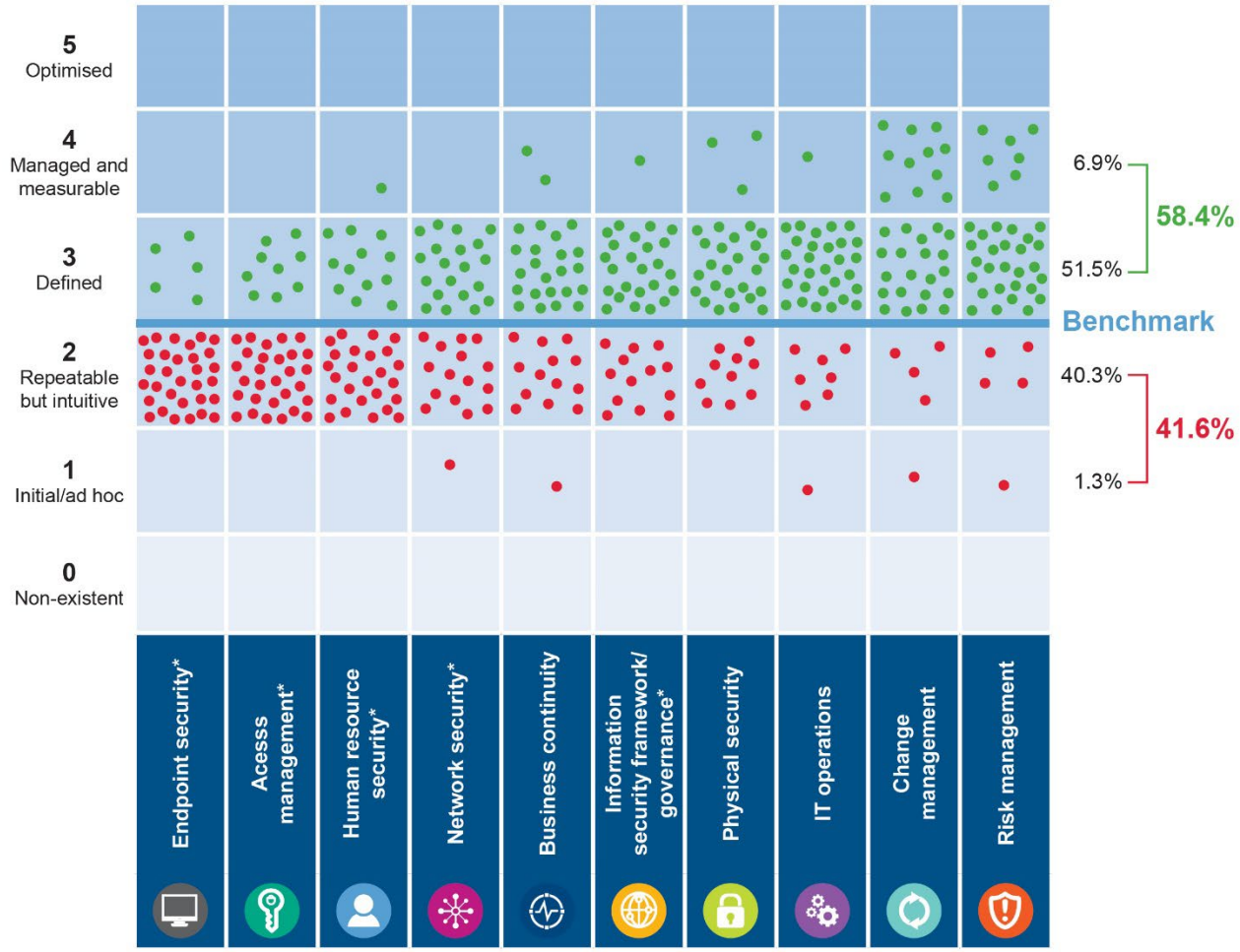
We use a 0-5 rating scale[4] (Figure 3) to evaluate each entities' capability maturity level in each of the 10 GCC categories. We expect entities to achieve a level 3 (Defined) rating or better in each category.

Source: OAG

Figure 3: Rating scale and criteria

[4] The information within this maturity model assessment is derived from the criteria defined within COBIT 2019, released in 2018 by ISACA.

Figure 4 shows the results of our capability assessments across the 10 control categories.



Source: OAG

** Information and cyber security control categories.*

Figure 4: Capability maturity assessment results

The percentage of entities rated level 3 or above for individual categories was as follows:

Category		2021-22 %		2020-21 %
1.	Endpoint security	14	Direct comparison not available. First year reported as separate categories.	50
2.	Access management	24		
3.	Human resource security	34		
4.	Network security	56		
5.	Information security framework	66		
6.	Business continuity	63	—	65
7.	Physical security	73	↓	94

Category		2021-22 %		2020-21 %
8.	IT operations[5]	79	↓	94
9.	Change management	86	–	85
10.	Risk management	87	–	86

Source: OAG

Table 2: Percentage of entities rated level 3 or above

Our assessments show that endpoint security, access management and human resource security require attention. In addition, while more than half of the entities met the benchmark for network security, 21% of weaknesses in this area were rated as significant and high risk.

There was no material change in IT risk management, change management and business continuity, but physical security saw a decline in performance this year. While the IT operations category also declined, this is mainly because some controls previously tested in this area now fall in the new access management category.

The Department of Water and Environmental Regulation met the benchmark in all 10 control categories.

The following entities met the benchmark in at least seven of the 10 categories and have consistently performed well in our prior reports:

- Department of Finance
- Department of the Premier and Cabinet
- Department of Training and Workforce Development
- Lotterywest
- Racing and Wagering Western Australia
- Landgate
- Curtin University.

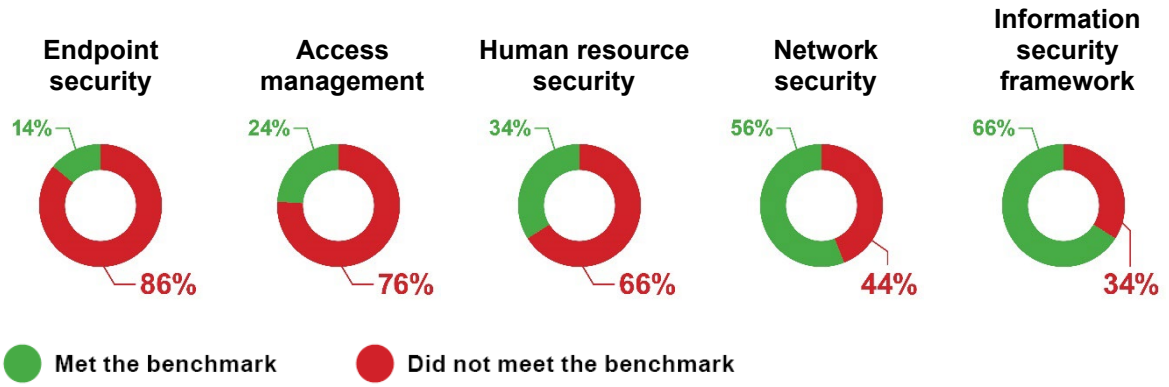
Information and cyber security

Last year we reported[6] that significant information security weaknesses contributed to the highest number of qualified opinions on financial statements controls or key performance indicators ever reported by this Office. In 2021-22, information cyber security control weaknesses continued to contribute towards an increased number of qualified opinions.

[5] Some controls tested under IT operations previously, have been moved to access management category in 2021-22.

[6] Office of the Auditor General, *Information Systems Audit Report 2022 – State Government Entities*, OAG, Perth, 2022.

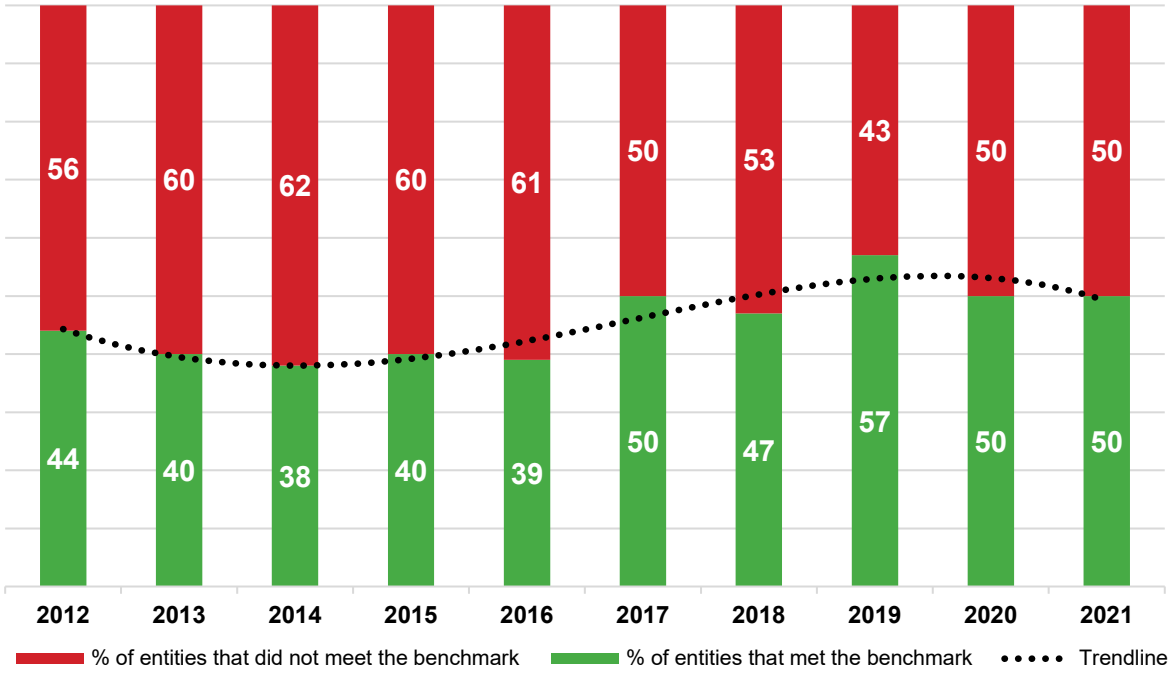
Our 2021-22 findings again highlight the need for entities to take proactive measures to address weaknesses and keep information and cyber security as a heightened area of focus.



Source: OAG

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

This year we have not directly compared our information and cyber security findings to prior year results as our model now separates controls in this area into five categories instead of one. Instead, the following graph provides past year results on the percentage of entities that met/did not meet the benchmark for our old information security category.



Source: OAG

Figure 6: Percentage of entities that met/did not meet the benchmark for information security from 2012 to 2021

As a result of seeing little noticeable improvement, information security has been our top concern over the past 10 years. We found numerous vulnerabilities and shortcomings in critical areas that could be remediated by implementing Australian Cyber Security Centre's (ACSC) mitigation strategies with a key focus on Essential 8 controls, also mandated by the

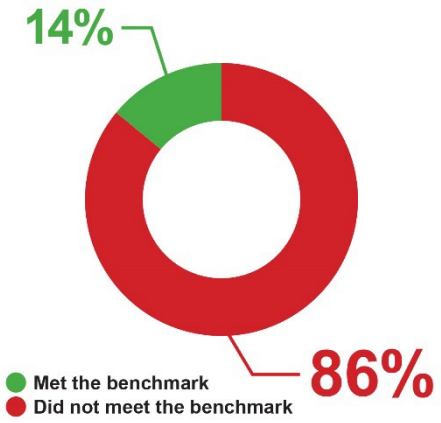
WA Government Cyber Security Policy[7]. Essential 8 strategies are designed to help entities manage and address common cyber security risks and improve their information and cyber security posture. While the *WA Government Cyber Security Policy* is not mandatory for Government trading entities or the tertiary sector, we encourage adoption of the principles in their approach to information and cyber security.

1. Endpoint security

Endpoint security was the weakest of the 10 categories, leaving entities more susceptible to attacks that compromise their information and operations. Only 14% of entities met the benchmark.

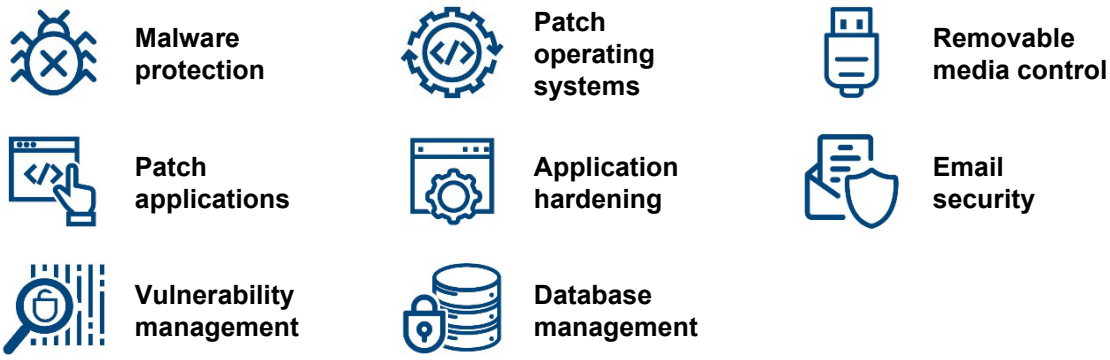
Endpoint security ensures devices connected to the network are secure. If left unsecured, the risk of cyber attacks and data breaches increase.

We reviewed entities' malware controls and if vulnerabilities are promptly identified and addressed. We also tested if the installation of software is controlled, unapproved applications and macros are prevented and if email authentication controls work. As staff and contractor devices may connect remotely we tested if entities checked the security posture of devices before allowing access.



Source: OAG

Figure 7: Percentage of entities that met/did not meet the benchmark for endpoint security



Source: OAG

Figure 8: Endpoint security controls included in our GCC audits

Common weaknesses included:

- **Unapproved applications were not blocked** – heightening the risk of malware infections that can compromise an entity's network and systems.
- **Untrusted code was not blocked** – malicious code including macros can spread malware resulting in loss of services or ransomware.
- **Email systems were not adequately configured** – lack of controls or misconfigured email authentication can result in impersonation and data breaches. Controls such as

[7] Department of the Premier and Cabinet, *WA Government Cyber Security Policy*, DPC, Perth, 2021.

domain-based message authentication (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented or not configured properly.

- **Ineffective vulnerability management processes** – a high number of vulnerabilities persisted due to unsupported or unpatched systems, which could be exploited by malicious actors.

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

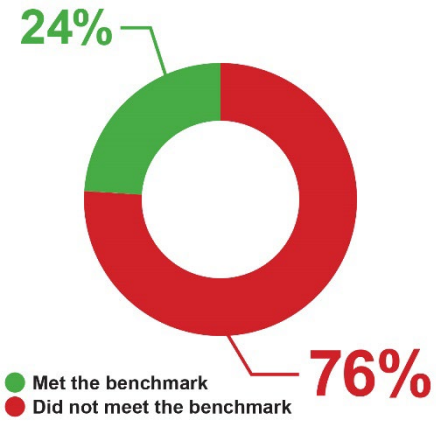
Case study 1: Malicious actor impersonated a government executive officer

Ineffective email authentication controls allowed a malicious actor to impersonate a government executive officer and sent emails containing false claims to internal and external parties. This incident could have been prevented with effective email authentication controls.

2. Access management

Access management is another area of information and cyber security weakness, with only 24% of entities meeting the benchmark. This is a concerning sign that entities are not doing enough to secure their sensitive data and systems. Poor access management controls increase the risk of security incidents, financial loss and reputational damage.

We reviewed entities' controls, including access rights and reviews for key business applications, active user accounts, privileged access, password policies, multi-factor authentication and the use of generic/shared accounts.



Source: OAG

Figure 9: Percentage of entities that met/did not meet the benchmark for access management

Source: OAG

Figure 10: Access management controls included in our GCC audits

Common weaknesses included:

- **Access was not promptly revoked** – there is a heightened risk of inappropriate or unauthorised access when accounts of former staff are not promptly deactivated.
- **Password configurations did not meet entities' standards** – insufficient enforcement of password requirements to access databases and applications can result in information loss or a data breach.
- **Privileged access given to an excessive number of accounts** – privileged accounts, including generic accounts, increase the risk of unintentional or intentional misuse of access.
- **Non-existent or ineffective system logging and monitoring** – malicious activity may go unnoticed if processes to log and monitor system access do not exist or are ineffective.
- **Multi-factor authentication (MFA) was not used for privileged accounts** – use of legacy authentication and not enforcing MFA can lead to unauthorised access.

These common weaknesses and their importance to information and cyber security are further highlighted in the following case studies.

Case study 2: Lack of MFA results in data breach

At one entity, a malicious insider reset the password of another staff member to gain access to a key business system and then copied information. This inappropriate access could have been prevented or made more difficult if multi-factor authentication was enforced.

The entity was unaware of the malicious access and data extraction for several months as their access logging and monitoring processes did not work properly.

We also found very weak database passwords were in use and network passwords did not fully comply with the entity's password standards. These vulnerabilities increase the entity's susceptibility to internal and external malicious actors.

Case study 3: Highly privileged account of a former employee was being used by other employees

At one entity, the privileged account of a former IT staff member who left the entity in 2019 was still active and being used by other staff in 2022. This highly privileged account had not been disabled.

Individual accounts allow entities to hold staff accountable for any unauthorised or unintentional modifications to IT systems and information.

Case study 4: Principle of least privilege not applied to cloud environment

One entity had assigned an unusually high number of accounts with privileged roles, contrary to better practice. It had:

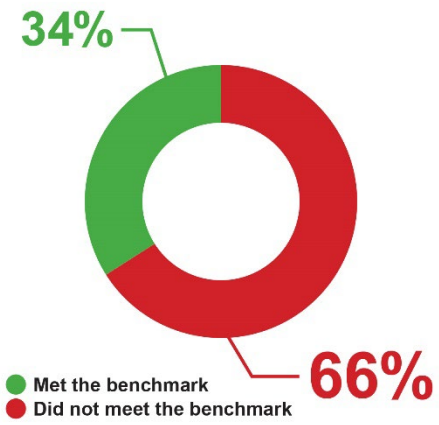
- 27 global administrators
- 20 exchange administrators
- 28 SharePoint administrators
- 12 enterprise administrators.

A large number of users with privileged roles increases the risk of a security breach and malicious activity. Accounts should only be given the privileges required for the role.

3. Human resource security

Only 34% of the entities met the benchmark in human resource (HR) security. If HR risks are not managed there is an increased likelihood that insider threats will go unnoticed which may result in theft of information and lead to other security incidents.

HR security ensures that employees, contractors and third-party vendors adhere to security policies and procedures. Proper screening, training and awareness programs can help prevent insider threats, protect against social engineering attacks and safeguard confidential information.



Source: OAG

Figure 11: Percentage of entities that met/did not meet the benchmark for human resource security

We reviewed if entities have formal and effective processes for pre-employment screening, staff induction, confidentiality/non-disclosure requirements and termination procedures. Entities also need programs to educate staff about their information security responsibilities, including ongoing security awareness programs and disciplinary processes to address breaches.

Source: OAG

Figure 12: Human resource security controls included in our GCC audits

Common weaknesses included:

- **Background screenings not performed** – if background checks are not performed for key positions, there is an increased risk of unauthorised system access, fraud and malicious activity.
- **Onboarding processes lacked IT acceptable use acknowledgement** – lack of acknowledgement of individual responsibilities can heighten the risk of misuse and inappropriate actions.
- **Information security awareness training was either not mandatory or not provided** – creating a culture of security requires regular training. Employees who haven't undergone information and cyber security training may not know what good security behaviours look like or how to practice them.
- **No contractor central register** – unauthorised network and system access may go undetected without visibility of contractors working for an entity.
- **Employee termination processes were not fully effective** – ineffective termination processes may contribute to unauthorised access to entity premises, information and systems, and financial loss if assets aren't returned by departing individuals.

The following case study illustrates common weaknesses in HR security.

Case study 5: Former employee gained unauthorised access to the financial system

One entity failed to complete exit procedures required to revoke an employee's access to network and systems. We found that a former employee accessed the entity's physical facility, logged on to the entity's network and accessed the financial system more than one month after their employment had been terminated. Usually, this type of behaviour is associated with malicious intent.

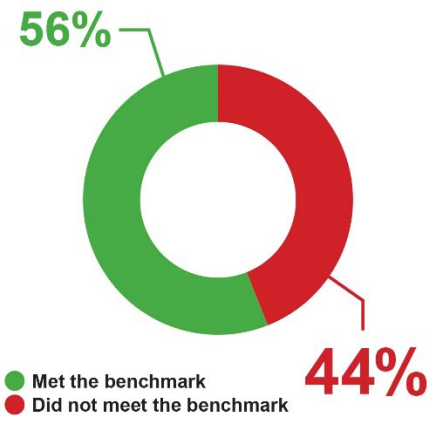
Additionally, a lack of security event logging and monitoring meant the entity could not perform a forensic analysis to determine what records or systems were accessed by the former employee and if any malicious activity occurred.

In addition to strengthening its employee termination processes, including revoking system access, the entity should log and monitor system access and develop a security incident response plan to help it respond to and contain security breaches.

4. Network security

Forty-four percent of the entities did not meet the benchmark for network security with 21% of the weaknesses rated as significant. Network security controls protect the network and key systems from cyber intrusions.

We assessed if entities had secure administration processes and network segregation, prevented unauthorised devices from connecting to the network and performed regular penetration tests.



Source: OAG

Figure 13: Percentage of entities that met/did not meet the benchmark for network security

Source: OAG

Figure 14: Network security controls included in our GCC audits

Common weaknesses included:

- **Outdated equipment** – aging network infrastructure may not support security controls and leave entities more susceptible to cyber intrusions.
- **Lack of network segregation** – cyber breaches may spread and be difficult to contain when networks are not segregated. IT and operational technology devices should also be segregated to avoid breaches and potential loss of life in clinical settings.
- **Unauthorised devices were allowed to connect to the network** – unauthorised devices could be used as an attack vector to spread malware or eavesdrop on communications.

The following case studies illustrate the importance of network security controls.

Case study 6: Network outage caused by an unauthorised device

One entity did not have any controls to stop unauthorised devices from connecting to its network and suffered a network intrusion when an unauthorised device was connected. Applications and systems became unavailable for a number of staff, disrupting the entity's key services to the public.

Lack of effective monitoring controls meant the entity was unable to locate the device or determine if it was connected for malicious purposes. The entity only prepared a cyber security incident report to appropriately investigate the matter after our audit notified them of the need to classify the incident as a cyber security breach.

Case study 7: Decades old network equipment leaves entity at significant security risk

One entity with a significant number of connected sites, has not kept its network infrastructure up-to-date. Key network devices lack modern security features, the network is not segregated and there are no controls to detect or prevent unauthorised devices at the majority of its sites. If one site is compromised, the attack would spread to other connected locations severely impacting the entity's ability to deliver important services to the community.

Furthermore, the entity has not segregated its IT network from its operational technology. This further increases the risk of cyber intrusion and loss of key service delivery if an attack

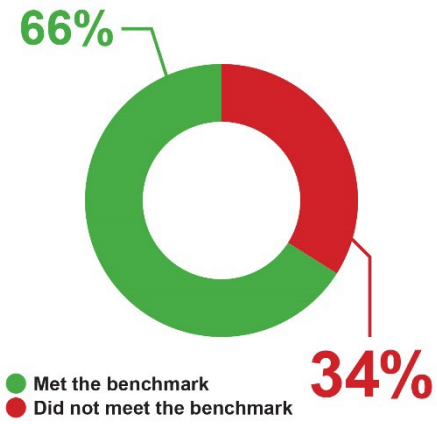
spreads to operational technology devices. As a result, in 2021-22 the entity's financial statement and controls opinion was qualified.

5. Information security framework

Entities generally performed well with 66% of entities meeting the benchmark in this category. The remaining entities need to improve their information and cyber security governance and use a structured approach to mitigate security risks and protect their sensitive information and key systems.

We assessed if entities have appropriate policies and roles, including a committee to govern information security, and communication processes with security groups. We also looked at:

- information classification procedures
- processes and controls to prevent information loss
- risk assessments for selecting cloud vendors and if regular assessments are conducted of cloud environment security.



Source: OAG

Figure 15: Percentage of entities that met/did not meet the benchmark for information security framework

Source: OAG

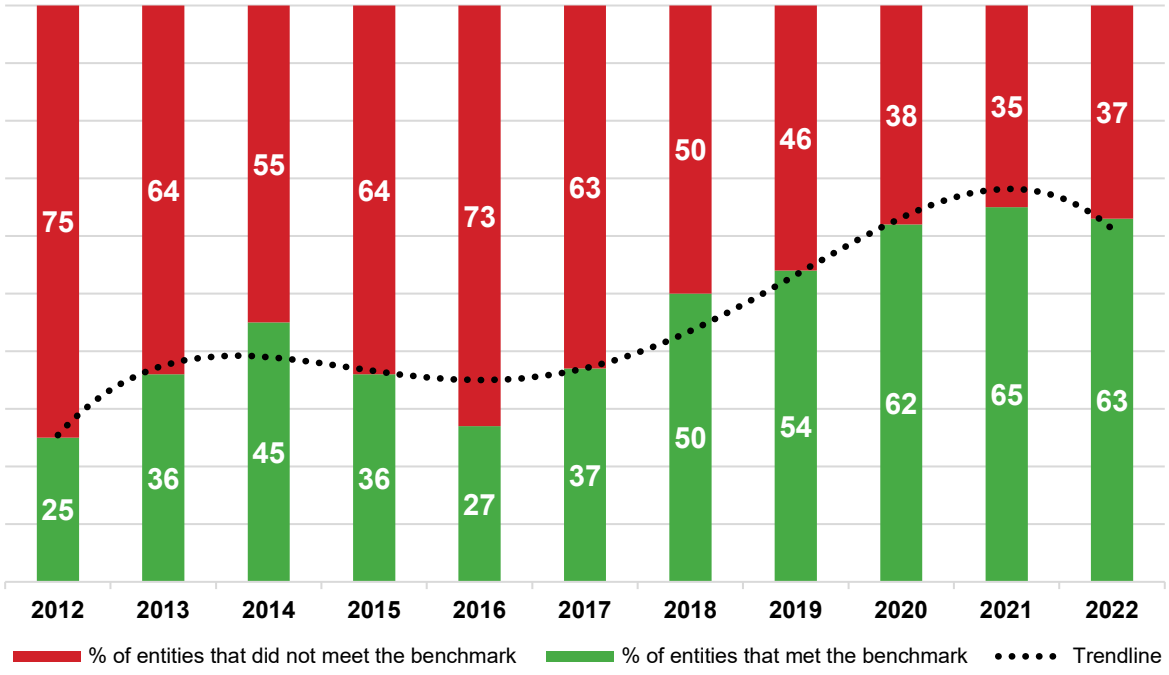
Figure 16: Information security framework controls included in our GCC audits

Common weaknesses included:

- **Information security policies were either in draft or overdue for review** – an entity's information security requirements and objectives are less likely to be achieved if their policies, standards and procedures are inadequate.
- **Lack of ongoing security assurance from service providers** – ineffective vendor management can result in outsourced IT services not meeting an entity's expectations, leaving an entity vulnerable to security, financial and reputational risks.
- **Data loss prevention controls were not adequate or not in place** – there is a risk that sensitive data leakage (through USB, cloud and email) and theft might not be detected in a timely manner to prevent or reduce data loss.

6. Business continuity

There was no material change this year with 63% of entities meeting the benchmark for business continuity. Effective business continuity processes focus on strategies, procedures and plans to ensure that an organisation can continue to operate, or quickly resume operations, when a disruption or disaster event strikes.



Source: OAG

Figure 17: Percentage of entities that met/did not meet the benchmark

We assessed if entities have business continuity, disaster recovery, backup and incident response plans and if their effectiveness is regularly tested.

Source: OAG

Figure 18: Business continuity controls included in our GCC audits

Common weaknesses included:

- **Outdated continuity plans** – entity activities and key service delivery to the public may experience prolonged downtimes during a disruption if plans do not align with current State processes. This can result in financial loss and reputational damage.
- **Lack of regular testing** – if not regularly tested, entities may not be aware of gaps in their continuity plans which may lead to data loss or extended recovery times for their key systems.

- **Lack of endorsed cyber incident response plans** – without a plan, entities may be unprepared to handle a cyber incident which can lead to a delayed response and it may not be able to contain the breach adequately.

The following case studies illustrate common weaknesses in continuity planning.

Case study 8: Disaster recovery plan not tested

One entity experienced several issues when it invoked its disaster recovery plan during an outage. Because it had not tested its recovery plan, staff were unaware of their responsibilities, which led to confusion and delays in the recovery process. Allowed system outage timeframes and data recovery objectives were not achieved, disrupting the delivery of important services to the public.

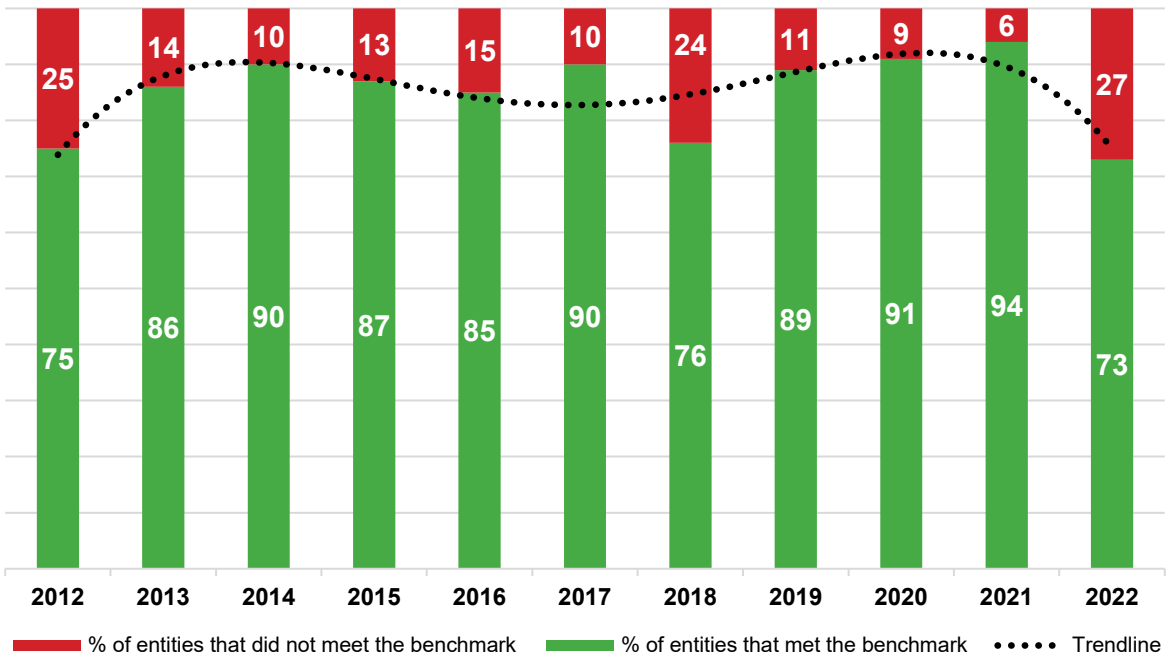
Not testing the disaster recovery plan can have serious consequences.

Case study 9: Outdated continuity plans and lack of testing

One entity did not update its continuity plans to reflect changes to its managed services providers and the shift of servers to a commercial data centre. The outdated plans do not reflect the current state of the entity's operations or infrastructure, which will make it difficult to execute the plans in an emergency.

7. Physical security

This year, 73% of entities met the benchmark for physical security compared to 94% last year, making it the lowest rating for this category in a decade. This was primarily due to poor server room access management and maintenance of facilities. It is important to maintain secure access and environmental controls in server rooms, whether on-premises or managed through a third-party vendor.



Source: OAG

Figure 19: Percentage of entities that met/did not meet the benchmark for physical security

We assessed how entities manage physical controls, access, power, fire hazards, temperature and humidity controls in server rooms. We tested assurance mechanisms for vendor controls where server rooms were managed by third-parties or entities used infrastructure as a service.

Source: OAG

Figure 20: Physical security controls included in our GCC audits

Common weaknesses included:

- **Inappropriate access management to server rooms and data centres** – if access is not controlled it can result in unauthorised or inappropriate access to key systems and damage to infrastructure.
- **Poor data centre maintenance practices** – a lack of proper and regular maintenance of environmental controls heighten the risk of unplanned downtime of services and can also pose a risk to health and safety.
- **Inappropriate temperature and humidity controls** – can cause equipment failures, system downtime and decreased performance resulting in data and financial loss.

The following case studies illustrate common weaknesses in physical security.

Case study 10: Poor server room maintenance and unprotected paper records

During our visit to an entity's server room we found the ceiling had a hole in it which the entity did not know about and its uninterrupted power supply was also not maintained as some parts needed to be replaced.

In addition, a building's external and internal doors were left open despite the building storing thousands of paper records containing details of staff names, invoices and expense reports. The entity immediately secured these records when we informed them of the risk.

Case study 11: Terminated employees still had access to data centres

At one entity, swipe cards to access the data centre were still being used despite known vulnerabilities and no longer being recommended by the vendor. The vulnerabilities could allow access cards to be cloned and used by unauthorised individuals.

We also found terminated employees' access to the data centre had not been revoked due to deficiencies in the data centre access management process. Many current staff also had access that was not required or authorised.

Without appropriate access controls, there is an increased risk of unauthorised access to the server room.

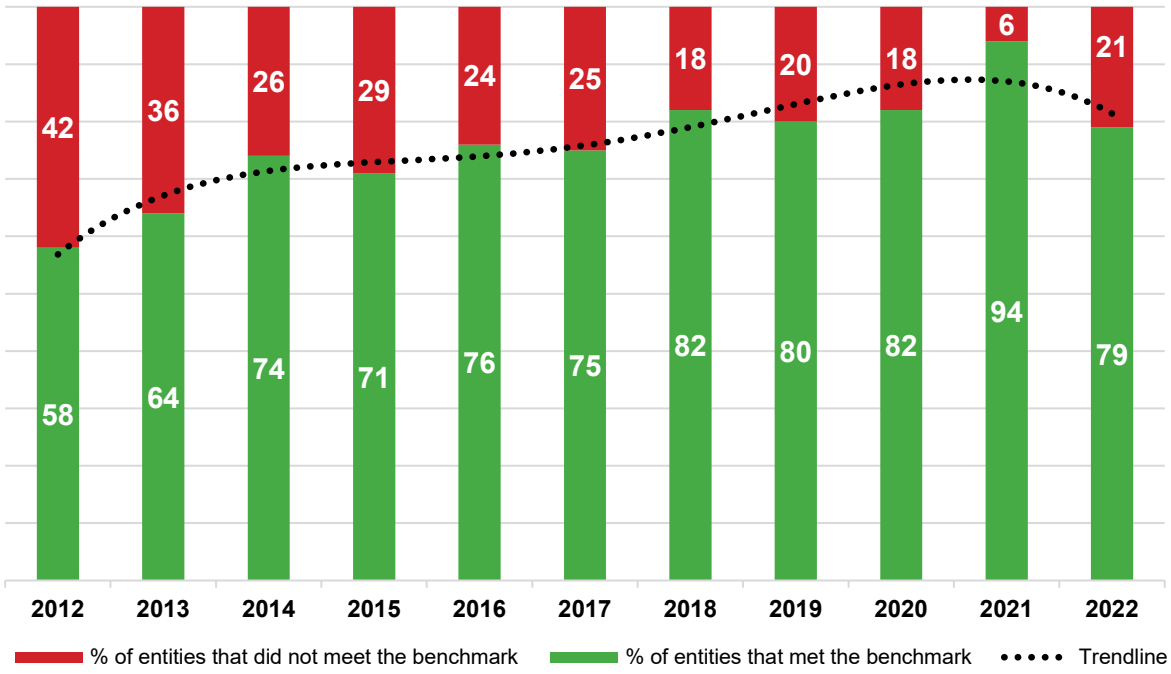
Case study 12: Inadequate assurance over managed data centre

One entity that uses a managed data centre had not regularly obtained and reviewed assurance reports from their data centre provider. Our review of the assurance reports identified the vendor did not terminate data centre access for its former staff. Assurance reports often disclose weaknesses that vendors need to remediate.

Entities should review assurance reports or undertake their own reviews to ensure they get the services they expect and controls implemented by the vendor are sufficient.

8. IT operations

This is another better performing category with 79% of entities meeting the benchmark. The decline in performance compared to last year is primarily due to some areas of IT operations moving to the access management category in our new capability maturity model.



Source: OAG

Figure 21: Percentage of entities that met/did not meet the benchmark for IT operations

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

IT assets lifecycle management

Supplier performance management

Incident and problem management

Source: OAG

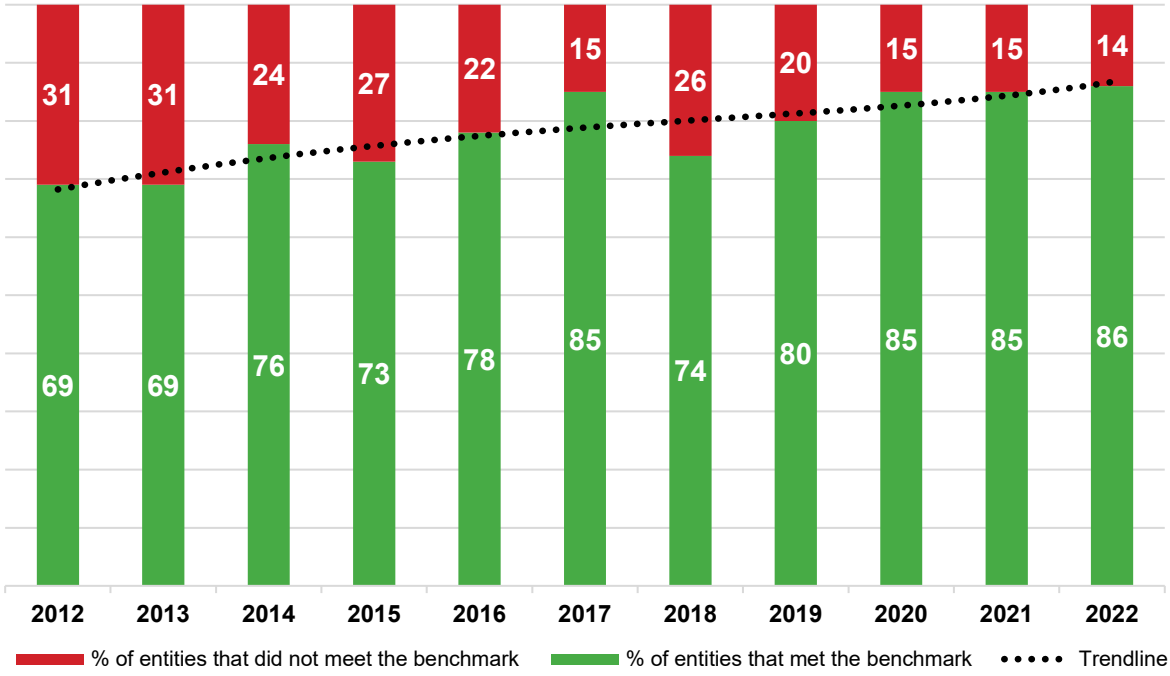
Figure 22: IT operational controls included in our GCC audits

Common weaknesses included:

- **IT asset management was not fully effective** – inadequate IT asset management processes increase the likelihood of lost or stolen IT assets, leading to potential financial loss and reputational harm.
- **Supplier performance was not monitored** – entities may not become aware when IT suppliers fail to fulfil their performance requirements and deliver substandard services. This can compromise entity systems and impact entity service delivery.
- **Lack of service level agreements** – vendors and entities may lack clarity about the expected levels of service delivery and entities may not receive the level of service they have paid for.

9. Change management

The percentage of entities that met the benchmark in change management was 86% in 2021-22, the highest since we started benchmarking this category 14 years ago and continuing an upward trend.



Source: OAG

Figure 23: Percentage of entities that met/did not meet the benchmark in change management

We assessed if entities have processes to authorise and test changes before releasing them to production systems and infrastructure. We also assessed how they manage emergency changes and if access to their production environments is segregated from test and development environments.

Source: OAG

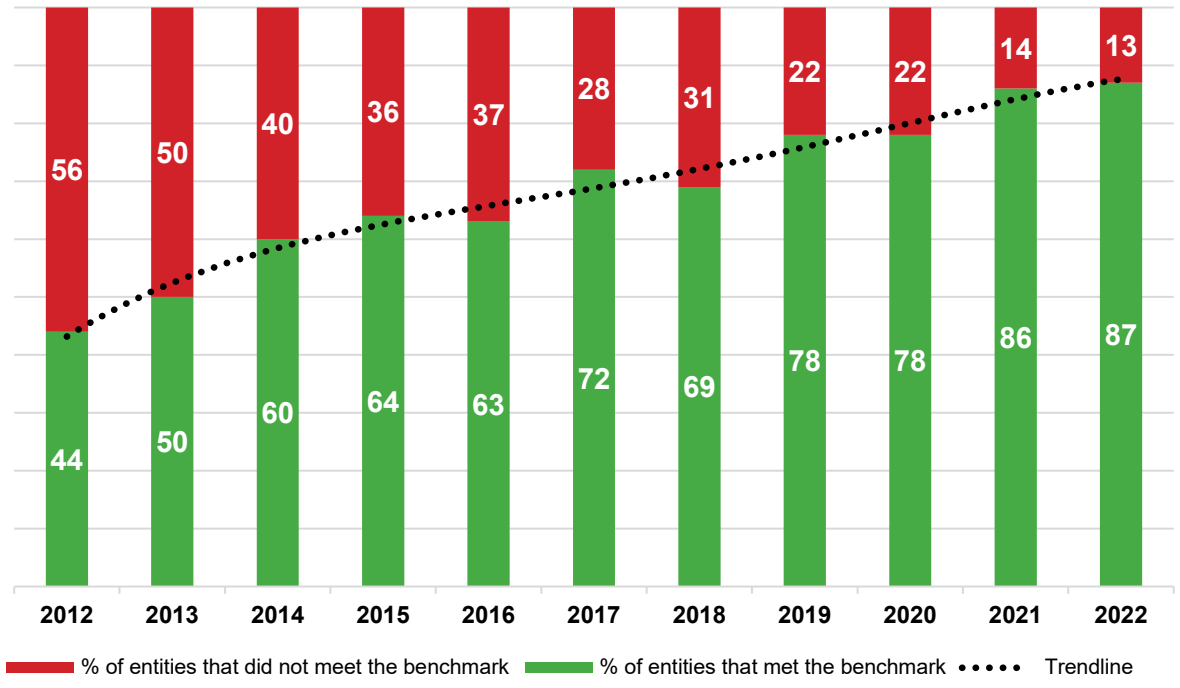
Figure 24: Change management controls included in our GCC audits

Common weaknesses included:

- **Change management procedures were not approved or up-to-date** – this increases the likelihood of errors, delays and failures in implementing changes.
- **No separation of production and non-production environments** – without separation, unauthorised changes may be made to key applications which compromise the integrity and availability of systems.

10. Risk management

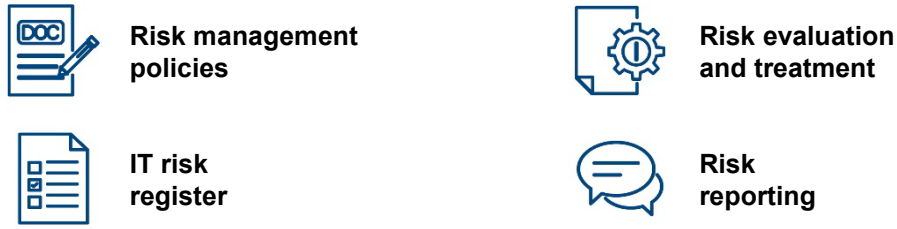
In 2021-22, 87% of entities met the benchmark for this category. This category has shown a consistent positive trend over the last decade. A robust risk management process reduces the likelihood and impact of negative events and enhances overall decision-making.



Source: OAG

Figure 25: 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 26: Risk management control included in our GCC audits

Common weaknesses included:

- **Outdated risk management policies or frameworks** – outdated policies and processes may not mitigate emerging risks and leave an entity exposed to potential harm.
- **Failure to maintain IT risk registers** – it is essential to identify, assess and record all relevant risks, including information and cyber risks, in a risk register.

The following case study illustrates common weaknesses in IT risk management**.**

Case study 13: Risks posed by unmanaged mobile devices were not formally assessed

One entity had not adequately assessed the risks of unmanaged mobile devices connecting to its network. As a result, the entity had not implemented controls to:

- apply software updates
- prevent the use of unauthorised applications
- remotely wipe data if mobile devices are lost or stolen
- restrict the use of public Wi-Fi.

The entity is at increased risk of unintentional data loss and unauthorised access to their systems.

Recommendations

1. **Endpoint security**

   Entities should:

   a. implement effective controls against malware

   b. promptly identify and address known vulnerability

   c. control installation of software on workstations

   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 have access, entities should:

   a. implement effective access management processes

   b. regularly review active user accounts

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

   d. limit and control administrator privileges

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

3. **Human resource 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 employees

   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 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, particularly for IT and Operational Technology systems

   d. limit 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 roles in line with the *WA Government Cyber Security Policy*

b. conduct regular assessments or gain comfort through assurance reports to ensure their IT supply chain is secure

c. classify information and implement data loss prevention controls

d. assign responsibility to a committee to direct information and cyber security activities.

6. Business continuity

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

7. Physical security

Entities should:

a. implement effective physical and access controls to prevent authorised access

b. maintain environmental controls to prevent fire hazards and damage to IT infrastructure

c. gain assurance that providers manage data centres appropriately.

8. 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.

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 the occurrence of problems

c. maintain change control documentation

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. They should incorporate good risk management practices in their core business activities

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

d. implement controls to detect unauthorised changes.

This page is intentionally left blank

Auditor General's 2022-23 reports

Number	Title	Date tabled
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation for Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee's Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

Office of the Auditor General
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