Western Australian
Auditor General's Report

Information Systems Audit Report 2022 – Local Government Entities

Report 22: 2021-22
28 June 2022

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Svetla Alphonso
Ben Goodwin
Khubaib Gondal
Michael Chumak
Sayem Chowdhury
Reshma Vikas
Sooraj Suresh
Tuck Owyong
Karen Telford
Paul Tilbrook
Fareed Bakhsh

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.

© 2022 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in
whole or in part provided the source is acknowledged.

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

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

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report 2022 – Local Government Entities

Report 22: 2021-22
June 2022

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEM AUDIT REPORT 2022 – LOCAL GOVERNMENT ENTITIES

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

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

This is the third local government annual information systems audit report by my Office. The report summarises the results of our 2021 annual cycle of information systems audits across a selection of 45 local government entities.

I wish to acknowledge the entities' staff for their cooperation with these audits.

CAROLINE SPENCER
AUDITOR GENERAL
28 June 2022

Contents

Auditor General's overview

This report summarises important findings and recommendations from our 2020-21 annual cycle of information systems audits at 45 local government entities (entities).

Entities rely on information systems to operate and deliver services to their communities. In doing so, they collect and store vast amounts of information about their residents and operations. As information and cyber security threats continue to evolve, it is increasingly important that entities implement appropriate controls to protect their valuable information and systems. My November 2021 audit report[1] on cyber security highlighted the need for entities to improve their management of cyber security risks and this year's general computer controls (GCC) audits at entities show that information security remains a significant area of concern.

Like last year, none of the 12 entities where we performed capability maturity assessments met our benchmark for information security and none of the entities met our expectations across all 6 control categories. While we saw some improvements in the management of IT risks, physical security and IT operations, change control showed the most progress.

Included in this report are case studies which highlight how weak controls can potentially compromise entities and result in system breaches, loss of sensitive and confidential information and financial loss. Entities need to continuously review and improve their practices to establish robust safeguards and enhance their resilience against cyber threats. Complex networks and systems require smaller entities to also dedicate resources to manage their information and cyber security.

Entities should use the recommendations in this report to address weaknesses in their information systems controls and improve their capability maturity. Given the nature of findings this year, I have chosen again not to identify the audited entities.

[1] Auditor General for Western Australia, *Cyber Security in Local Government*, Report 9: 2021-22, November 2021.

Introduction

Local government entities (entities) rely on information systems to prepare their financial statements and to deliver a wide range of services to their communities. Our general computer controls (GCC) audits assess if entities have effective system controls in place to support the confidentiality, integrity and availability of their IT systems and financial reporting. These audits are performed as an integral part of, and inform, our financial audit program.

This report summarises the GCC audit findings reported to 45 entities for 2020-21. For 12 of these entities, generally medium to large, we also performed capability maturity assessments. A GCC audit with a capability maturity assessment is the most comprehensive information systems audit we undertake. We use these findings to inform our financial audit risk assessment and work program for the sector.

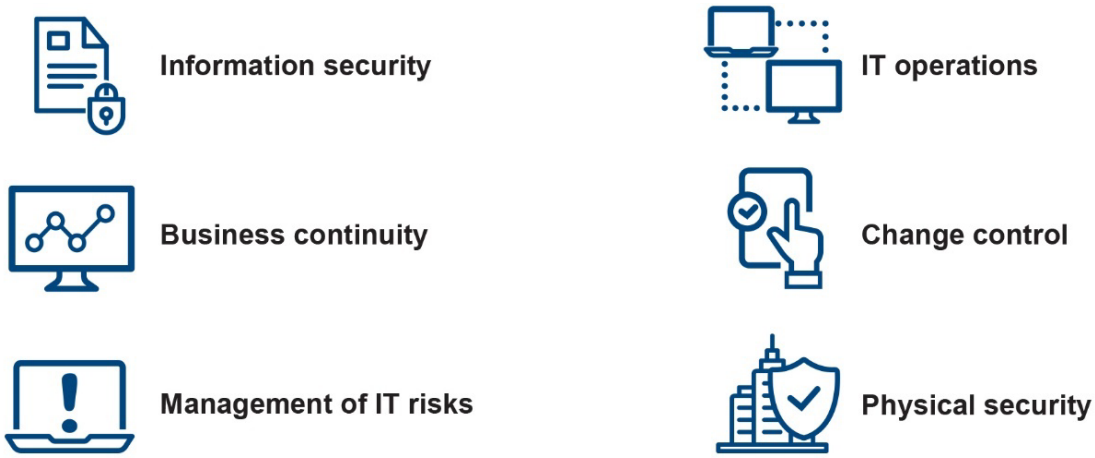
For our capability maturity assessments, we asked the 12 entities to self-assess against the provided capability maturity model. We then compared their results to ours (which were based on the results of our GCC audits). These assessments are a way to see how well-developed and capable entities' established IT controls are.

For the remaining 33 entities, our contract audit firms or our financial audit teams examined the GCCs but did not undertake capability maturity assessments. Information system findings identified during these audits are included in this report.

The methodology we have developed for our GCC audits is based on accepted industry good practice. Our assessment is also influenced by various factors including:

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

We focused on the following 6 categories (Figure 1) for both our GCCs and capability maturity assessments.



Source: OAG

Figure 1: GCC categories

Throughout the report we have included case studies that illustrate the significant impact poor controls can have on entities.

Conclusion

We reported 358 control weaknesses to 45 entities this year, compared to 328 weaknesses at 50 entities last year. Ten percent (37) of this year's weaknesses were rated as significant and 71% (254) as moderate. These weaknesses represent a considerable risk to the confidentiality, integrity and availability of entities' information systems and need prompt resolution.

Fifty-six percent (202) of the findings were unresolved issues from last year. Entities need to address these weaknesses to reduce the risk of their systems and information being compromised.

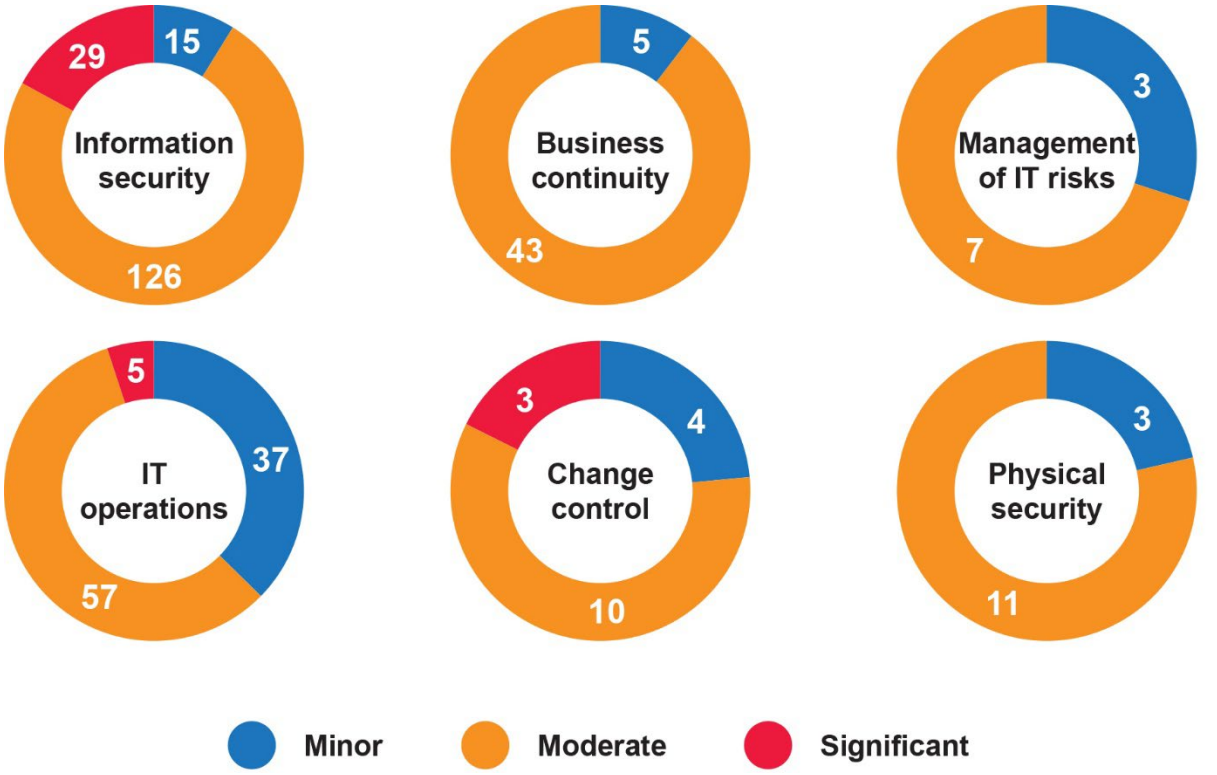
None of the 12 entities that had capability maturity assessments met our expectations across all 6 control categories, a similar finding to last year. Information security remains a significant risk again this year and needs urgent attention. Compared to 2019-20, there have been some improvements in change control, management of IT risks, physical security and IT operations. However, entities need to improve in all 6 control categories.

What we found: General computer controls

In 2020-21, we reported 358 findings to the 45 entities we audited. We reported the weaknesses we found to each entity in a management letter. As management letters are often made public, we removed any sensitive technical details which could increase an entity's risk of cyber attacks. To assist entities to address weaknesses we reported these sensitive details to them in separate confidential letters. Entities generally agreed to implement our recommendations.

Figure 2 summarises the distribution and significance of our findings across the 6 control categories.

Like last year, we rated most of our findings as moderate. Entities that fail to address these moderate risks can, over time, become more exposed to vulnerabilities. We have included in this report specific case studies to highlight how weak controls can potentially compromise entities' systems.



Source: OAG

Figure 2: Distribution and significance of GCC findings in each control category

What we found: Capability assessments

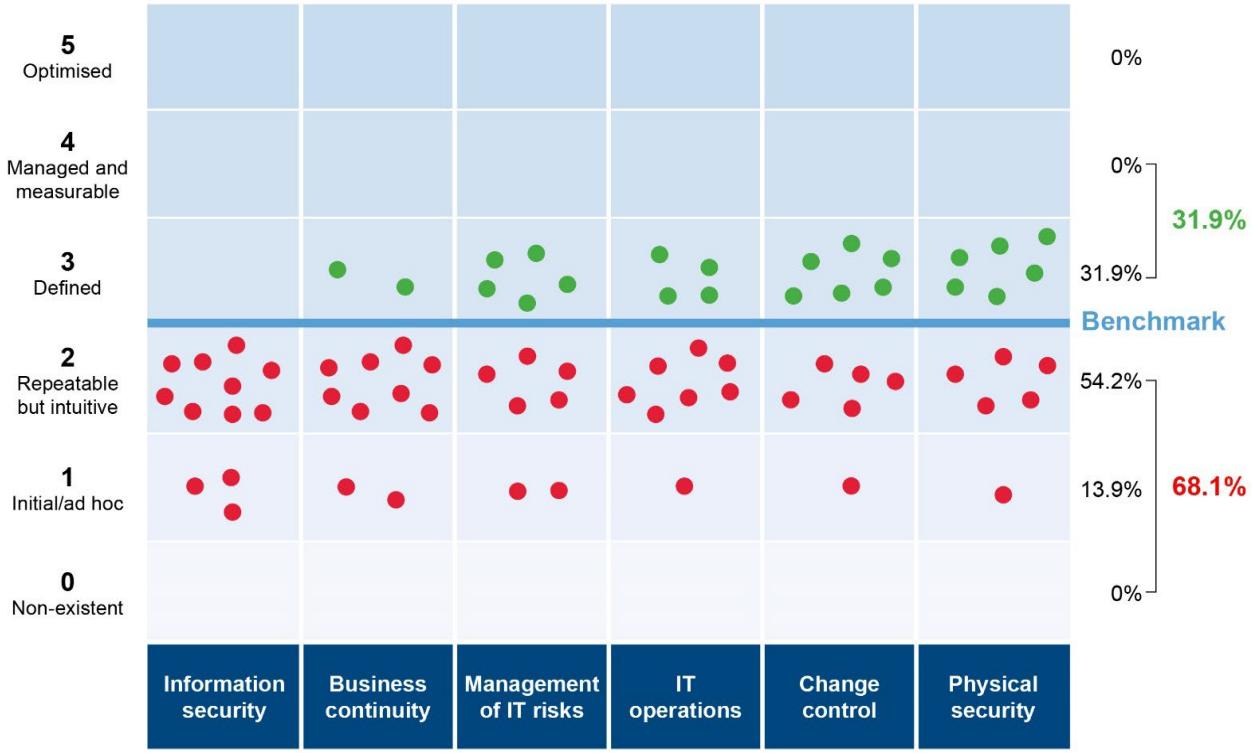
We conducted in-depth capability maturity assessments at 12 entities. We used a 0 to 5 rating scale[2] (Figure 3) to evaluate each entity's capability maturity in each of the 6 GCC categories. Our model allows us to compare entity results from year to year. We expect entities to achieve a level 3 (Defined) rating or better across all 6 categories.

Source: OAG

Figure 3: Rating scale and criteria

Figure 4 shows the results of our capability assessments across all 6 control categories for the 12 entities we assessed in 2020-21.

[2] The information within this maturity model assessment is derived from the criteria defined within COBIT 4.1, released in 2007 by ISACA.



Source: OAG

Figure 4: 2020-21 capability maturity model assessment results

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

Category	2020-21 %		2019-20 %
Information security	0	—	0
Business continuity	17	↓	18
Management of IT risks	42	↑	27
IT operations	33	↑	18
Change control	50	↑	18
Physical security	50	↑	45

Source: OAG

Table 1: Percentage of entities rated level 3 or above

None of the 12 entities met our expected benchmark (level 3 Defined) across all control categories.

There were some improvements in the management of IT risks, IT operations, change control and physical security, however, most entities still fell below our benchmark. Information security remains a significant concern, with all entities below our benchmark and not able to demonstrate adequate controls. A lack of robust controls can expose entities and impact critical services provided to the public.

Information security

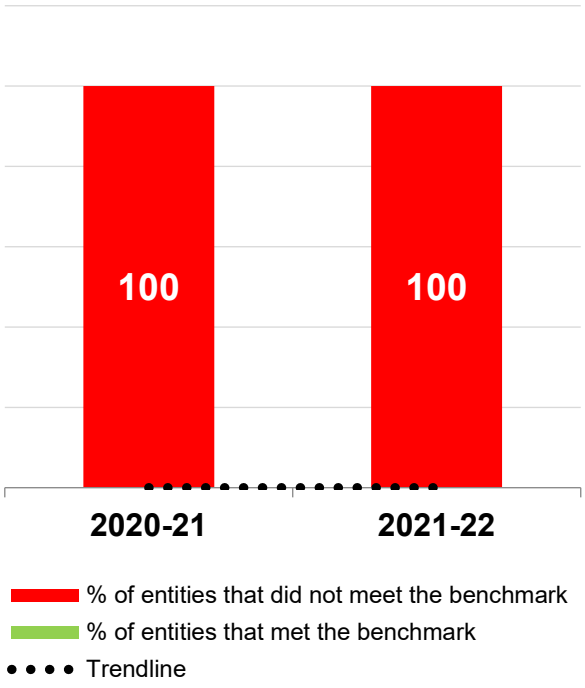
Cyber intrusions are becoming more sophisticated and frequent. Transitioning to digital services to achieve efficiencies increases the risk profile of many entities. Protection of sensitive and critical information that entities hold within their financial and operational systems should be managed with the highest priority using better practice information security controls to mitigate risks.

Our GCC audits and capability maturity assessments assess against better practice controls for information and cyber security. Figure 5 lists some of these controls.

Source: OAG

Figure 5: Information security – Better practice controls

None of the 12 entities met our benchmark for information security either because they did not have documented policies, processes and controls or they were not effective (Figure 6). Entities have a responsibility to implement adequate and robust controls to protect key systems and information.



Source: OAG

Figure 6: Information security – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Inadequate information and cyber security policies** – policies did not sufficiently cover key areas of information and cyber security or were out of date.
- **Multifactor authentication not used** – a number of systems did not have multifactor authentication to strengthen access.
- **Administrator privileges not managed well** – administrators did not have separate unprivileged accounts for normal day to day tasks. Limiting privileges and separating administrative accounts are important mitigations against network and system compromise.
- **Vulnerability management is not effective** – entities did not have appropriate processes to identify and address vulnerabilities, which increases the risk of compromise.
- **Network segregation not appropriate** – networks were not segregated to limit and contain the impact of a compromise. Partitioning the network into smaller zones and limiting the communication between these zones is an important control.
- **Unauthorised device connectivity** – there are a lack of controls to detect or prevent unauthorised devices from connecting to entity internal networks. These devices can serve as an attack point and spread malware or listen in on network traffic.
- **Emails not protected** – entities did not have controls to ensure the integrity and authenticity of emails to reduce the likelihood of successful phishing attacks. Controls such as domain-based message authentication reporting and conformance (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented to prevent email impersonation.

- **Lack of data loss prevention controls** – no processes to detect or block unauthorised transfers of sensitive data outside of the entities.

The importance and potential impact of common information and cyber security weaknesses are illustrated in the following case studies.

Case study 1: No policy to manage information and cyber security

Information security policy

One entity did not have a policy to manage cyber and information security. This means, systems or services may not meet security expectations of senior management and the entity may fail to achieve its objectives.

Adequate and clear policies are needed to ensure the security of information systems.

Case study 2: Weak password results in a network compromise

Password

One entity experienced a security breach when a cybercriminal was able to guess a weak password on an account used to access a public facing server through remote desktop protocol (RDP). A lack of network segregation allowed the attacker to access other parts of the network, gain privileged access to the domain controller and maliciously encrypt servers and information.

The use of strong password/passphrases, network segregation and multi-factor authentication reduce the risk of compromise.

Case study 3: No controls to mitigate malware infections

Malware protection

One entity had anti-malware protection installed on some servers but not others. It did not have application whitelisting and blocking in place or only allow trusted macros. These controls prevent delivery and execution of malicious programs.

Without appropriate controls to protect systems against malware, there is an increased risk of compromise to the confidentiality, integrity and availability of entity information or data.

Case study 4: Default domain administrator account is not controlled

Limit admin privilege

One entity shared the highly privileged default domain administrator account with individuals in different business units and had not changed the account password since 2005. The account was also heavily used for day to day operations and services, instead of using separate dedicated service accounts.

Inappropriate management of the account increases the risk that the entity will not be able to hold individuals to account for unauthorised modifications to its systems and information.

Case study 5: Poor management of technical vulnerabilities

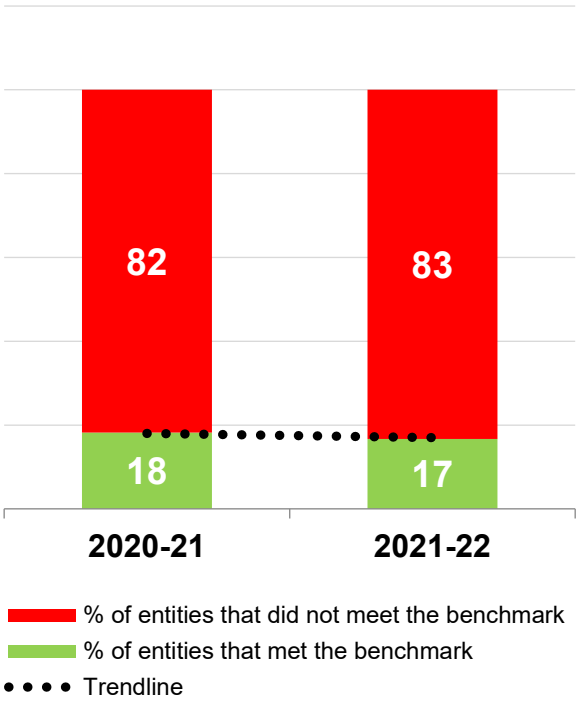
Vulnerability management

An audited entity did not have a process to manage technical vulnerabilities and system currency. It had not tested the adequacy of its external network controls to detect and prevent cyber attacks. Its process to apply software patches was also not operating well as we identified critical and high severity vulnerabilities dating back to 2013 that had not been patched.

Without effective procedures and processes to manage technical vulnerabilities in a timely manner, entities leave their IT systems exposed to malicious attackers. This could result in unauthorised access and system compromise.

Business continuity

There was no material change from last year with only 2 of the 12 entities (17%) meeting our benchmark in this category (Figure 7). Business continuity and disaster recovery plans help entities to promptly restore key business functions and processes during or after an unplanned disruption. Without these plans, entities could suffer extended outages and disruption to the delivery of important services to their communities.



Source: OAG

Figure 7: Business continuity – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Lack of business continuity and disaster recovery plans** – entities did not have appropriate business continuity and disaster recovery plans, or they were out-of-date.
- **Disaster recovery plans not tested** – without appropriate testing of disaster recovery plans, entities cannot be certain the plan will work when needed.

Documented up-to-date business continuity and disaster recovery plans help entities to promptly recover critical information systems in the event of an unplanned disruption to their operations and services. The plans should identify critical business functions and IT systems along with their recovery time objectives.

The effectiveness of these plans should be periodically tested to identify improvements where required. Tests can also be used to check that key staff are familiar with the plans and their specific roles and responsibilities in a disaster situation.

The following case study illustrates common weaknesses in recovery procedures.

Case study 6: Configuration backups are not performed

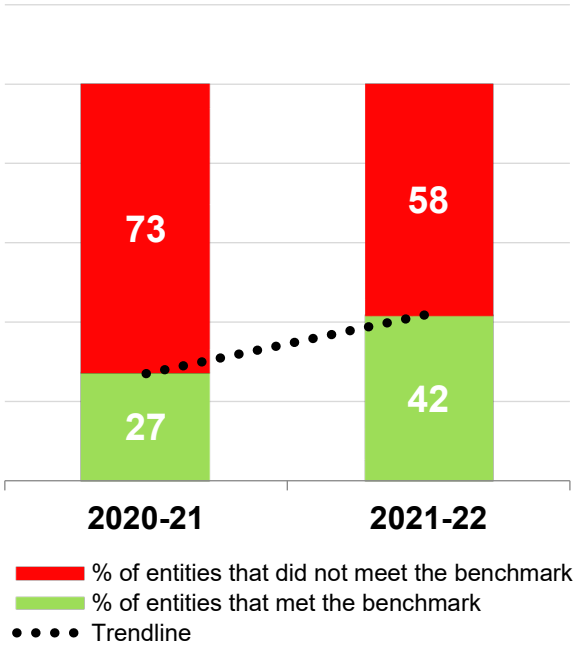
Configuration backups

An audited entity did not backup the configuration of its firewall which protects its network from cyber attacks. In the event of an emergency, the entity may not be able to recover its firewall in a timely manner, which will impact delivery of services and security of its network.

Management of IT risks

Forty-two percent of entities met our benchmark for this category in 2020-21, compared to 27% last year (Figure 8).

Entities should be aware of information and cyber security risks associated with IT including operational, strategic and project risks. All entities should have risk management policies and processes to assess, prioritise, address and monitor the risks that affect key business objectives.



Source: OAG

Figure 8: Management of IT risks – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Out-of-date policies and processes to identify, assess and treat IT risks** – without appropriate policies and processes entities cannot effectively manage their IT risks.
- **Inadequate risk registers** – risk registers did not record controls and treatment action plans and risk ratings were not appropriately assessed.

Without IT risk management policies and practices to identify, mitigate and manage threats within reasonable timeframes, entities may not meet their business objectives to deliver key services to their communities.

The following case study illustrates that entities need processes to identify their risks.

Case study 7: Entity is not aware of its information and cyber risks

Information and cyber security risk management

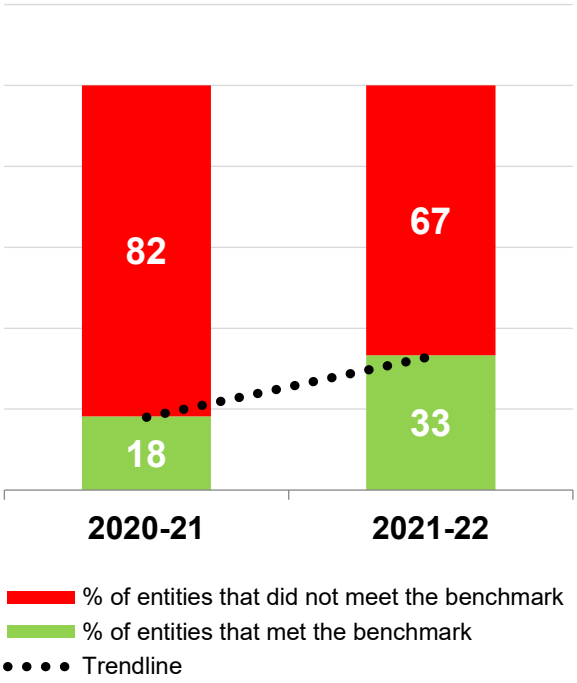
An audited entity maintained other corporate and financial risks, but it did not have a process to identify and address its cyber security risks.

The entity is at an increased risk of information and cyber security breaches.

IT operations

Entities improved in this category with 33% meeting our benchmark in 2020-21 (Figure 9). However, we identified similar weaknesses to those highlighted in last year's report.

IT operations maintain and support the delivery of entity services. Clearly defined and effectively managed IT operations support IT infrastructure that can withstand and recover from errors and failures.



Source: OAG

Figure 9: IT operations – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Processes are not defined** – a lack of or out of date procedures to support day to day operations, such as incident and problem management.
- **Inadequate monitoring of events** – entities did not have policies and procedures to monitor event logs. System logs provide an opportunity to detect suspicious or malicious behaviour in key business applications.
- **Supplier performance not monitored** – supplier performance was not reviewed to identify and manage instances of non-compliance with agreed service levels.
- **Background checks for new starters were not performed** – staff in privileged IT positions did not go through background checks (e.g. police clearance).
- **Access was not reviewed** – regular checks were not done to validate users had the level of access to systems applicable to their role or function, and revoke user access upon termination.

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

Case study 8: Contractor access was not revoked in a timely manner

User account management

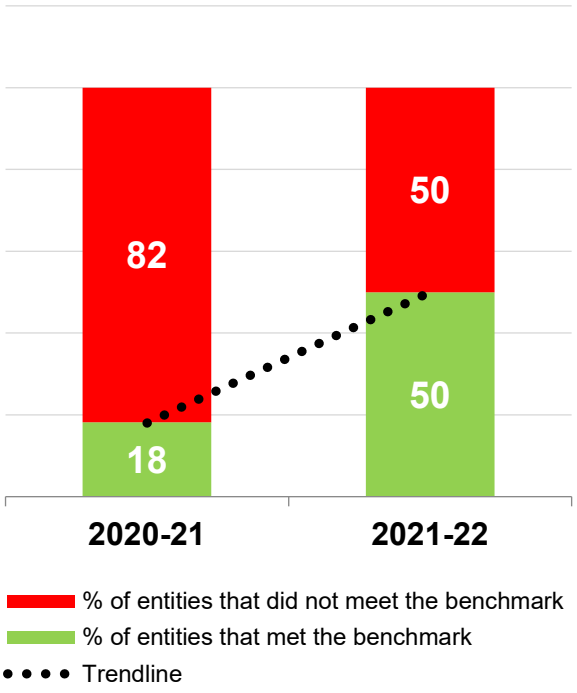
One entity did not have a central record of contract staff and therefore could not easily assess if their network access was appropriate. We sampled 13 active accounts and found that 8 belonged to terminated contract staff who no longer worked with the entity.

Poor processes to manage contract staff increases the risk of unauthorised access to the entity's IT systems and information.

Change control

Fifty percent of entities met our benchmark in 2020-21 (Figure 10), the largest improvement across the 6 control categories. This is 1 of the 2 categories where at least half of the entities met the benchmark and it is pleasing to see significant year on year improvement.

We reviewed entities' approaches to managing IT changes to minimise the risks and impacts to stakeholders. We covered change authorisation, testing, implementation and outcomes. An overarching change control framework ensures changes are made consistently and reliably.



Source: OAG

Figure 10: Change control – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Change processes not followed** – changes to critical systems did not follow change procedures. If formal procedures are not followed, there is a risk changes may be applied inconsistently resulting in unplanned system downtime and interruption to critical services.

- **Change management processes not documented** – without documented processes, changes made to IT infrastructure can adversely affect entities' operations leading to unplanned or excessive system downtime.
- **Changes were not assessed prior to implementation** – allowing significant changes without appropriate scrutiny or approval increases the risk of system outages.

Without appropriate change control, entities risk compromising the integrity of their systems and information. This can lead to excessive outages and downtime to key systems and impact their delivery of services.

The following case study illustrates the risks when IT changes are not controlled and monitored.

Case study 9: Poor change management practices could result in financial system instability

Change management

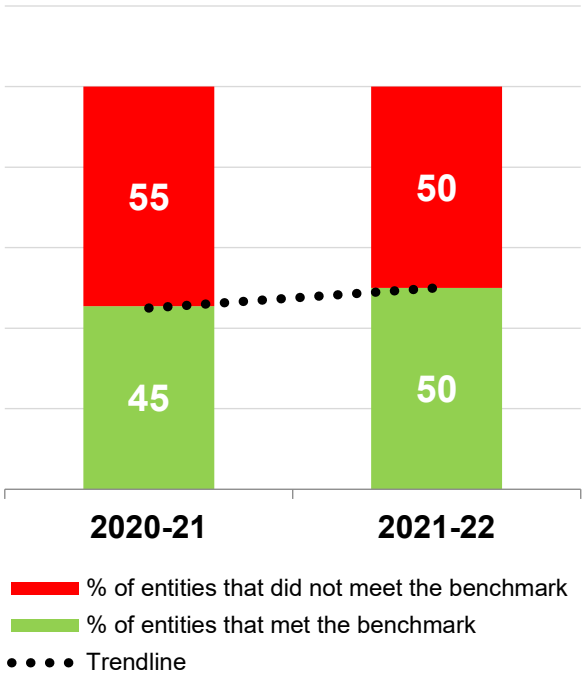
One entity made changes to its financial system without testing the impact on system integrity and availability in an independent test environment. Uncontrolled changes can have significant unintended consequences to systems and the delivery of key services.

These changes were also not recorded, contrary to the entity's change management policy. Failure to record changes increases the effort required to respond, recover and restore business as usual operations.

Physical security

There was a small improvement in physical security with half the entities meeting our benchmark this year (Figure 11).

IT systems are housed in purpose-built server rooms, which must have restricted access and adequate cooling and power. We reviewed if IT systems were protected against potential environmental hazards and tested access restrictions to ensure only authorised individuals could access the server rooms.



Source: OAG

Figure 11: Physical security – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Combustible and non-essential items were stored in server rooms** – the risk of outages is higher if server rooms are not appropriately maintained.
- **Unnecessary access to server rooms** – staff and contractors were assigned access to server rooms that they did not require and visitor access to server rooms was not logged. Lack of controlled access increases the risk of system outages and compromise from unauthorised access.
- **Fire suppression systems were not installed** – without appropriate fire suppression systems, IT infrastructure is likely to be damaged in the event of a fire.

The following case study illustrates the risk of server room outages if not protected against physical and environmental hazards.

Case study 10: Poor management of server rooms

Physical security

One entity stored combustible materials such as furniture and cardboard boxes in their server room. In addition, an excessive number (114) of people had access to the server room and a visitor log was not maintained.

There is an increased risk of accidental or deliberate damage and unauthorised access to systems.

Recommendations

1. Information security

a. Senior executives should implement appropriate policies and procedures to ensure the security of information systems and support their entity business objectives.

b. Management should ensure good security policies and practices are implemented and continuously monitored for control areas identified in Figure 5, including:

i) patching and vulnerability management

ii) application hardening and control

iii) implement technical controls to prevent impersonation and detect/prevent phishing emails

iv) strong passphrases/passwords and multi-factor authentication

v) limit and control administrator privileges

vi) segregate network and prevent unauthorised devices

vii) secure cloud infrastructure, databases, email and storage, and know clearly 'who' they are handing entity and citizen data to through their use of cloud services

viii) cyber security monitoring, intrusion detection and protection from malware.

2. Business continuity

Entities should have appropriate business continuity, disaster recovery and incident response plans to protect critical systems from disruptive events. These plans should be periodically tested.

3. Management of IT risks

Entities should:

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

b. ensure IT risks are identified, assessed and treated within appropriate timeframes. Senior executives should have oversight of information and cyber security risks.

4. IT operations

Entities should implement policies and procedures to guide key areas of IT operations such as incident management and supplier performance monitoring.

5. Change control

Approved change control processes should be consistently applied when making changes to IT systems. All changes should go through planning and impact assessment to minimise the occurrence of problems. Change control documentation should be current and approved changes formally tracked.

6. Physical security

Entities should develop and implement physical and environmental control mechanisms to prevent unauthorised access, or accidental or environmental damage to IT infrastructure and systems.

Under section 7.12A of the *Local Government Act 1995*, the 45 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 3 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 that they are relevant to their entity.

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
21	Delivering School Psychology Services	23 June 2022
20	Fraud Risk Management - Better Practice Guide	22 June 2022
19	Forensic Audit – Construction Training Fund	22 June 2022
18	Opinion on Ministerial Notification – FPC Sawmill Volumes	20 June 2022
17	2022 Transparency Report Major Projects	17 June 2022
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impact	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

@OAG_WA

Office of the Auditor General for
Western Australia