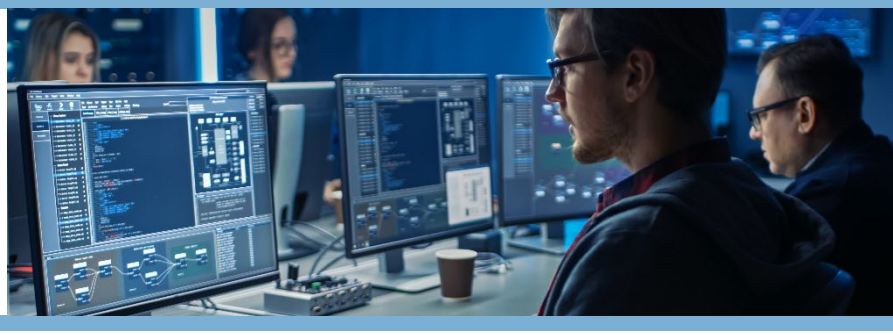
Western Australian
Auditor General's Report



Information Systems Audit Report 2022 – State Government Entities

Report 13: 2021-22
31 March 2022

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Paul Tilbrook
Fareed Bakhsh
Michael Chumak
Ben Goodwin
Khubaib Gondal
Reshma Vikas
Sayem Chowdhury
Svetla Alphonso
Ghulam Wahid
Tuck Owyong
Izak de Vries
Xuan Ong

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.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report 2022 – State Government Entities

Report 13: 2021-22
March 2022

This page intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2022 – STATE GOVERNMENT ENTITIES

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 14th 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
31 March 2022

Contents

Auditor General's overview

This report summarises the results of the 2020-21 annual cycle of information systems audits for State government entities and tertiary institutions in the Western Australian public sector. These audits were performed between February 2021 and February 2022.

Global trends show more organisations are experiencing information and cybersecurity attacks. Compromise of supply chains, ransomware, and exploitation of vulnerabilities remain high. Government entities are not immune to these attacks as they deliver key services and hold valuable citizen data. As internal and external threats continue to evolve it is important that entities constantly improve the key controls that protect their information systems and IT environments from information and cybersecurity risks.

This year's audits show many entities are still not addressing audit findings quickly, with nearly half of all findings previously reported remaining unresolved by the following year's audit. It is also disappointing that many entities continue to have poor controls over information security. Only 50% of entities met our benchmark in this area, with no noticeable improvement from the previous year. These results contributed to the highest number of qualified opinions on financial statements, controls or key performance indicators ever reported by my Office in 2020-21[1]. Effective general computer controls support entities to achieve their objectives and defend against information systems' compromise and data breaches.

It is promising to see more entities this year met our benchmark consistently in all 6 general computer control categories, building on a positive trend. Nine entities compared to 5 last year. To further help entities, we have modernised our capability maturity model for use in our 2022 audits. The new model builds upon the previous model and provides increased guidance on information and cybersecurity controls (Appendix 1).

I encourage entities to take note of the recommendations in this report as they work to improve their general computer controls, ensuring information security remains a heightened area of focus. This is an area that without constant effort, entities will go backwards in their security environment, exposing their systems, their operations and citizen data to harm.

[1] Western Australian Auditor General's Report, Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities, Report 10: 2020-21

Introduction

This is our 14th report on the audits of State government entities' general computer controls (GCC). The objective of our GCC audits is to determine whether entities' computer controls effectively support the confidentiality, integrity and availability of information systems. These controls are important to protect information systems and IT environments from information and cybersecurity risks.

For 2020-21, we reported GCC findings to 54 State government entities (Table 1). We provided 36 of the 54 entities with capability maturity self-assessments. These assessments look at how well-developed and capable entities' established IT controls are. We then compared their self-assessments with results from our GCC audits.

36 entities issued GCC findings and capability assessments			
Central Regional TAFE	Curtin University	Department of Biodiversity, Conservation and Attractions	Department of Communities
Department of Education	Department of Finance	Department of Jobs, Tourism, Science and Innovation	Department of Justice
Department of Local Government, Sport and Cultural Industries	Department of Planning, Lands and Heritage	Department of the Premier and Cabinet	Department of Primary Industries and Regional Development
Department of Training and Workforce Development	Department of Transport	Department of Treasury	Department of Water and Environmental Regulation
Disability Services Commission	East Metropolitan Health Service	Edith Cowan University	Health Support Services
Housing Authority	Western Australian Land Information Authority (trading as Landgate)	Lotteries Commission (trading as Lotterywest)	Commissioner of Main Roads
Murdoch University	North Metropolitan TAFE	North Regional TAFE	Racing and Wagering Western Australia
Rottnest Island Authority	South Metropolitan Health Service	South Metropolitan TAFE	South Regional TAFE
The University of Western Australia	WA Country Health Service	Police Service	Western Australian Tourism Commission
18 entities issued GCC findings only			
Animal Resources Authority	Botanic Gardens and Parks Authority	Department of Fire and Emergency Services	Department of Health
Electricity Generation and Retail Corporation (trading as Synergy)	Electricity Networks Corporation (trading as Western Power)	Kimberley Ports Authority	Mental Health Commission
North Metropolitan Health Service	Office of the Information Commissioner	PathWest Laboratory Medicine WA	Pilbara Ports Authority

Public Transport Authority of Western Australia	Water Corporation	Western Australian Land Authority	Western Australian Sports Centre Trust (trading as VenuesWest)
Western Australian Treasury Corporation	Zoological Parks Authority		

Source: OAG

Table 1: State government entities issued GCC findings

The model we have developed for our audits is based on accepted industry better practice and considers various factors including the:

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

We focused on the following 6 categories:

Source: OAG

Figure 1: GCC categories

Conclusion

We reported 526 GCC findings to 54 audited entities this year, compared to 553 findings at 59 entities last year. These findings continue to represent a considerable risk to the confidentiality, integrity and availability of entities' information systems.

It is disappointing that 49% of this year's audit findings were weaknesses unresolved from the previous year, compared to 42% unresolved last year. As internal and external threats continue to evolve it is important entities promptly address audit findings to protect their information systems and IT environments.

The 36 entities that had capability assessments improved their controls in 4 of the 6 categories. A similar finding to last year, building a positive trend. However, information security is still our biggest area of concern with no noticeable improvement from the previous year, and similar to prior years. Half of the entities failed to meet our benchmark in this area

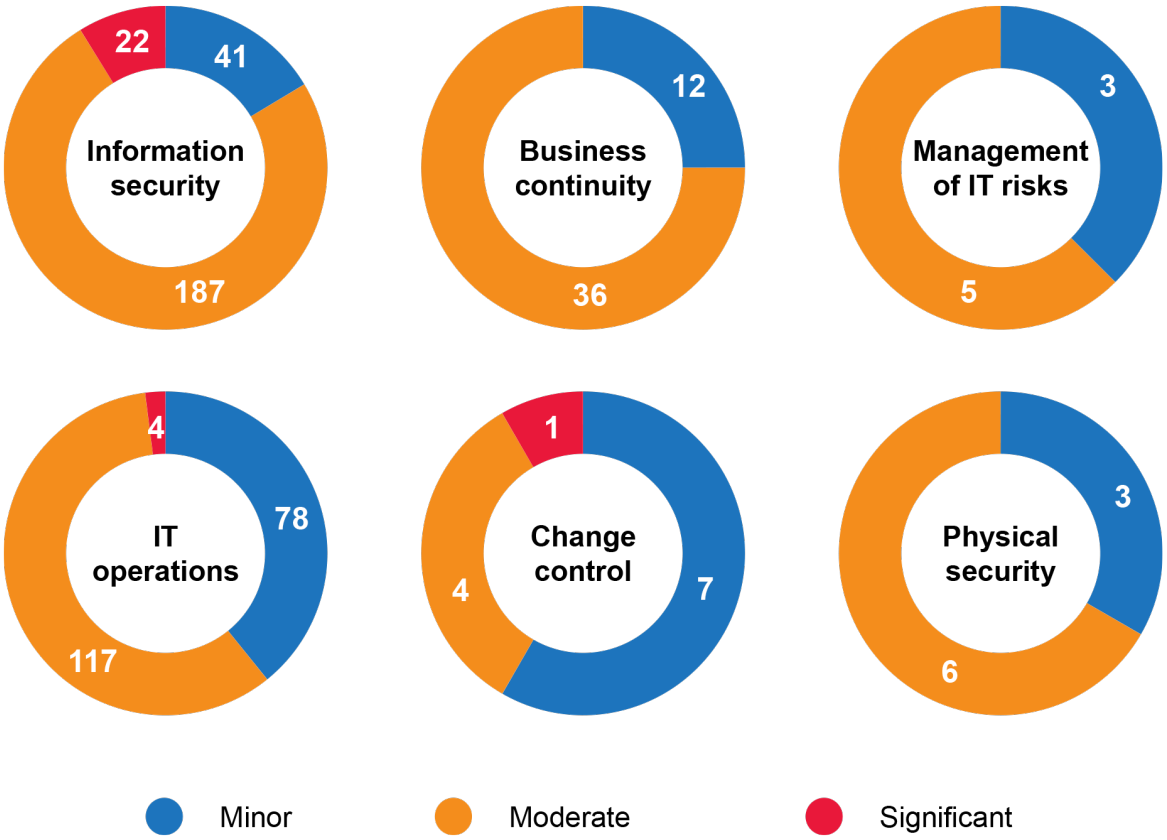
and implement effective controls to protect their information systems. At 6 entities[2] control weaknesses were so pervasive and significant that their financial audit controls opinions were qualified.

[2] Western Australian Auditor General's Report, Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities, Report 10: 2020-21, p. 12 - 18

What we found: General computer controls

In 2020-21, we reported 526 findings to 54 State government entities. Findings in the information security area accounted for 47% of the findings. These weaknesses leave entities' information systems, data and IT environments exposed to vulnerabilities which may affect confidentiality, integrity and availability of systems and information.

Most identified weaknesses are rated as moderate (Figure 2) because they are of sufficient concern to warrant action being taken by the entity as soon as possible. However, combinations of moderate findings can expose entities to more serious risks.



Source: OAG

Figure 2: Ratings for GCC findings in each control category

What we found: Capability assessments

We conducted capability assessments at 36 State government entities.

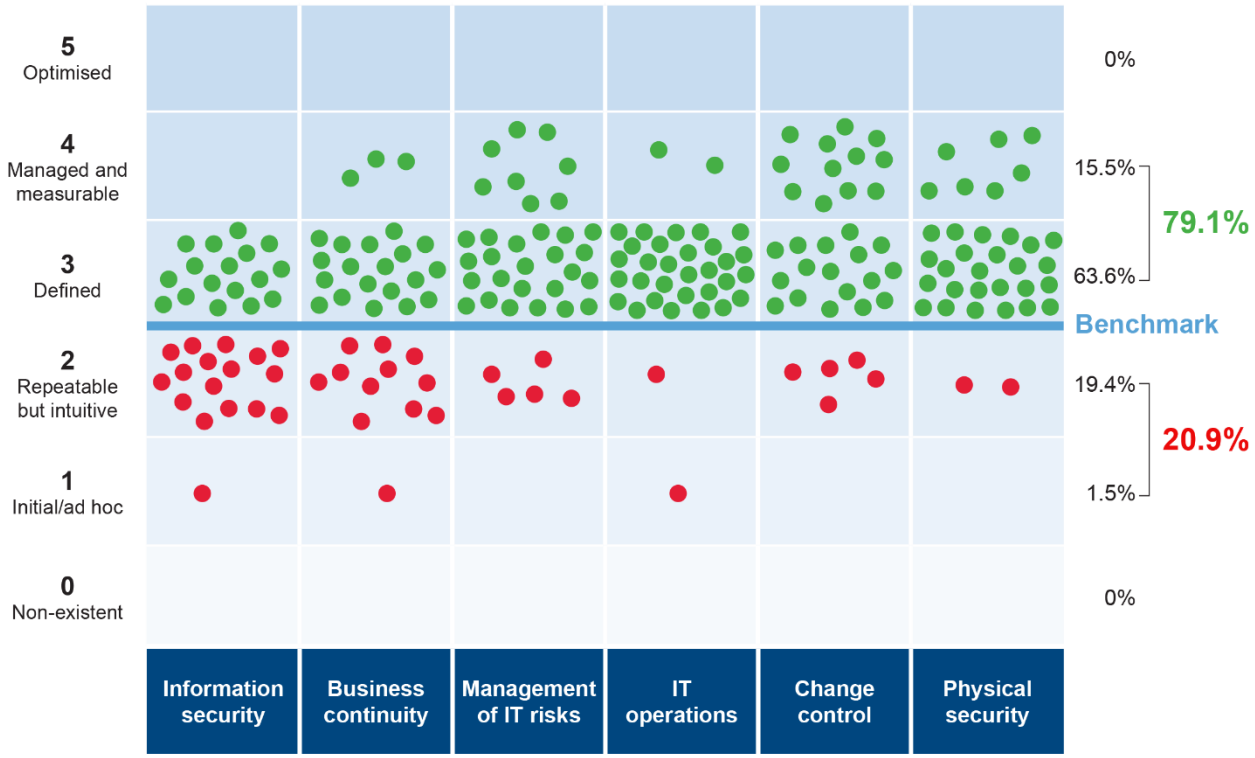
We use a 0-5 rating scale[3] (Figure 3) to evaluate each entities' capability maturity level in each of the 6 GCC categories. We expect entities to achieve a level 3 (Defined) rating or better in each category.

Source: OAG

Figure 3: Rating scale and criteria

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

Figure 4 shows the results of our capability assessments across the 6 control categories[4].



Source: OAG

Figure 4: 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	50	–	50
Business continuity	65	↑	62
Management of IT risks	86	↑	78
IT operations	94	↑	82
Change control	85	–	85
Physical security	94	↑	91

Source: OAG

Table 2: Percentage of entities rated level 3 or above

Entities improved their controls in 4 categories and remained constant in 2. Information security continues to be our biggest area of concern where, similar to last year, half of the entities failed to meet the benchmark.

[4] We assessed 34 entities across all 6 categories. At 2 entities we only assessed 1 category (management of IT risks) as their IT services were delivered by other state government entities.

Nine of the entities we perform a capability assessment at every year have consistently demonstrated good practices across all 6 control categories:

- Department of the Premier and Cabinet (9 years at level 3 or higher)
- Racing and Wagering Western Australia (8 years at level 3 or higher)
- Western Australian Land Information Authority (6 years at level 3 or higher)
- Curtin University (6 years at level 3 or higher)
- Edith Cowan University (5 years at level 3 or higher)
- Department of Training and Workforce Development (5 years at level 3 or higher)
- Lotteries Commission (4 years at level 3 or higher)
- South Metropolitan TAFE (4 years at level 4 or higher)
- Department of Finance (4 years at level 4 or higher).

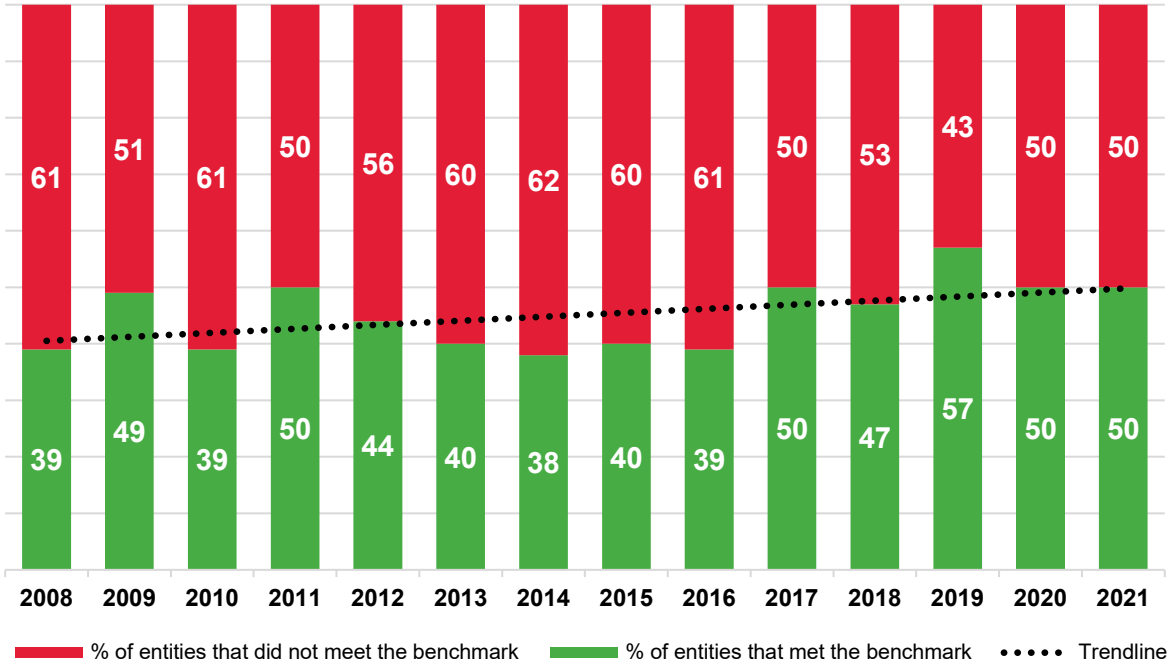
Information security

We assessed whether entity controls were administered and configured to protect information systems and IT environments from internal and external threats. We examined entities' operations, information systems and security policies. Our audits also included an assessment against better practice controls for information and cyber security. These controls may include:

Source: OAG

Figure 5: Information security controls included in our GCC audits

The number of entities that met our benchmark for information security remained the same as last year at 50% (Figure 6). Over the last 14 years there has been little improvement in this area with only 11% increase in the number of entities since 2008. 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 2020-21.



Source: OAG

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

Common weaknesses we found included:

- **Inadequate information security policies** – policies were out of date or did not sufficiently cover key areas of information and cyber security.
- **Endpoints missing essential controls** – blocking of untrusted code and application whitelisting[5] was not in place to reduce the risk of compromise through malware, and anti-malware software was not appropriately maintained.
- **Emails not protected** – entities did not have controls to ensure the integrity and authenticity of emails and reduce the likelihood of successful phishing attacks. Controls such as domain-based message authentication (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented to prevent email impersonation.
- **Multifactor authentication not used** – a number of public facing systems did not require multifactor authentication to strengthen access to systems.
- **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.

[5] Application whitelisting ensures that only allowed programs run on the computers or the network.

- **Vulnerability management tools not appropriately used** – the tools were not correctly configured or appropriately used to detect vulnerabilities in systems, networks and endpoints, which increases the risk of compromise.
- **Network segregation not appropriate** – networks were not segregated to limit 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** – 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.
- **Lack of data loss prevention controls** – no processes to detect or block unauthorised transfers of sensitive data outside of the entities.
- **Weak database security controls** – weak database passwords, excessive permissions granted by default and a lack of data encryption increased the risk of compromise. These controls are also important to deter insider threats.
- **Cloud security controls** – inadequate controls to secure cloud resources and prevent unauthorised network traffic from untrusted networks.

These common weaknesses, and their importance to information and cybersecurity, are further illustrated in the following case studies.

Case study 1: Corporate information removed without delegation

Information security

An entity without formal policies and processes for the removal of corporate records, removed an email about bullying allegations from 15 staff email accounts, including the account of the person that raised the allegations. We found the allegation had not been entirely deleted as an official record, only removed from inappropriate circulation as it contained sensitive information. However, the entity could not confirm if the staff member who ordered the removal had the appropriate delegation to do so, or if the sender was provided a copy of the email for their records. Without appropriate policies and procedures, the integrity and availability of corporate information may be compromised.

Case study 2: Use of legacy protocols results in compromise

Vulnerability management

An entity was using legacy authentication protocols (IMAP) to access emails when it experienced a cybersecurity breach that resulted in staff emails being compromised. It is good practice not to use legacy protocols that cannot be secured with multifactor authentication.

Case study 3: Poor controls to protect sensitive information

Information security

An entity had stored sensitive information in a shared folder which was accessible to all staff on the network. The folder contained emails of very senior staff. The entity had no controls to prevent the sensitive emails from being copied to personal devices, or controls to monitor if this had happened. These weaknesses expose the entity's sensitive information to inappropriate disclosure, loss or misuse.

Case study 4: Multifactor authentication not applied to restrict access to key systems

Multi-factor authentication

An entity's staff could access a key system without multifactor authentication. We first raised this issue with the entity in 2019. Since then the entity has enabled multifactor authentication on some systems, but not all. The entity remains at increased risk of unauthorised and inappropriate access to its systems.

Multifactor authentication strengthens access and has become a standard control to protect critical systems, especially if accessed remotely.

Case study 5: Entity not aware of all disclosed vulnerabilities by vendors

Vulnerability management

An entity had not applied updates (plugins) to its vulnerability detection software and would not be aware if its systems had known vulnerabilities. The entity could experience interruptions to its delivery of services to the public, and financial and reputational loss if its systems are compromised.

During our audits we perform scans to understand what vulnerabilities affect entities' systems and how they are being managed. We often find entities are not using their vulnerability management software correctly.

Case study 6: Highly sensitive information could be accessed without logging and monitoring controls

Information classification

At 1 entity we found staff could access highly sensitive reports sourced from multiple systems without logging and monitoring controls. Entity allowed this access only to those staff who had appropriate security clearance however, we found that over 200 staff with access to the reports did not have the required security clearances. Appropriate controls to restrict access and monitor system use reduce the risk of unauthorised access to information.

Case study 7: Lack of appropriate process to manage contractor access

User account management

An entity did not maintain a central record of contractor access to its network and systems. The entity does not have readily available information to assess the validity of contractor access and take timely action if necessary.

We identified 8 contractor accounts that accessed the entity's network (4 remotely accessed) after their termination date recorded in the system. While the entity's security team identified these accounts for termination, and advised the IT team, the IT team did not disable the accounts.

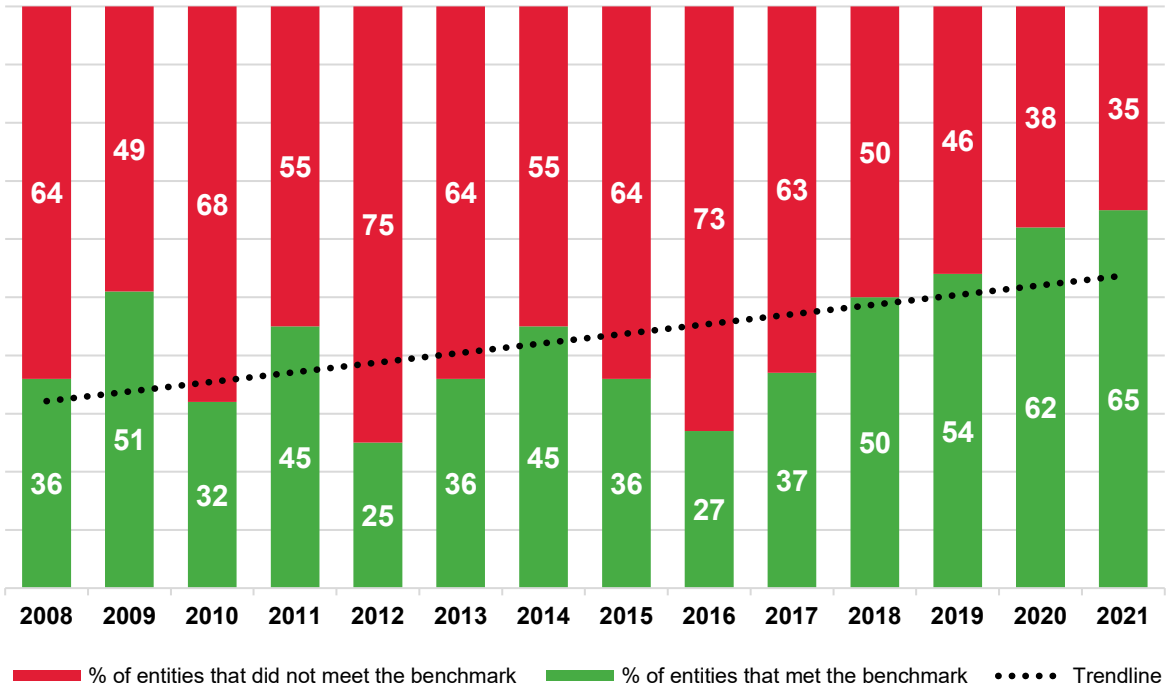
Business continuity

We continue to see improvement in this area with 65% of entities meeting the benchmark, compared to 62% last year and 54% in 2018-19 (Figure 7). This improvement may, in part, be attributable to the need for entities to continue to respond to the COVID-19 pandemic. However, many entities still did not have an up-to-date business continuity plan and disaster recovery plans, which was a surprise in the current environment.

Business continuity, disaster recovery and incident response plans help entities recover critical information systems in the event of an unplanned disruption to their operations and services. Without these plans IT teams may struggle to restore key business functions and processes after a disruption. This could lead to extended outages and disruption to the delivery of important services to the public.

Critical operations are identified and prioritised in the business continuity plan and inform the resourcing and focus areas of the disaster recovery plans. Potential incidents and the immediate steps to ensure a timely, appropriate and effective response are considered in incident response plans.

Entities should test these plans on a periodic basis to assess and improve their processes to recover in the event of an unplanned disruption. Senior executives should monitor that plans are developed and tested in accordance with the risk profile and appetite of the entity.



Source: OAG

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

Common weaknesses we found included:

- **IT disaster recovery plans were outdated and did not consider changes in the IT environment** – in an event of disruption there could be delays in recovering key systems and key services.
- **Lack of business continuity planning** – no business continuity plans, or they were out-of-date. An up-to-date business continuity plan is crucial to an entity's restoration of key functions in the event of a disruption. The scope of a business continuity plan should cover all business-critical areas, including IT.
- **Lack of disaster recovery plan testing** – without appropriate testing of disaster recovery plans, entities cannot be certain the plan will work when needed.
- **No backup testing procedures** – no formal procedures to verify that systems and data can be recovered from a backup.

The following case study illustrates common weaknesses in disaster recovery plans.

Case study 8: Outdated disaster recovery plans

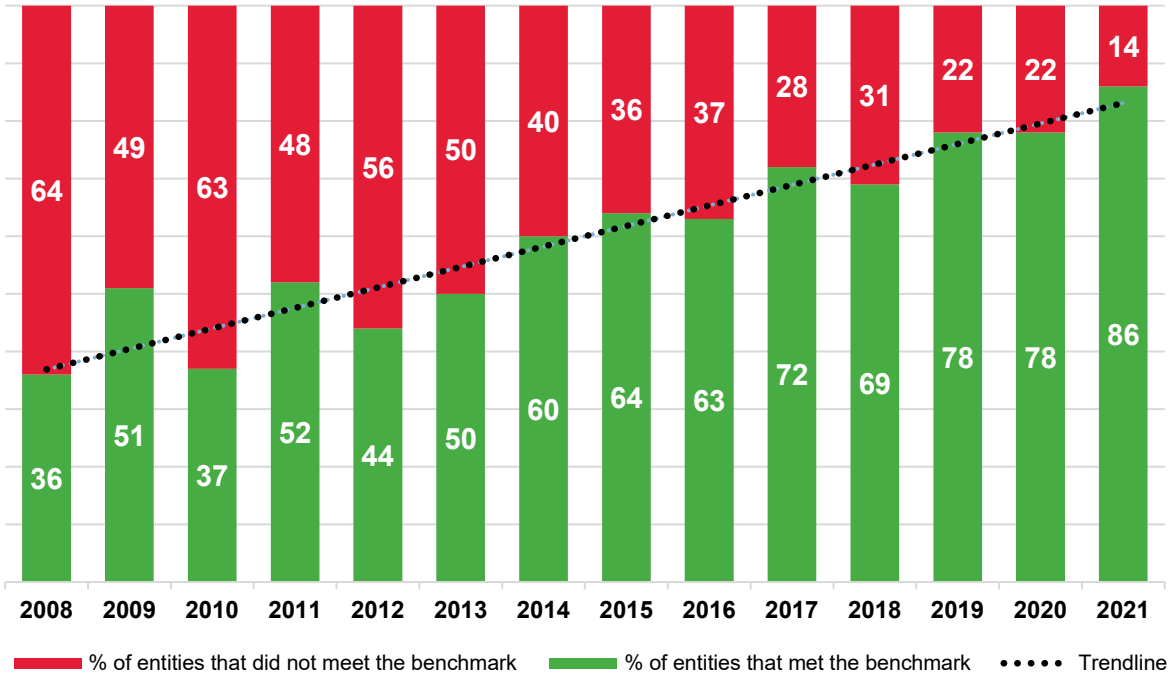
Disaster recovery plan

One entity did not update its disaster recovery plans after it moved a considerable amount of its IT infrastructure from on-premise to the cloud. In the event of an unplanned disruption the entity may experience delayed recovery of its key systems and services, and extended interruption of service delivery to the public because it will not readily know system configuration and dependencies in the cloud.

Management of IT risks

The percentage of entities that met our benchmark for this category in 2020-21 was 86% (Figure 8). This is the highest since we started benchmarking 14 years ago.

Entities should be aware of information and cybersecurity risks associated with IT including operational, strategic and project risks. All entities should have risk management policies and practices to assess, prioritise, address and monitor these risks affecting key business objectives.



Source: OAG

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

Common weaknesses we found included:

- **Lack of policies and processes to identify, assess and treat IT risks** – without appropriate policies and processes, entities cannot effectively manage their IT risks.
- **Lack of IT risk register** – risk registers were not maintained for ongoing monitoring and mitigation of identified risks.
- **IT risks not reported to senior management** – key IT risks may not be addressed if senior management is not aware of them.

Without appropriate IT risk policies and practices, entities may not identify, mitigate, and manage threats within reasonable timeframes, and may not meet their business objectives.

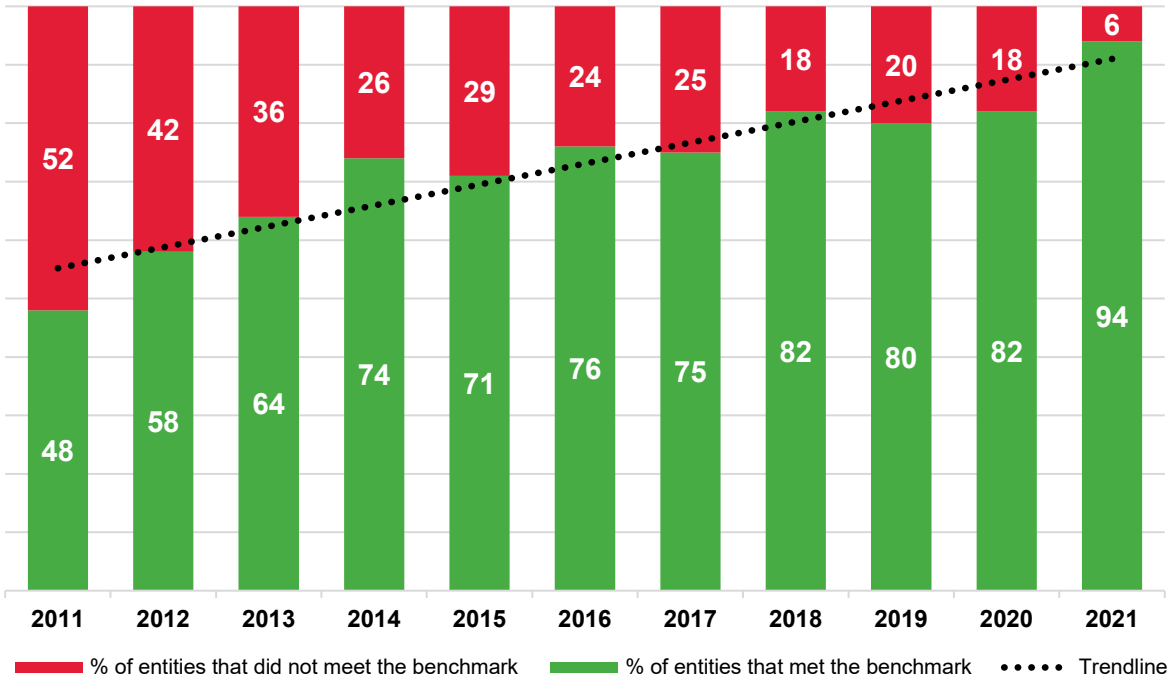
IT operations

Entities continued to improve with 94% reaching our benchmark (Figure 9). This is the highest since we started auditing this category in 2011. It is also the category that showed the largest improvement since last year.

Effective management and visibility of IT operations is key to maintaining data integrity and ensuring IT infrastructure can withstand and recover from errors and failures. We assessed if

entities had adequately defined their requirements for IT service levels and allocated sufficient resources to meet these requirements. We also tested whether service and support levels were adequate and met better practice. Other tests included if:

- policies and plans were implemented and working effectively
- repeatable functions were formally defined, standardised, documented and communicated
- effective prevention and monitoring controls and processes had been implemented to ensure data integrity.



Source: OAG

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

Note: data is only available from 2011 when we added this category to the capability maturity model.

Common weaknesses we found included:

- **Supplier performance not monitored** –supplier performance was not reviewed to identify and manage instances of non-compliance with agreed service levels and ensure value for money.
- **Inadequate staff termination processes** – failure to consistently apply the pre-exit checklist procedures to staff terminations resulted in an increased risk of unauthorised access and loss of confidential information.
- **Inadequate monitoring of events** – entities did not have effective policies and procedures to monitor event logs. System logs provide an opportunity to detect suspicious or malicious behaviour in key business applications.

Without appropriate IT strategies and supporting procedures, IT operations may not meet business requirements and may not be able to recover from errors or failures.

The following case studies illustrate common weaknesses in IT operations.

Case study 9: Inefficiencies and risks due to multiple systems

Multiple systems

A large State government entity used 4 different finance systems, despite also having a licensed enterprise system for the entity with about 500 user licences not in use. In addition to being inefficient, this use of multiple finance systems increases financial risk and underutilises licensed resources.

Case study 10: Important application events not monitored

Logging and monitoring

One entity did not proactively monitor or review event logs for a key business application. While the application did not have event log and monitoring capability, the entity did have access to another system with the same business functionality and monitoring capability, but it was not used.

Without monitoring, the entity may not identify potential problems or attempts to compromise their systems or data.

Case study 11: Lack of vendor performance management

Assurance over third-party services

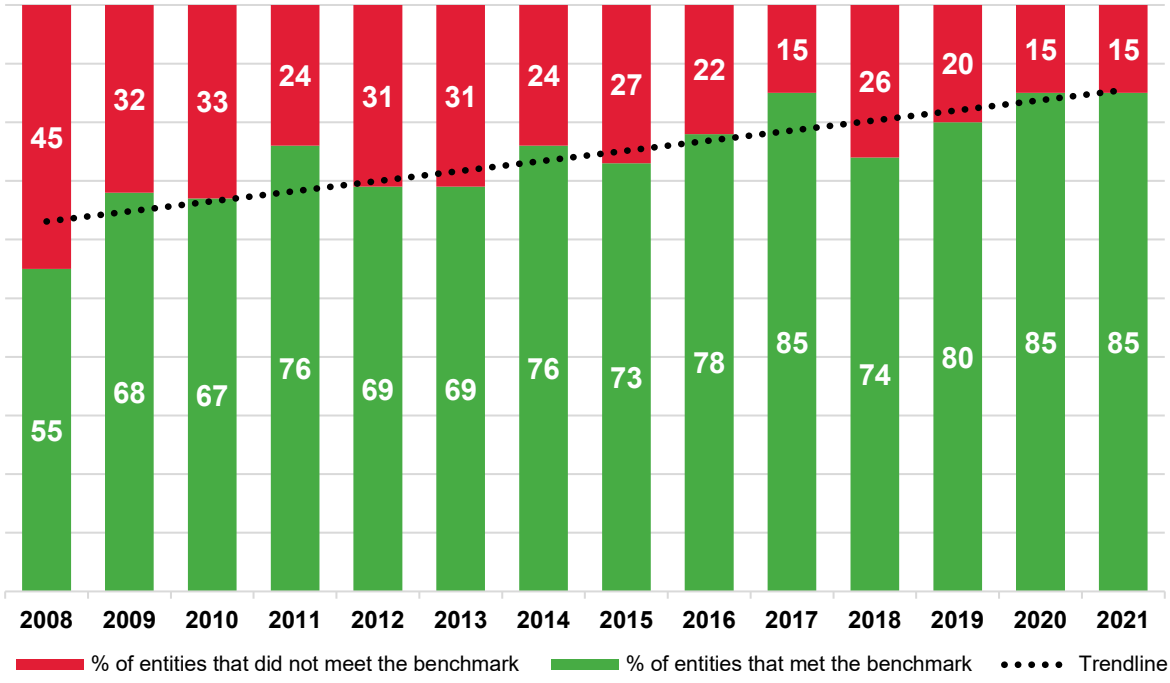
One entity does not periodically verify that its third-party vendor delivers agreed network security and management services in line with service agreements, including if network devices are secured and managed as expected. The vendor maintains core firewalls, routers, and access points for the entity. The entity is at increased risk of successful supply chain attack if the vendor's environment is not secure.

Processes to periodically review the vendor's performance would help the entity effectively manage its IT operations to resist and recover from errors and failures.

Change control

Entities' change control practices were consistent with last year with 85% of entities meeting our benchmark in 2020-21 (Figure 10).

We examine if system changes are controlled to minise the risks and impact to stakeholders. An overarching change control framework is essential to ensuring changes are made consistently, reliably and efficiently. All changes should be appropriately authorised, tested, implemented and recorded. Implementation and rollback plans should be part of change control to recover from any adverse impacts.



Source: OAG

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

Common weaknesses we found included:

- **Change management processes not documented** – without documented processes and procedures, changes made to IT infrastructure can adversely affect entities' operations leading to unplanned or excessive system down time.
- **Change processes not followed** – changes to critical systems may be applied inconsistently if formal change processes are not followed. This can result in unplanned system downtime and interrupt entities' delivery of critical services to the public.

Without adequate change control procedures, systems may not process information as intended and entities' operations and services may be disrupted. There is also a greater chance of information loss, and access being given to unauthorised persons.

The following case study illustrates common weaknesses in entity change controls.

Case study 12: Changes to key finance system were not recorded

Change management

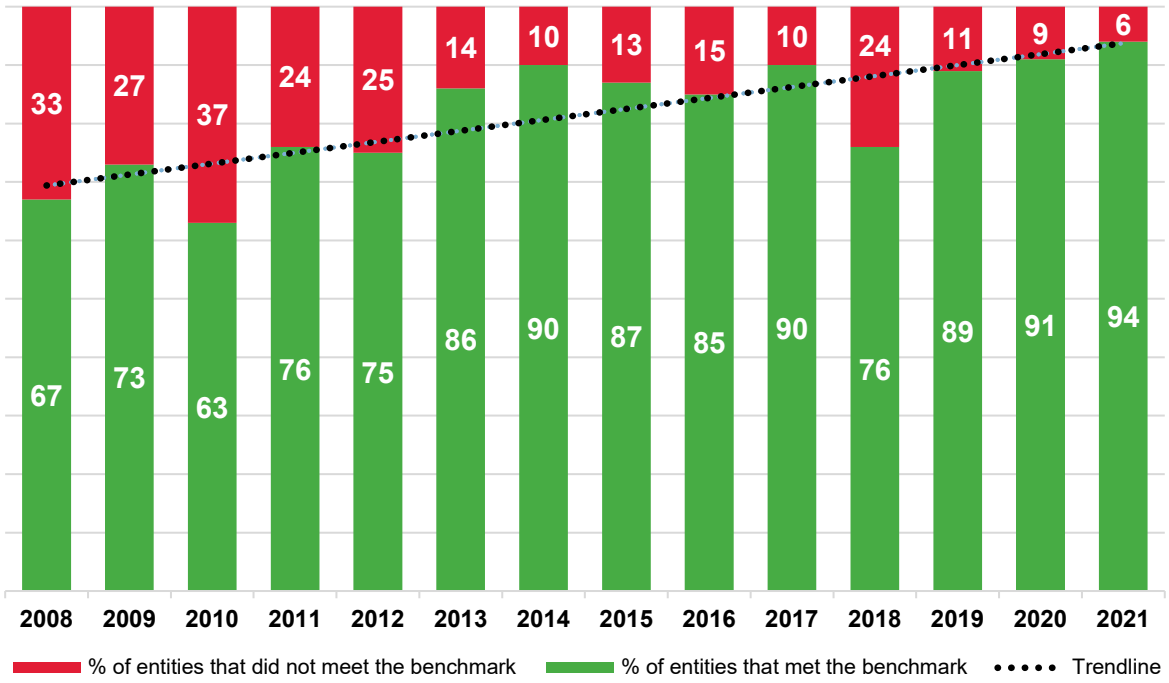
An entity did not record changes made to its finance system and it was unclear to us whether changes were approved and tested prior to implementation. This increased the risk of unauthorised or inappropriate changes being made.

Entities should record changes to their systems, along with supporting evidence that changes were approved and tested.

Physical security

Ninety-four percent of entities met our expectations for the management of physical security (Figure 11). This is a 27% improvement since our first assessment in 2008.

We examined if entities' IT systems were protected against environmental hazards and related damage. We also reviewed if entities had implemented and monitored physical access restrictions to ensure that only authorised individuals could access or use computer systems.



Source: OAG

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

Common weaknesses we found included:

- **Lack of fire suppression systems** –without an appropriate fire suppression system, systems are likely to be damaged in the event of a fire.
- **Access to server rooms was not managed well** – processes to review and limit access to server rooms reduce the risk of system outages and compromise from unauthorised access.
- **Untidy cabling and non-essential equipment in server rooms** – the risk of outages is higher if server rooms are not appropriately maintained.

Recommendations

1. Information security

Executive managers should:

a. implement better practice security measures in the following areas:

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

b. conduct ongoing reviews and monitor user access to information to ensure access is appropriate at all times

c. develop and implement mechanisms to continually raise awareness of information and cyber security practices among all staff.

2. Business continuity

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

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 and embed practices as core business activities and executive oversight.

4. IT operations

Entities should implement policies and procedures that reference better practice standards and frameworks in key areas such as IT risk management, information security, business continuity and change control. IT strategic plans and objectives should support overall business strategies and objectives.

5. Change control

Entities should consistently apply approved change control processes when making changes to their IT systems. To minimise the occurrence of problems, these processes should include the requirement for thorough planning and impact assessments. 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 damage to computing infrastructure and systems.

Appendix 1: Control categories in our updated capability maturity model (for 2022 audits)

1. Manage IT risk
2. Information security framework
3. Human resource security
4. Manage access
5. Endpoint security
6. Network security
7. Physical security
8. Manage change
9. Manage IT operations
10. Manage continuity

Auditor General's 2021-22 reports

Number	Title	Date tabled
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