OAG
Office of the Auditor General
Serving the Public Interest

Report 19: 2022-23 | 29 March 2023

INFORMATION SYSTEMS AUDIT

Local Government 2021-22

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Paul Tilbrook
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: Chim/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit – Local Government 2021-22

Report 19: 2022-23
29 March 2023

This page is intentionally left blank

THE PRESIDENT LEGISLATIVE COUNCIL	THE SPEAKER LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT – LOCAL 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 our fourth report on the audits of local government entities' general computer controls.

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

CAROLINE SPENCER
AUDITOR GENERAL
29 March 2023

Contents

Auditor General’s overview

This is the fourth local government annual information systems (IS) audit report by my Office. It summarises the results of the 2021-22 cycle of information systems audits for 53 local government entities[1]. These audits were performed between April 2022 and March 2023.

Local government entities are increasingly adopting technologies and systems to deliver efficiencies in their operations and improve the delivery of services to the communities they serve. As local government entities’ digital footprints increase, so too do their risks. Our information systems audits are designed to help local government entities to identify and mitigate these risks and protect citizens’ information against inappropriate disclosure, loss or misuse.

We reported 324 control weaknesses to 53 entities. Disappointingly, 69% (225) of these weaknesses were unresolved issues from the prior year. A large proportion of weaknesses, 72% (235), related to information and cyber security risks.

In recognition of evolving cyber security threats, we have updated our capability maturity model to include 10 control categories. Five of the 10 categories relate broadly to information and cyber security – areas of significant concern to us. The updated model provides more information on the state of system, information and cyber security in the local government sector and what can be done to address weaknesses.

The majority of entities failed to meet the benchmark in the five information and cyber security categories: human resource security and network security being the weakest, followed by access management, endpoint security and information security framework. In other categories, we saw improvements in the areas of IT risk management, change management, physical security, IT operations and business continuity. We have included case studies throughout this report to highlight how poor controls increase the risk to entities’ systems.

Local government entities of all sizes can fine-tune their existing systems and practices to uplift their resilience to the ever present and evolving nature of cyber security threats. Notably, many weaknesses do not require expensive technology investments to fix.

The local government sector should use the case studies and recommendations in this report to inform enhancements to their general computer controls. This will build much needed digital trust and public confidence in the local government sector’s capacity to successfully operate in the digital economy.

[1] Local government entities issued with general computer control findings as at 24 March 2023.

2021-22 information systems audits at a glance

Auditing local government entities

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

12 audits included capability maturity assessments

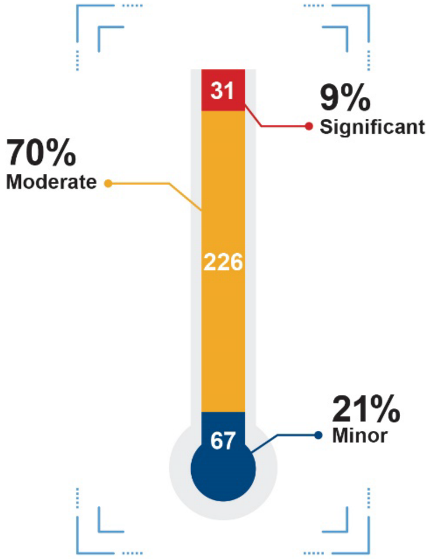
4th year reporting on the results of local government entities' general computer controls

Audit results

324 information systems control weaknesses (page 10)

225 (69%) weaknesses were unresolved issues from previous years

Of the **12** capability maturity assessments performed **no entity** met the benchmark in all 10 control categories



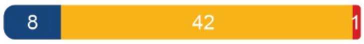
Information security framework

25%

entities met the benchmark

(page 19)

Number of issues identified:



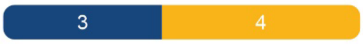
Risk management

67%

entities met the benchmark

(page 23)

Number of issues identified:



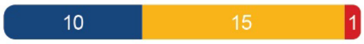
Human resource security

0%

entities met the benchmark

(page 13)

Number of issues identified:



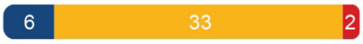
Business continuity

25%

entities met the benchmark

(page 20)

Number of issues identified:



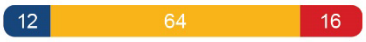
Access management

8%

entities met the benchmark

(page 16)

Number of issues identified:



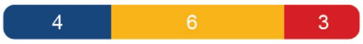
Change management

67%

entities met the benchmark

(page 24)

Number of issues identified:



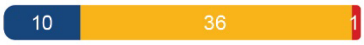
Endpoint security

8%

entities met the benchmark

(page 18)

Number of issues identified:



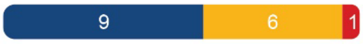
IT operations

42%

entities met the benchmark

(page 22)

Number of issues identified:



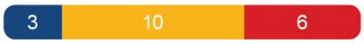
Network security

0%

entities met the benchmark

(page 15)

Number of issues identified:



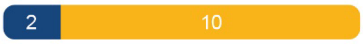
Physical security

67%

entities met the benchmark

(page 25)

Number of issues identified:



● Minor ● Moderate ● Significant

Introduction

This is our fourth report on the audits of local 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 against data breaches and cyber security threats.

For 2021-22, we reported GCC findings to 53[2] local government entities and provided 12 of the 53 entities with capability maturity assessments. These assessments look at how well-developed and capable entities' established IT controls are. We have not named the entities issued with GCC findings and capability assessments so as not to increase their exposure to cyber threats.

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.

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] Entities issued with GCC findings as at 24 March 2023.

Our 2021-22 audits focused on these 10 categories:

Information security framework

Human resource security

Access management

Endpoint security

Network security

Risk management

Business continuity

Change management

IT operations

Physical security

Source: OAG

Figure 1: GCC categories for 2021-22

Conclusion

For 2021-22 we reported 324 general computer control findings to 53 entities, compared to 358 findings to 45 entities last year. Nine percent (31) of this year's findings were rated as significant and 70% (226) as moderate. A large proportion of these findings relate to information and cyber security weaknesses and, 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.

Disappointingly, 69% (225) of the findings were unresolved issues from the prior year, including 27 of the 31 significant findings. Entities need to prioritise addressing audit findings to safeguard their systems and information, and reduce the risk of compromise to their confidentiality, integrity and availability.

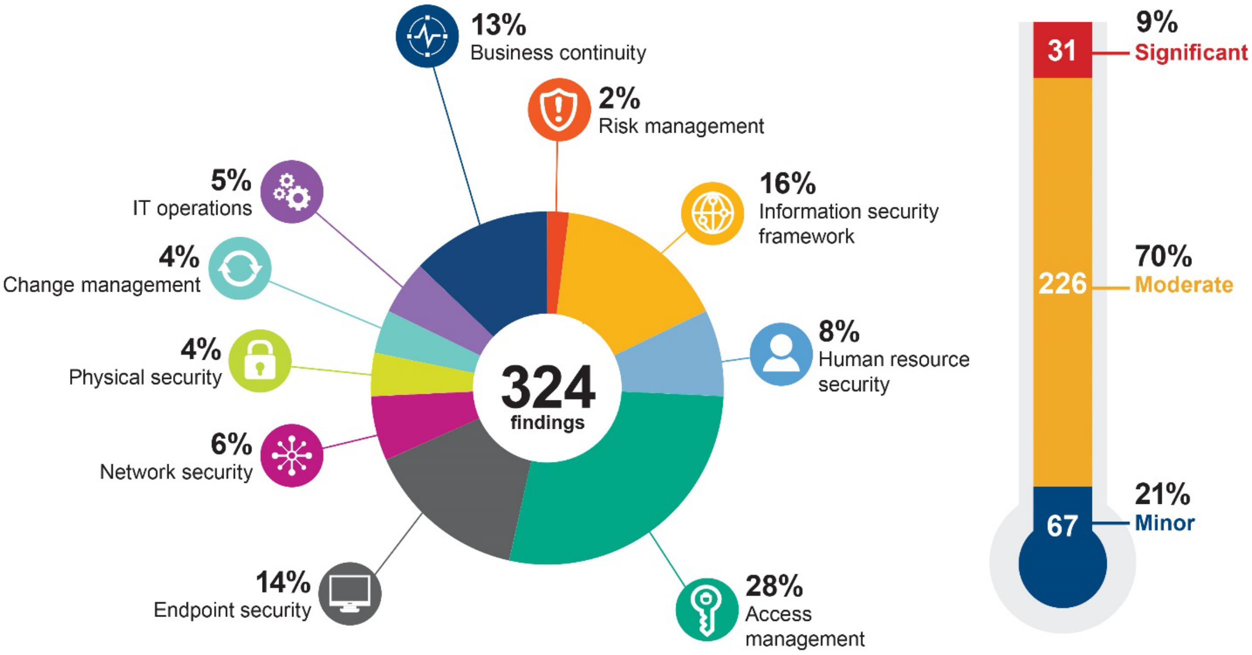
Our updated capability maturity model now includes 10 control categories, five of which relate broadly to information and cyber security. The majority of entities failed to meet the benchmark in these categories: human resource security and network security being the weakest, followed by access management, endpoint security and information security framework. Compared to last year, we saw improvements in the areas of IT risk management, change management, physical security, IT operations and business continuity.

What we found: General computer controls

We reported 324 information system weaknesses to 53 entities: 31 were rated significant, 226 moderate and 67 minor.

Figure 2 summarises the distribution and significance of our findings across the 10 control categories.

The majority of findings (70%) were rated moderate. However, when combined, these moderate risks increase an entity's overall exposure to cyber threats.



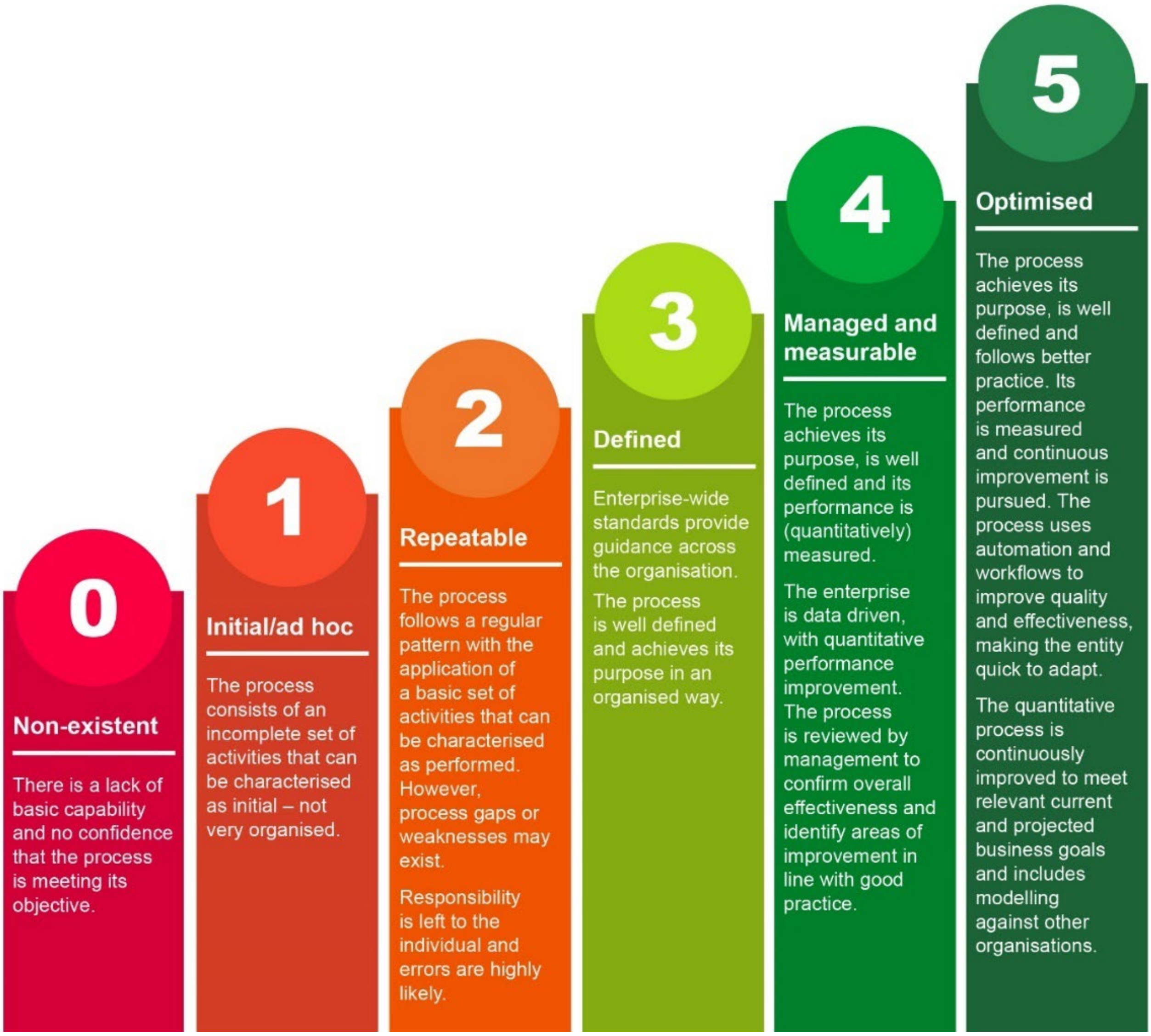
Source: OAG

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

What we found: Capability assessments

We provided capability maturity assessments covering 10 GCC categories to 12 local government entities.

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



0 **Non-existent**

There is a lack of basic capability and no confidence that the process is meeting its objective.

1 **Initial/ad hoc**

The process consists of an incomplete set of activities that can be characterised as initial – not very organised.

2 **Repeatable**

The process follows a regular pattern with the application of a basic set of activities that can be characterised as performed. However, process gaps or weaknesses may exist.

Responsibility is left to the individual and errors are highly likely.

3 **Defined**

Enterprise-wide standards provide guidance across the organisation.

The process is well defined and achieves its purpose in an organised way.

4 **Managed and measurable**

The process achieves its purpose, is well defined and its performance is (quantitatively) measured.

The enterprise is data driven, with quantitative performance improvement. The process is reviewed by management to confirm overall effectiveness and identify areas of improvement in line with good practice.

5 **Optimised**

The process achieves its purpose, is well defined and follows better practice. Its performance is measured and continuous improvement is pursued. The process uses automation and workflows to improve quality and effectiveness, making the entity quick to adapt.

The quantitative process is continuously improved to meet relevant current and projected business goals and includes modelling against other organisations.

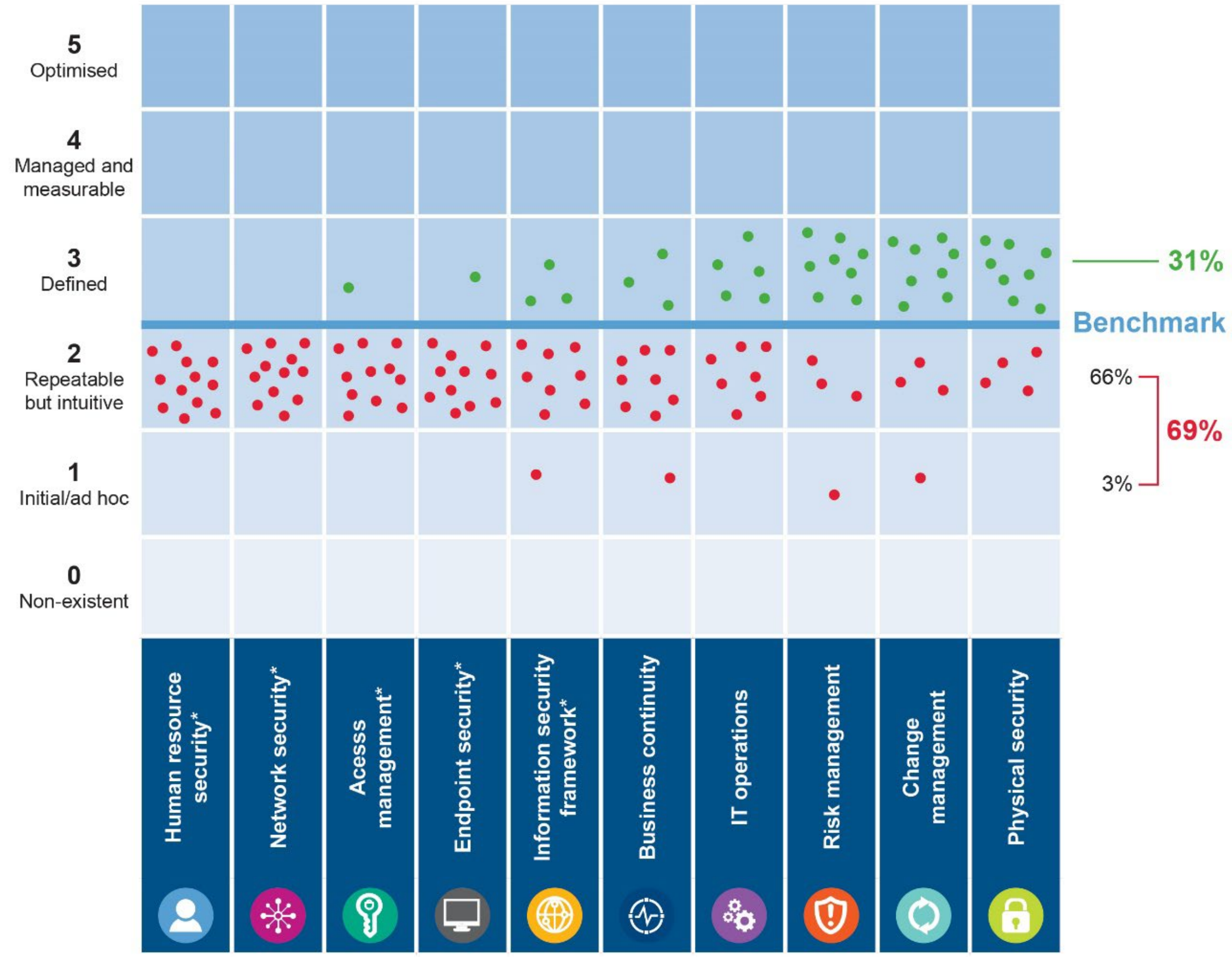
Source: OAG

Figure 3: Rating scale and criteria

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

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

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.	Human resource security	0	Direct comparison not available. First year reported as separate categories.	0
2.	Network security	0		
3.	Access management	8		
4.	Endpoint security	8		
5.	Information security framework	25		
6.	Business continuity	25	⬆	17
7.	IT operations[5]	42	⬆	33
8.	Risk management	67	⬆	42
9.	Change management	67	⬆	50

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

Category		2021-22 %		2020-21 %
10.	Physical security	67	⬆	50

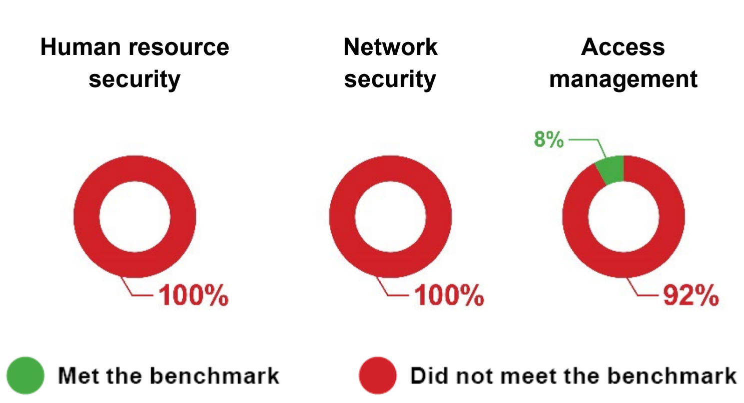
Source: OAG

Table 1: Percentage of entities rated level 3 or above

In 2021-22 there were improvements in five categories but of most concern are the weaknesses in the five information and cyber security categories: human resource (HR) security, network security, access management, endpoint security and information security framework.

Information and cyber security

We found many control weaknesses across all five information and cyber security categories.



Source: OAG

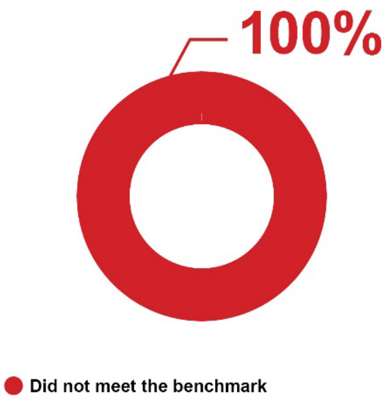
Figure 5: Percentage of entities that met/did not meet the benchmark in the five categories for information and cyber security

Well operating information and cyber security controls help entities to manage risks, protect sensitive information and deliver services securely. Entities are encouraged to implement the Australian Cyber Security Centre's mitigation strategies[6] designed to protect against common cyber threats with a key focus on Essential 8 controls.

1. Human resource security

None of the entities met the benchmark in this area. HR security ensures employees, contractors and third-party vendors adhere to security policies and procedures.

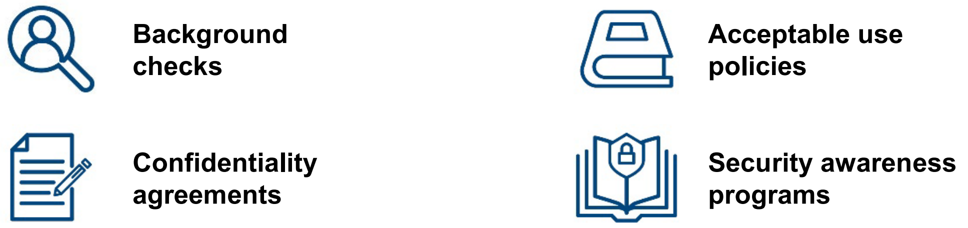
Proper screening, training and awareness programs can help identify and prevent insider threats, protect against social engineering attacks and safeguard confidential information.



Source: OAG

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

[6] Australian Cyber Security Centre, *Strategies to Mitigate Cyber Security Incidents*, ACSC, Canberra, 2017.



Background checks

Acceptable use policies

Confidentiality agreements

Security awareness programs

Source: OAG

Figure 7: Human resource security controls included in our GCC audits

Common weaknesses included:

- **Inadequate background screening** – appropriate background checks of staff were not performed due to a lack of policy or ineffective processes. Without these checks entities may employ unsuitable individuals to positions of trust increasing the risk of unauthorised system access, fraud and malicious activity.
- **Lack of acceptable use and confidentiality agreements** – staff were not informed of their information security responsibilities or required to acknowledge acceptable use of IT systems. This heightens the risk of misuse and it makes it more difficult to hold staff accountable in the event of a security or data breach.
- **Exit processes were not completed in a timely manner** – IT accounts were not disabled and IT assets were not returned promptly by departing staff. This may contribute to unauthorised access to entity premises, information and systems, and financial loss to the entity.
- **Lack of cyber security awareness training** – creating a culture of security requires regular training. Staff who haven't undergone information and cyber security training may not know what good security behaviours look like or how to practice them. There is a higher chance of compromise through phishing attacks or security breaches that take advantage of unsuspecting staff.

The following case studies illustrate common weaknesses in HR security.

Case study 1: Cyber security awareness training not provided

One entity did not have a cyber security awareness program despite experiencing three cyber attacks in three years. The entity attributes these attacks to phishing or poor password hygiene. We first raised this issue with the entity in 2020.

Regularly training staff to raise their awareness of cyber threats and how to respond is a key control against attacks.

Case study 2: Lack of timely notice of termination

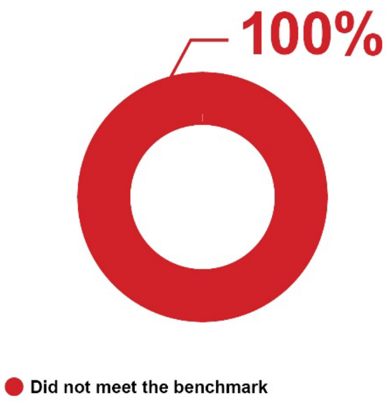
At one entity we found the exit procedures failed to notify the IT service desk of staff termination, resulting in five accounts being left enabled despite staff no longer working at the entity.

Our testing did not find any evidence of these accounts being used after termination but failing to complete exit procedures increases the risk of unauthorised access to IT systems and information.

2. Network security

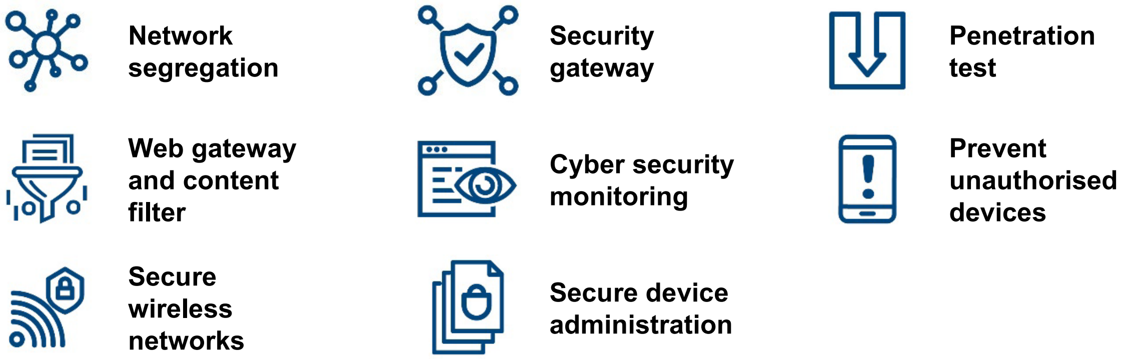
None of the entities met the benchmark in this area. Network security is important to protect the network and key systems from cyber intrusions.

Appropriate controls detect and limit the spread of cyber intrusions. Network segregation and device access controls are important for entities, and even more so if they have public facing facilities, such as libraries, that contain network access points. Cyber criminals could exploit weaknesses to gain unauthorised access and disrupt local government services.



Source: OAG

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



Network segregation

Security gateway

Penetration test

Web gateway and content filter

Cyber security monitoring

Prevent unauthorised devices

Secure wireless networks

Secure device administration

Source: OAG

Figure 9: Network security controls included in our GCC audits

Common weaknesses included:

- **Firewall rules were not reviewed** – entities were not performing planned periodic reviews of firewall rules to detect and block malicious or unauthorised network traffic.
- **Networks were not segregated** – networks have been divided into smaller segments, but controls to restrict the flow of traffic and an attacker from moving between segments were lacking. Without proper network segregation a cyber breach would be difficult to contain.
- **Unauthorised devices can gain network access** – there were no controls to detect or prevent unauthorised devices from connecting to entity internal networks. These devices could be used to spread malware or eavesdrop on communications.

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

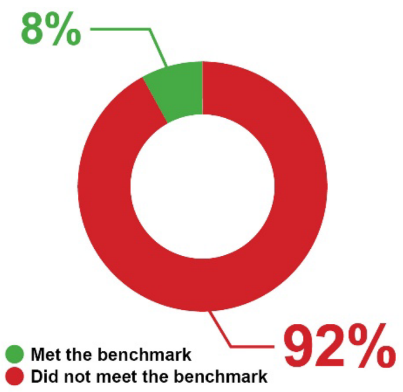
Case study 3: Increased risk of successful attack

At one entity we used a test device to scan the network and communicate with key application and database servers. This type of access if malicious could be used to attack internal systems or eavesdrop network communication. The entity did not have any controls to detect or prevent such devices on their network.

3. Access management

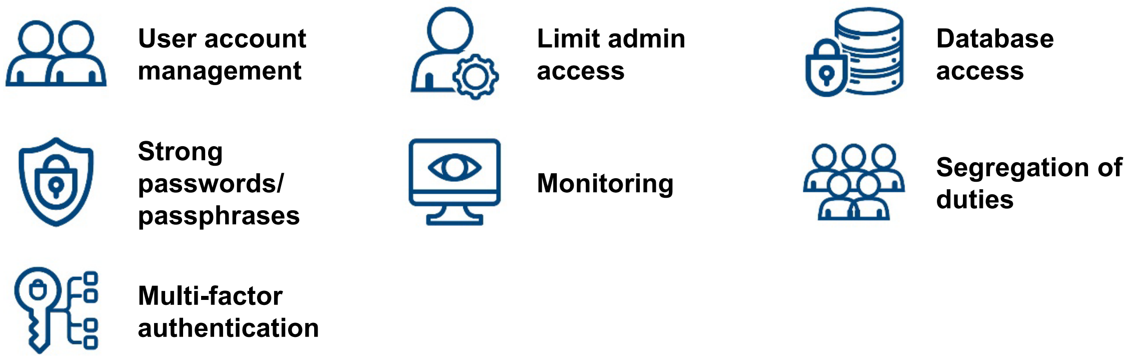
Access management is another area of concern with only one of the 12 entities meeting the benchmark. Poor access management controls increase the risk of security incidents, financial loss and reputational damage.

Entities should adopt the principal of least privilege and only allow approved employees and contractors access to systems, applications and databases. Access should be authenticated, logged and monitored.



Source: OAG

Figure 10: Percentage of entities that met/did not meet the benchmark for access management



- User account management
- Limit admin access
- Database access
- Strong passwords/ passphrases
- Monitoring
- Segregation of duties
- Multi-factor authentication

Source: OAG

Figure 11: Access management controls included in our GCC audits

Common weaknesses included:

- **Poor password configuration** – network, application and database passwords did not meet best practice increasing the risk of information loss or a data breach.
- **Multi-factor authentication (MFA) was not used** – a number of systems did not have MFA which could lead to unauthorised system access and compromise.
- **Administrator privileges were not well managed** – administrators did not have separate non privileged accounts for day-to-day tasks and administrator activity was not logged and monitored. Additionally, excessive numbers of staff were given administrator privileges. Highly privileged accounts need to be managed to protect the confidentiality, integrity and availability of key systems and services.
- **Default passwords not changed** – administrator accounts used default passwords or did not have their passwords changed for long periods, even after staff had left. If accessed, these accounts would give an attacker complete control of an entity’s network.
- **Access was not reviewed** – entities did not review user, generic, system or administrator accounts to ensure they were still required and had the appropriate privileges.

- **Activity not logged and monitored** – user activity was either not appropriately logged or monitored for malicious activity. Entities may not be able to detect unauthorised activity nor determine what information has been changed or accessed by malicious actors.

The following case studies illustrate how effective controls can prevent compromise and common weaknesses in access management.

Case study 4: MFA effectively prevented compromise

One entity had the usernames and passwords of two staff compromised through a phishing attack. However, the attacker could not gain access to systems as the entity had secured access and protected itself against further compromise through MFA.

Case study 5: Privileged access rights were not managed

An entity did not have separate day-to-day accounts for their highly privileged domain administrators who used their accounts for all activities including web access and email. Administrators should use non-privileged accounts for day-to-day activities and only use privileged accounts for those activities that require it.

This entity also allowed all its staff to have local administrator rights on their laptops which were also used for personal use. There were no controls to prevent the execution of malicious applications, scripts or untrusted macros.

This combination of control weaknesses significantly increases the entity's exposure to data breaches and compromise of its network.

Case study 6: Shared generic administrator account was not controlled

One entity allowed its vendor to use a shared generic administrator account to perform maintenance for its key business application. Instead of just-in-time access, the account was always enabled and the entity did not review activity on this account.

Use of a shared administrator account makes it more difficult for an entity to attribute actions to individuals in the event of an unintentional or malicious change. This is particularly important where the entity does not have visibility of vendor staff turnover.

Case study 7: Poor application configuration increases the risk of fraud

One entity had not configured its finance application to stop the same individual from approving purchase orders and invoices for the purchase of goods and services. Although the entity had manual controls in place, these could be bypassed.

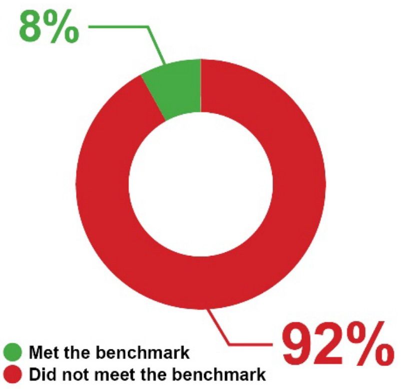
Entities' systems should be configured to segregate duties so no individual can perform all steps in the purchasing process.

4. Endpoint security

Only one of the 12 entities met the benchmark.

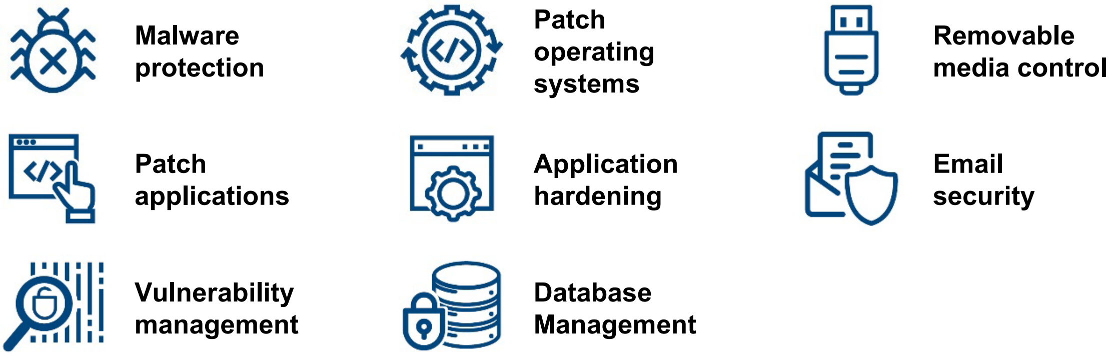
Entities need to ensure endpoints, including servers, workstations, laptops and mobile devices, are protected against cyber threats such as malware.

Malicious applications should be blocked, and regular scans done to identify vulnerabilities. Operating systems, databases and applications should be patched with updates.



Source: OAG

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



Source: OAG

Figure 13: Endpoint security controls included in our GCC audits

Common weaknesses included:

- **Vulnerability management was ineffective** – systems were not scanned, not scanned regularly or scans were misconfigured to identify vulnerabilities. Vulnerabilities were not consistently patched, or patches were not tested before being applied. Exploitation of known vulnerabilities is a common attack method used to compromise systems.
- **Outdated or no malware protection** – endpoints did not have anti-malware installed or the software was out-of-date. The risk of system compromise is higher if endpoints are not protected against cyber threats.
- **Untrusted macros were not blocked** – entities should prevent untrusted macros from running as they can contain malicious code used by attackers to spread malware. This can result in loss of services or ransomware. Macros are pieces of code that run inside applications, such as the Microsoft suite, generally to automate tasks.
- **Authenticity and integrity of emails not verified** – lack of controls or misconfigured email authentication can result in impersonation and data breaches. Controls such as domain-based message authentication (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented or not configured properly.

- **Unsupported systems** – key business systems were running software that was no longer supported by vendors and therefore not receiving updates designed to fix known vulnerabilities.
- **Unauthorised software was not controlled** – unapproved applications were not blocked. This increases the likelihood of malicious applications successfully attacking systems and information.

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

Case study 8: Lack of endpoint protection

One entity had a number of servers and workstations without anti-malware protection installed and also did not block unapproved applications from running. These controls are essential to prevent malicious software.

While the entity performed weekly system vulnerabilities scans, the scans were misconfigured and therefore failed to identify all vulnerabilities on most of the systems. Scan reports were also not reviewed to determine the cause of the failures and remediate errors.

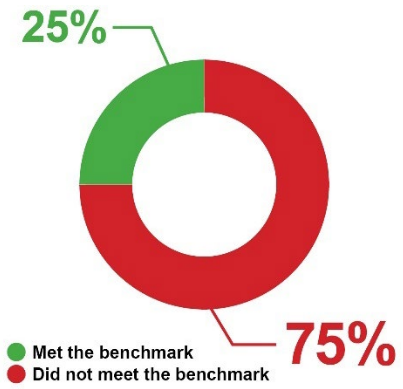
Additionally, the entity did not consistently apply or test software patches to it servers. We identified unpatched critical and high severity vulnerabilities dating back to 2005.

This entity has not effectively protected itself against known vulnerabilities.

5. Information security framework

Twenty-five percent of the entities performed well and met our benchmark. The remaining entities need to improve their information and cyber security governance. Entities should use a structured approach to mitigate security risks and protect their sensitive information and key systems.

We assessed if entities have appropriate policies and information security governance structures.



Source: OAG

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

Information and cyber security policy

Roles and responsibilities

Governance and compliance

Information classification

Assurance over cloud / third-party services

Source: OAG

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

Common weaknesses included:

- **Lack of governance** – business objectives may not be met if appropriate governance roles are not in place to oversee and direct information and cyber security.
- **Inadequate information and cyber security policies** – policies either did not exist, were out of date or did not cover key areas of information and cyber security. An entity's information security requirements and objectives are less likely to be achieved if their policies, standards and procedures are inadequate.
- **Sensitive information was not classified** – entities did not specifically identify and classify their sensitive information to ensure it is protected against accidental or unauthorised disclosure.
- **Lack of ongoing security assurance from service providers** – ineffective vendor management can result in outsourced IT services not meeting an entity's expectations and leave them vulnerable to security, financial and reputational risks.

The following case study illustrates a common weakness with information security frameworks.

Case study 9: Sensitive information was not identified and protected

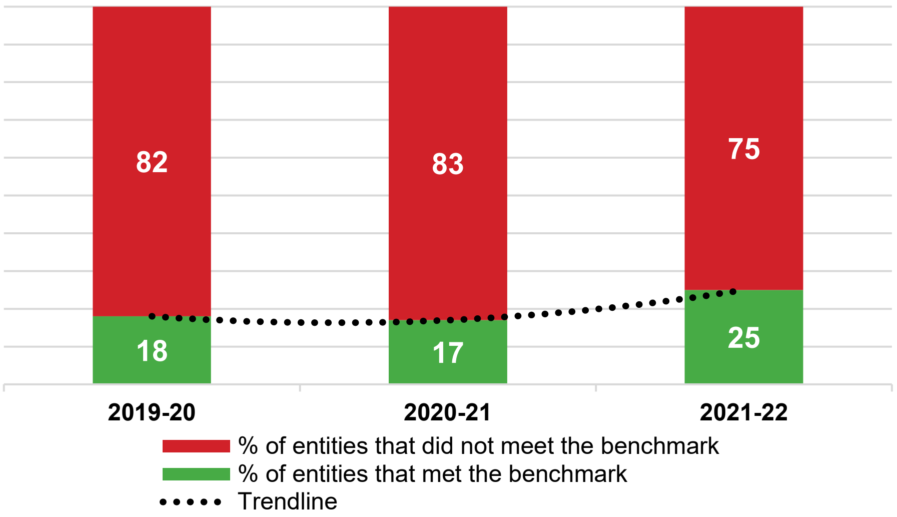
An entity did not identify the sensitivity of its information to adequately protect it. Staff are able to share sensitive entity information through their personal cloud storage services (e.g. Dropbox, iCloud, Google storage) and removeable media.

It would be difficult for the entity to keep track of their sensitive information increasing the risk of information loss.

6. Business continuity

We saw a minor improvement in 2021-22, however 75% of entities still do not have adequate and tested continuity plans. Entities should have plans to guide their response to events that disrupt their operations. These should be based on a business impact assessment and agreed recovery objectives and include:

- business continuity plans – detail how an entity can maintain operations during a disruption and return to normal operations after the event
- disaster recovery plans – provide details on restoring IT services after an outage
- cyber security incident response plans – are essential to ensure effective response and recovery after cyber security incidents. Ideally, specific response plans should be documented for common cyber security incidents such as ransomware or data breaches.



Source: OAG

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

Backup and recovery procedures

Disaster recovery plan

Business continuity plan

Cybersecurity incident response plan

Source: OAG

Figure 17: Business continuity controls included in our GCC audits

Common weaknesses included:

- **Outdated and absent continuity plans** – entity operations and service delivery to the public may experience prolonged downtimes during a disruption if plans do not align with current processes. This can result in financial loss and reputational damage.
- **Plans were not tested** – if not regularly tested, entities may not be aware of gaps in their continuity plans that could lead to data loss or extended recovery times for their key systems.
- **Restore of backups** – if backups are not tested through restoration, entities will not know if their IT systems can be recovered in a timely manner or if their data can be consistently recovered.

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

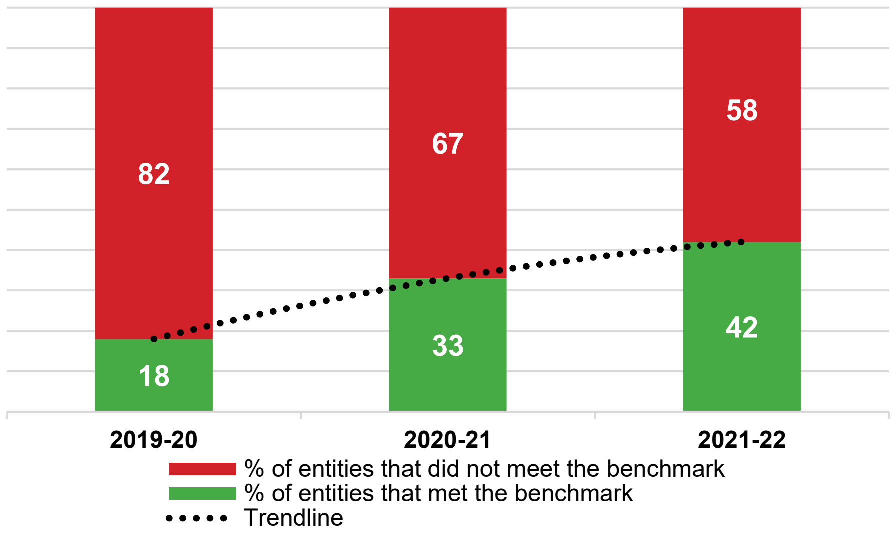
Case study 10: Cyber security incident response plan lacking

In 2022, an entity's staff account was compromised and used to instigate a phishing attack on third parties. The entity did not have a cyber security incident response plan to coordinate a response and communicate with impacted third parties. We had previously informed the entity to develop a plan in 2021.

A documented cyber security response plan could have helped the entity respond to the incident more efficiently.

7. IT operations

IT operations was another area of improvement in 2021-22 with 42% of entities meeting our benchmark. This category has shown slow but consistent improvement over the years.



Source: OAG

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

We assessed if entities had a formal incident management process and managed supplier contracts and IT assets. Entities should have robust processes to ensure:

- IT incidents are resolved within agreed service levels
- the lifecycle of IT assets is managed and assets are disposed of securely
- vendors have appropriate contracts and performance is monitored.

IT assets lifecycle management

Supplier performance management

Incident and problem management

Source: OAG

Figure 19: IT operations controls included in our GCC audits

Common weaknesses included:

- **Supplier performance was not monitored** – entities may not become aware when IT suppliers fail to fulfil performance requirements and deliver substandard services. This can compromise entity systems and impact entity service delivery.
- **IT asset registers were poorly maintained and stocktakes not performed** – inadequate management of IT assets can result in their loss or theft, leading to financial loss and reputational harm for the entity.
- **Incident procedures were not developed** – incidents may not be resolved in line with expectations and the root cause of incidents may not be adequately addressed.

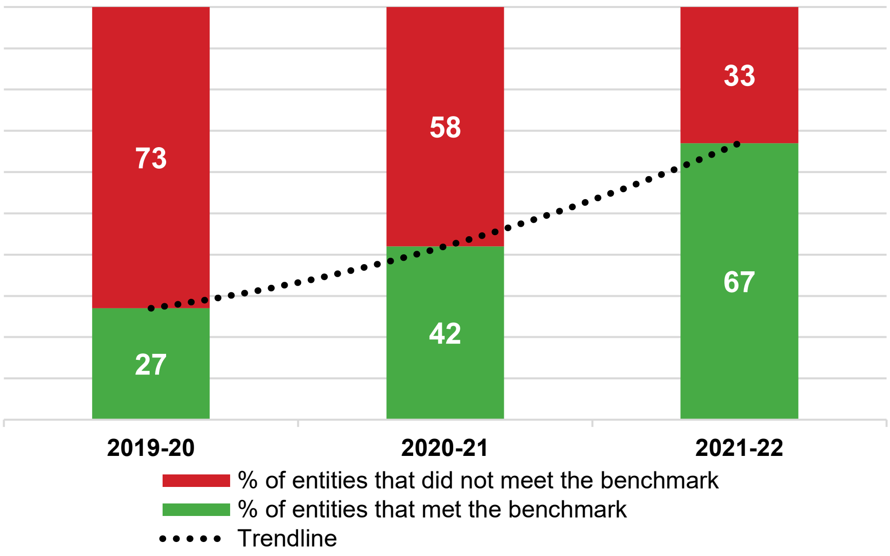
The following case study illustrates a common weakness in IT operations.

Case study 11: Lack of disposal policy increases risk of information disclosure

An entity who uses a vendor to dispose of its IT assets, which may contain entity information, had not defined expectations for the assets secure disposal. There is a risk that entity information may be inadvertently or maliciously disclosed, causing damage to the entity and members of its community.

8. Risk management

More than half (67%) of entities met our benchmark in this area in 2021-22 showing a positive trend. Senior management should understand information and cyber security risks facing their entities and prioritise remediation.



Source: OAG

Figure 20: 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.

Risk management policies

Risk evaluation and treatment

IT risk register

Risk reporting

Source: OAG

Figure 21: Risk management controls included in our GCC audits

Common weaknesses included:

- **Outdated or absent risk management policies** – entities may not identify and treat known and emerging risks.

- **IT risk registers were not maintained** – entities either had no risk register or key information such as risk ratings, treatment controls and risk owners were not recorded in the risk register. Entities may not be effectively addressing their known and emerging risks.

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

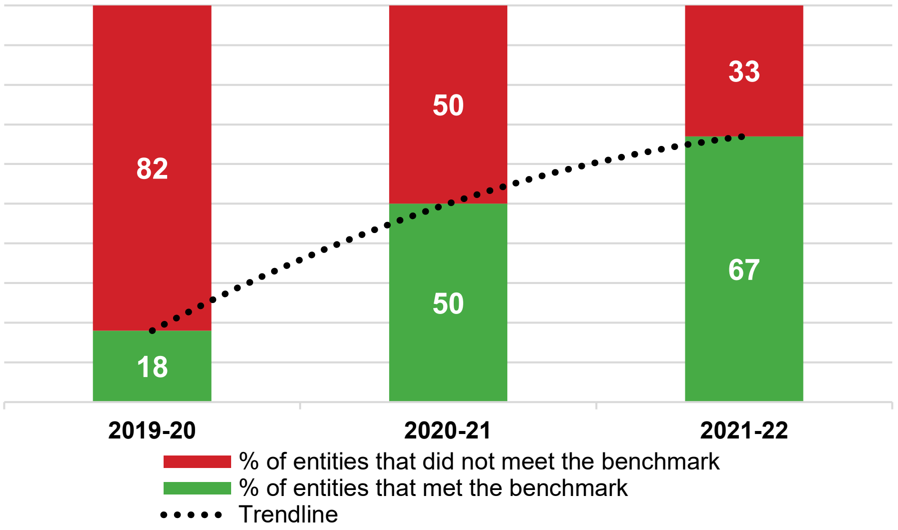
Case study 12: Senior management unaware of cyber risks

An entity did not report significant cyber security risks to senior management. It also did not review existing risks and, for some risks, treatment actions were not recorded.

As a result, these risks may not be appropriately prioritised and remediated.

9. Change management

In 2021-22, we saw an improvement in change management with 67% of entities meeting the benchmark, a 49% increase from 2019-20.



Source: OAG

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

We reviewed if entities had processes to authorise, test, implement and monitor changes to their IT systems. Well operating change management processes allow timely implementation of changes and reduce the risk to business operations.

Change management procedures

Emergency changes

Change evaluation

Production, test and development environments

Source: OAG

Figure 23: Change management controls included in our GCC audits

Common weaknesses included:

- **Changes were not documented** – changes to critical systems were not documented or documentation did not contain sufficient information to properly risk assess the changes. This increases the likelihood of unplanned outages.
- **Change management processes were not documented** – increasing the likelihood of errors, delays and failures in implementing changes.

The following case studies illustrate common weaknesses in change management.

Case study 13: Change documentation

One entity bulk changed the active/inactive status of 4,000 suppliers. The entity did not document the approval for these changes and there was no record of who performed them. Without appropriate documentation it is difficult to know if these changes were authorised or correctly implemented.

This entity may be at an increased risk of erroneous or fraudulent supplier payments.

Case study 14: Change monitoring

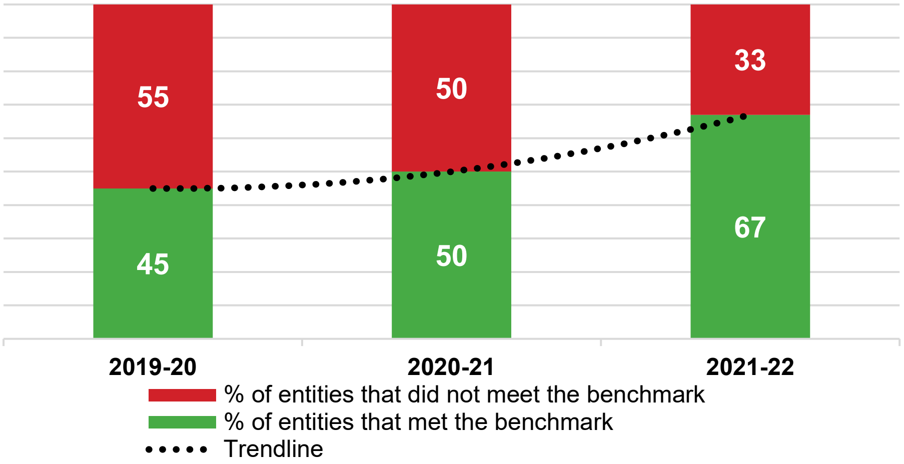
An entity implemented a control to alert its staff when a third-party vendor accesses its financial application to make changes. However, the entity does not review these notifications to determine if changes were requested or implemented as expected.

Without verification and review of system changes, including those made by a third party, there is an increased risk of unauthorised or erroneous changes.

10. Physical security

Physical security also saw improvement with 67% of entities meeting the benchmark. It is important to maintain secure access and environmental controls in server rooms, whether on premises or managed through a third-party vendor.

We assessed if cooling, power, fire detection and suppression systems were in place to protect entities' IT hardware from hazards. We also assessed if physical access to server rooms was restricted and monitored. Where server rooms were managed by third-parties or entities used infrastructure as a service, we tested how entities gain comfort that vendor controls were appropriate.



Source: OAG

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

Source: OAG

Figure 25: Physical security controls included in our GCC audits

Common weaknesses included:

- **Equipment poorly located** – we found instances where IT hardware was not located in suitably controlled environments, increasing the risk of system failure, outages and decreased performance. Without appropriate controls, entities will be unaware if equipment is operating outside manufacture's recommended parameters.
- **Access to server rooms was not monitored** – access and entry logs should be reviewed and monitored for instances of unauthorised entry to reduce malicious or unintentional damage to IT equipment.
- **Server rooms were left unlocked** – if access is not controlled it can lead to unauthorised or inappropriate access to key systems and damage to infrastructure.

The following case studies illustrate common weaknesses in physical security.

Case study 15: Doors not secured

At one entity we found the back door to the office and records room were kept unlocked during the day despite being publicly accessible. Cash takings were also left in an unlocked safe. These weaknesses increase the likelihood of unauthorised access and theft.

Case study 16: Network equipment located in a staff toilet block

At one entity a network equipment rack was located in a staff toilet block without any temperature and humidity controls, and above head height.

There is a risk of equipment failure and decreased performance leading to system downtime. The location of the equipment high on a wall in the toilet block also represents a health and safety risk.

Recommendations

1. Human resources security

Local government 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.

2. Network security

Entities should:

a. implement secure administration processes for network devices

b. regularly review their network security controls through penetration tests

c. segregate their network

d. limit unauthorised devices from connecting to their network

e. adequately secure wireless networks.

3. 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.

4. Endpoint security

Entities should:

a. implement effective controls against malware

b. promptly identify and address known vulnerabilities

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 network

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

g. review and harden server and workstation configurations.

5. Information security framework

Entities should:

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

b. conduct regular assessments or gain comfort through assurance reports 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. IT operations

Entities should:

a. implement appropriate IT incident management processes

b. regularly monitor supplier performance

c. perform regular reviews of inventory assets

d. have formal service level agreements with suppliers.

8. 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.

9. Change management

Entities should:

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

b. assess and test changes before implementation to minimise errors

c. maintain change control documentation

d. implement controls to detect unauthorised changes.

10. 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 their data centres appropriately.

Under section 7.12A of the *Local Government Act 1995*, the 53 audited entities are required to prepare an action plan to address significant matters relevant to their entity for submission to the Minister for Local Government within three months of this report being tabled in Parliament, and for publication on the entity's website. This action plan should address the points above, to the extent they are relevant to their entity.

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

Auditor General’s 2023-23 reports

Number	Title	Date tabled
18	Opinions on Ministerial Notifications – Tourism WA’s Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
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