Western Australian
Auditor General's Report

Information Systems Audit Report 2021 – State Government Entities

Report 29: 2020-21
16 June 2021

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Jordan Langford-Smith
Kamran Aslam
Paul Tilbrook
Fareed Bakhsh
Steven Bertke
Sayem Chowdhury
Michael Chumak
Khubaib Gondal
Reshma Vikas

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 2021 – State Government Entities

Report 29: 2020-21
June 2021

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2021 – STATE 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 13th year we have separately reported on State government entities' general computer controls (GCCs). The objective of our GCC audits is to determine whether entities' computer controls effectively support the confidentiality, integrity and availability of information systems.

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

CAROLINE SPENCER
AUDITOR GENERAL
16 June 2021

Contents

Auditor General's overview

The report summarises the results of the 2020 annual cycle of information systems audits for State government entities and tertiary institutions in the Western Australian public sector.

In the context of intensifying cyber attacks on all sectors, this report contains a number of important findings and recommendations resulting from our general computer controls audits and capability maturity assessments. All public sector entities should consider how they can apply the recommendations and case studies in the report to their operations with the expectation of an increasingly demanding threat environment into the future.

While entities improved their controls in 4 categories and remained constant in 1, information security continues to be an area of significant weakness. It is disappointing to see only 50% of entities met our benchmark in this area, a drop of 7% from last year. Poor information security controls leave entity systems and information vulnerable to misuse and may impact critical services provided to the public.

The report also includes a summary of common issues related to remote access. During the COVID-19 response periods, entities supported their workforces with flexible working from home arrangements. This transformation also brought security challenges as entities changed the way they operate, in some cases significantly. In this changing environment, it is important that entities identify risks around information security and take appropriate mitigation measures.

Remote work is stated to become more prevalent and entities may continue to operate with a mix of remote and on-site workforces. Entities should consider these findings and ensure that adequate policies, strong access controls and monitoring are in place to address the inherent risks associated with remote working arrangements. This will require them to develop plans and implement controls to manage a range of hybrid environment risks including information security and business continuity. There may, however, be some specific functions, types of sensitive information or aspects of service delivery for which such risks cannot be adequately managed and these should be identified and incorporated into business continuity plans.

Consistent with previous years, entities are not quickly addressing audit findings with 42% of the findings having been reported previously. This is the first year that I have decided to list the entities who received audit findings in the 2019-20 cycle of audits, in addition to entities who have been consistently demonstrating good practices.

Upcoming changes to the Australian Auditing Standards clarify and enhance the need for auditors to understand general computer controls and their impact on the financial report. In particular, auditors are required to assess controls for each aspect of the IT environment including the network, operating system, database and application layers.

Introduction

This is our 13th report on the audits of State government entities' general computer controls (GCCs). The objective of our GCC audits is to determine whether entities' computer controls effectively support the confidentiality, integrity and availability of information systems.

For 2019-20, we reported GCC issues to 59 State government entities (Table 1). We provided 36 of the 59 entities with capability maturity assessments and asked them to self-assess. We then compared their results with results from our GCC audits. These assessments look at how well-developed and capable entities' established IT controls are.

Generally smaller entities and those audited by our contract audit firms did not include capability assessments.

This report also includes the findings of our assessment of entities' remote access controls, an area of increasing significance following the COVID-19 pandemic and more staff working from home.

Thirty-six entities issued GCC findings and capability assessments			
Animal Resources Authority	Department of Jobs, Tourism, Science and Innovation	Department of Water and Environmental Regulation	Rottnest Island Authority
Central Regional TAFE	Western Australian Tourism Commission	Disability Services Commission	South Metropolitan TAFE
Department of Justice	Edith Cowan University	South Regional TAFE	Commissioner of Main Roads
Department of Local Government, Sport and Cultural Industries	Health Support Services	University of Western Australia	Curtin University
Department of Planning, Lands and Heritage	Housing Authority	WA Country Health	Department of Biodiversity, Conservation and Attractions
Department of the Premier and Cabinet	Lotteries Commission of Western Australia	Department of Communities	Department of Primary Industries and Regional Development
Murdoch University	WA Police Force	Department of Education	Department of Training and Workforce Development
North Metropolitan TAFE	Western Australian Land Information Authority (Landgate)	Department of Finance	Department of Transport
North Regional TAFE	Department of Fire and Emergency Services	Department of Treasury	Racing and Wagering Western Australia
Twenty-three entities only issued GCC findings			
Child and Adolescent Health Services	Western Australian Greyhound Racing Association	Parliamentary Services Department	Water Corporation

Building and Construction Industry Training Board	Infrastructure Western Australia	Perth International Arts Festival Limited	Western Australian Sports Centre Trust (trading as Venues West)
Botanic Gardens and Parks Authority	Office of the Information Commissioner	Pilbara Ports Authority	Western Australian Treasury Corporation
Department of Mines, Industry Regulation and Safety	Kimberley Ports Authority	Public Transport Authority of Western Australia	Electricity Networks Corporation (trading as Western Power)
Forest Products Commission	Western Australian Land Authority	Electricity Generation and Retail Corporation (trading as Synergy)	Zoological Parks Authority
Fremantle Port Authority	Minerals Research Institute of Western Australia	The National Trust of Australia (WA)	

Source: OAG

Table 1: State government entities issued GCC findings

The model we have developed for our audits is based on accepted industry good practice. Our assessment is also influenced by 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 553 GCC issues to the 59 audited entities this year compared to 522 issues at 50 entities last year.

Entities are still not addressing audit findings quickly, with 42% of this year's findings previously reported. One way entities can remain vigilant against the rapidly changing threats to information systems is by promptly addressing audit findings.

For our capability assessments, entities improved their controls in 4 of the 6 audited categories. However, we continue to find a large number of weaknesses that could compromise the confidentiality, integrity and availability of information systems.

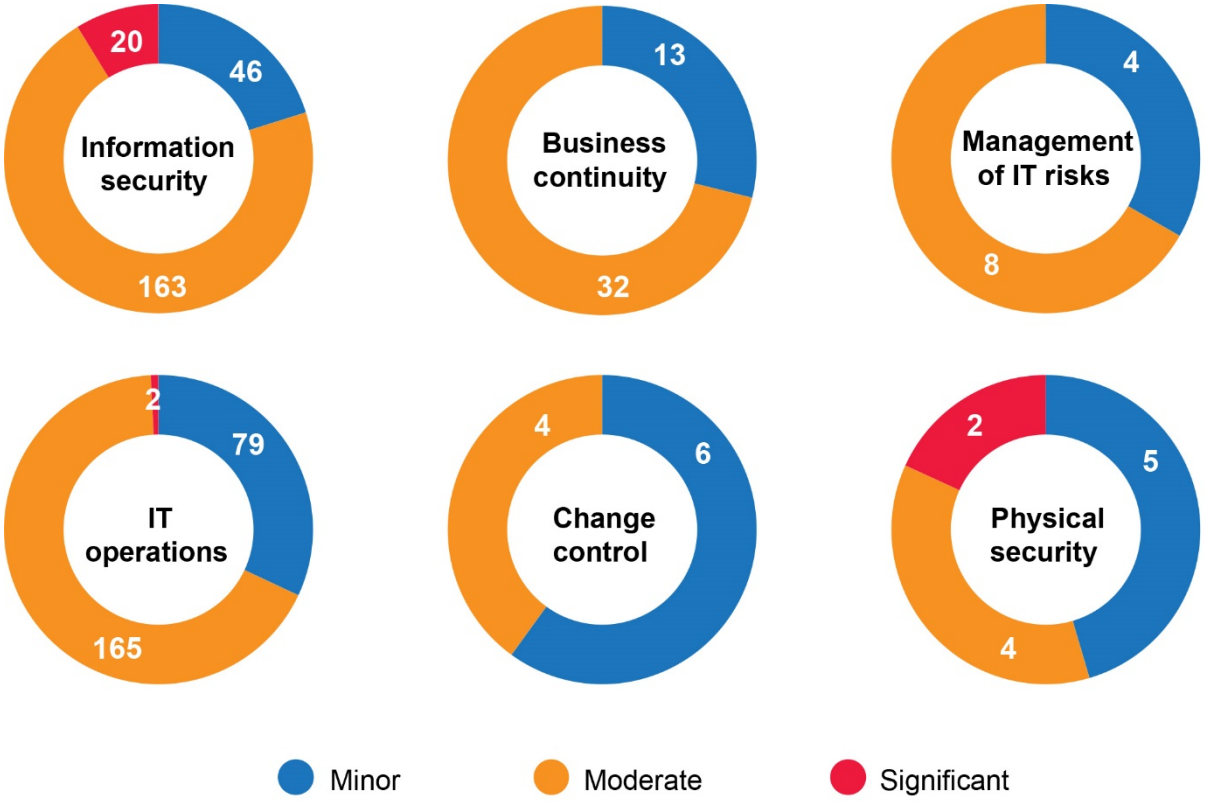
Information security remains our biggest area of concern with only 50% of entities meeting our benchmark in this category, a drop of 7% from last year. While addressing shortcomings in complex legacy systems can require time for careful planning and coordination and significant resources, poor information security controls leave entity systems and information vulnerable to misuse and may impact critical services provided to the public.

What we found: General computer controls

In 2019-20, we reported 553 findings to 59 State government entities.

Most of our findings 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 issues can expose entities to more serious risks.

Although we did not rate a large proportion of findings as significant, of particular concern are findings in the information security area, because these leave systems directly exposed or can introduce vulnerabilities.



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. For 2 entities, we only assessed their management of IT risks as their remaining IT functions were delivered by other entities.

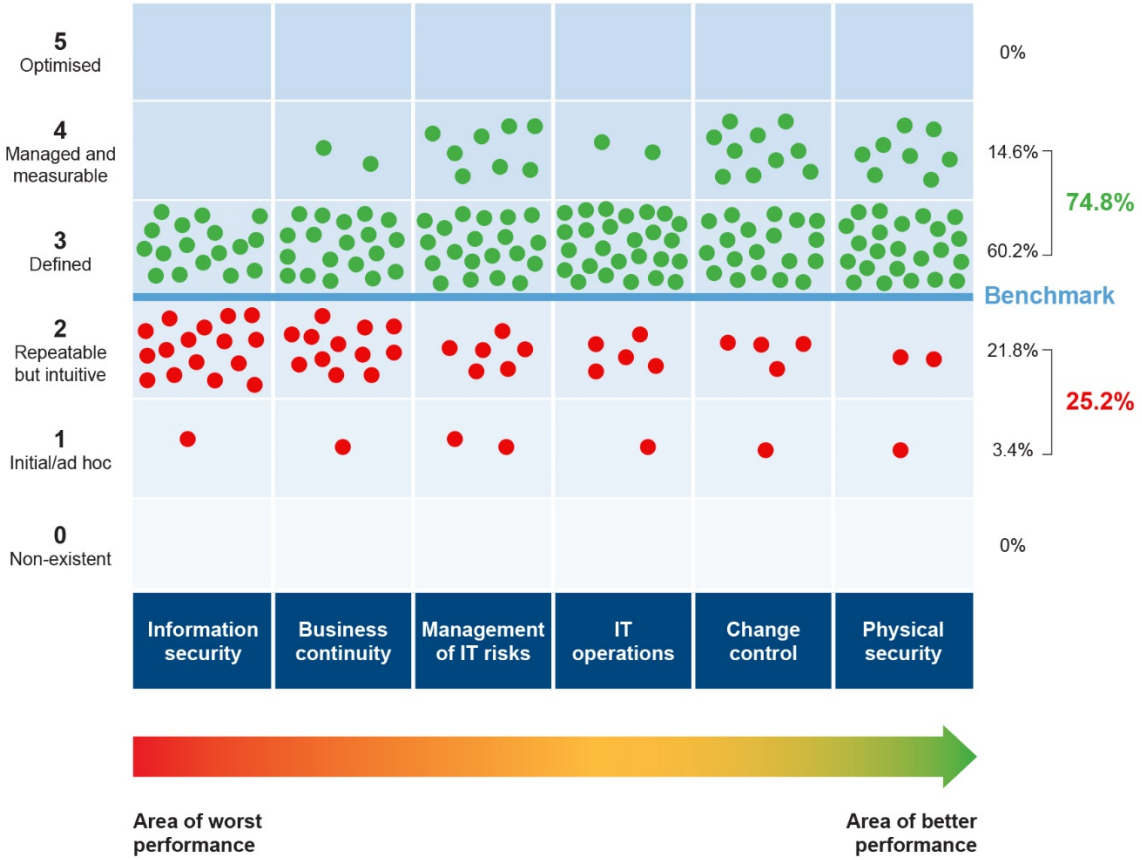
We use a 0-5 rating scale[1] (Figure 3) to evaluate each entities' capability maturity level in each of the 6 GCC categories. We expect entities to achieve a level 3 (Defined) rating or better across all the categories.

Source: OAG

Figure 3: Rating scale and criteria

[1] 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.



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	2019-20 %		2018-19 %
Information security	50	↓	57
Business continuity	62	↑	54
Management of IT risks	78	–	78
IT operations	82	↑	80
Change control	85	↑	80
Physical security	91	↑	89

Source: OAG

Table 2: Percentage of entities rated level 3 or above

While entities improved their controls in 4 categories and remained constant in 1, information security continues to be an area of concerning weakness.

Only 5 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 (8 years at level 3 or higher)

- Racing and Wagering Western Australia (7 years at level 3 or higher)
- Western Australian Land Information Authority (5 years at level 3 or higher)
- Curtin University (5 years at level 3 or higher)
- Department of Training and Workforce Development (4 years at level 3 or higher).

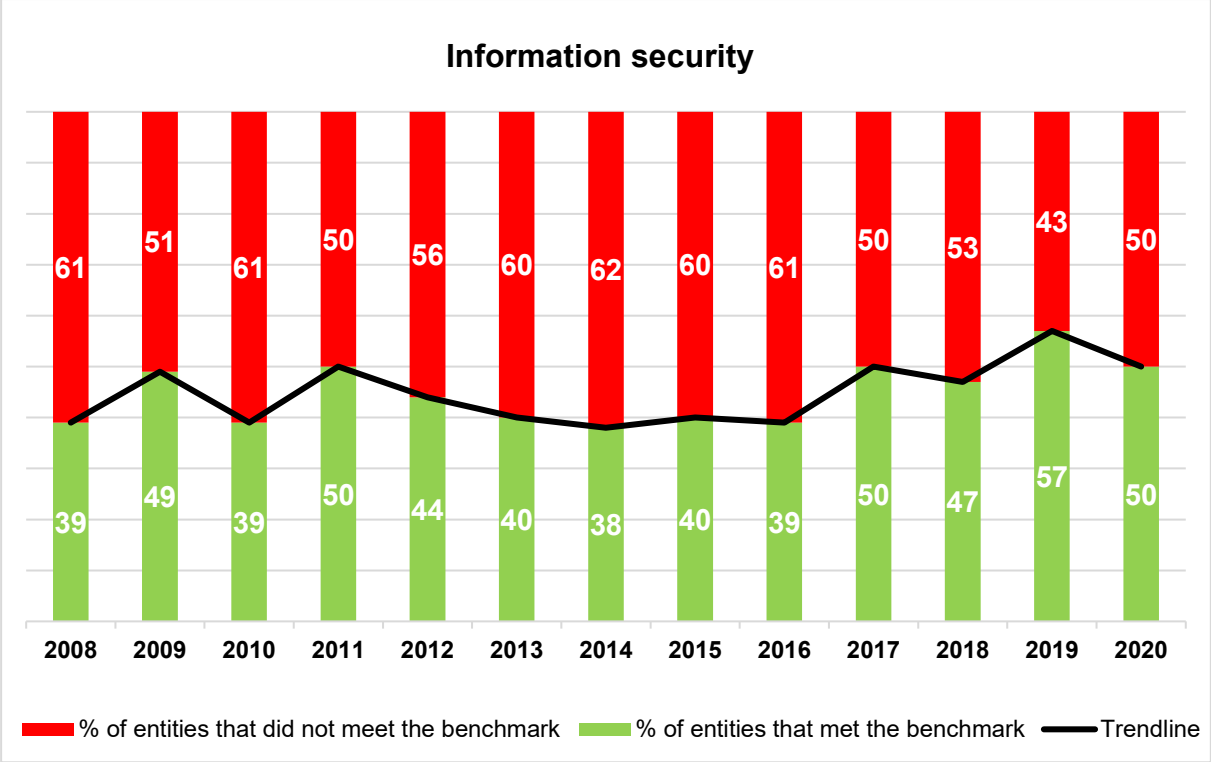
Information security

We assessed whether entity controls were administered and configured to appropriately restrict access to programs, data and other information resources. Our audits include 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 who met our benchmark for information security decreased from 57% in 2018-19 to 50% in 2019-20. We continue to see little improvement in this space over the last 13 years.



Source: OAG

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

Common weaknesses we found include:

- **Inadequate information security policies** – policies were out of date or did not sufficiently cover key areas of information security.
- **Ineffective management of technical vulnerabilities** – a lack of appropriate policies and procedures to patch operating system software and application vulnerabilities increase the risk of compromise.
- **Inadequate access controls** – network and public facing systems did not require multifactor authentication to strengthen access to systems.
- **Administrator privileges are not managed well** – limiting privileges and reducing the number of privileged users is an important mitigation against network and system compromise.
- **Lack of data loss prevention controls** – no processes to detect or block unauthorised transfers of sensitive data outside of the entities.
- **Network segregation is not appropriate** – networks are 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 vector and spread malware or listen in on network traffic.

- **Weak database security controls** – weak database passwords, excessive permissions granted by default and a lack of data encryption increase 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, such as the Internet, to cloud-based applications.

The following case studies illustrate the risks to an entity of mismanaging information security. A summary of information security weaknesses specifically related to remote access is provided on page 20.

Case study 1: Ineffective management of vulnerabilities leads to compromise of systems

We review entities' practices to patch operating system and application vulnerabilities as part of the GCC audits. A large department with a complex network did not identify and address vulnerabilities in its key systems promptly. We found that this entity was compromised by a well-known malware. This usually occurs when organisations leave vulnerabilities unpatched for too long or do not respond quickly to new threats.

We found that the entity:

- was running its key systems without any malware protection
- had not scanned all key systems to identify vulnerabilities for over 6 months
- did not include workstations in its vulnerability identification process
- had a large number of critical and high severity vulnerabilities on its key servers that we scanned.

In response to our findings, the department has committed to develop policy and implement procedures for vulnerability management.

Case study 2: Weaknesses in software allows full control of workstations and servers

One entity had a custom-built program to change the local administrator account and password for new workstations and servers. This program is used to configure new assets. We identified that this program had security weaknesses which revealed the administrator account password. This would allow any user on the network to take full control of the workstations or servers.

Case study 3: Cloud security controls were inappropriate

One entity had recently migrated a significant part of its infrastructure to the cloud. Our assessment of its cloud-based systems revealed several weaknesses including:

- over 70 storage accounts without access restrictions
- over 290 virtual machines with vulnerable configurations

- over 50 virtual machines without an anti-malware solution.

We also found a significant number of systems with inadequate encryption to secure information including:

- over 30 web applications which could be accessed over an insecure protocol
- over 260 storage accounts that don't support secure data transfers.

The lack of appropriate controls places cloud applications and infrastructure at risk of compromise.

It is important to know if cybercriminals are targeting systems or insider threats are attempting to exploit weaknesses. One entity we audited had implemented good processes to detect such activities. The following case study shows the importance of effective monitoring processes.

Case study 4: Former staff member attempted to access the financial system

An entity we audited had implemented a monitoring process which alerted them if a number of access attempts were made in succession to important systems. Through these alerts, the entity detected a malicious logon attempt to its financial system from an employee who left over a year before.

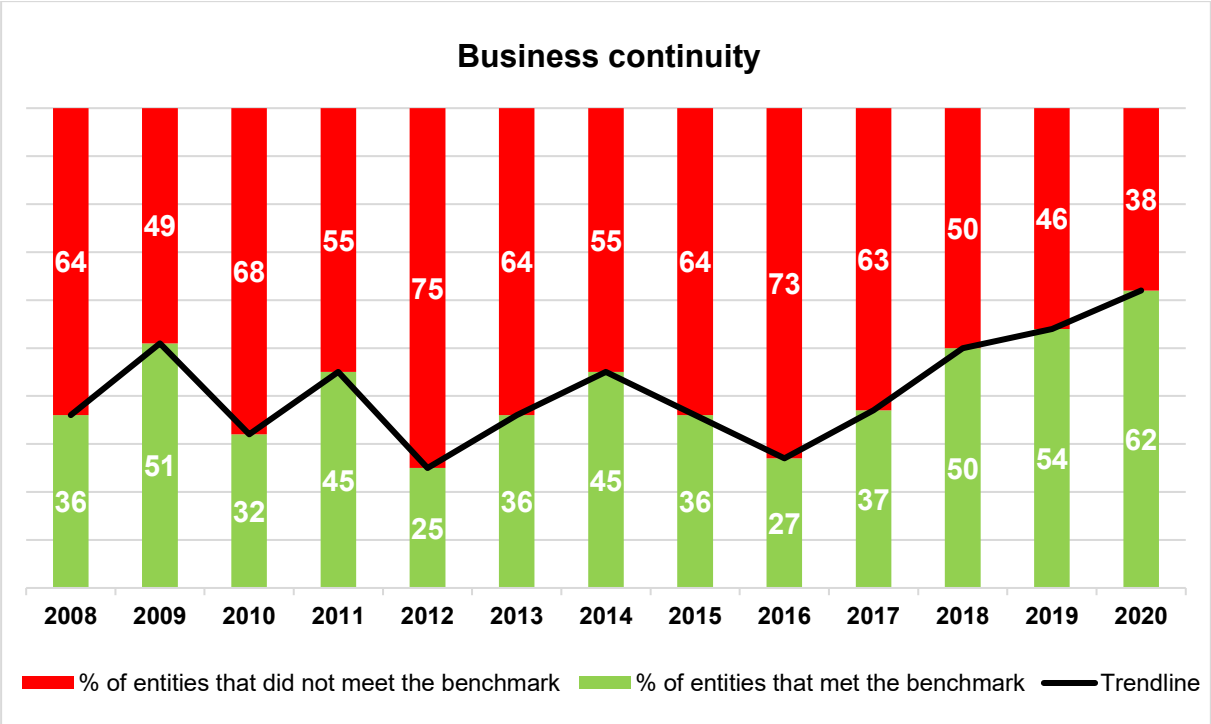
The matter was subsequently referred to for investigation. Without an effective monitoring process, it would have been extremely difficult for the entity to pro-actively detect this activity.

Business continuity

The percentage of entities that met our benchmark for this category in 2019-20 was the highest since we started benchmarking 13 years ago. This may, in part, be attributable to the need for entities to respond to COVID-19 pandemic. However, we found many still do not have adequate business continuity and disaster recovery arrangements in place.

Interruptions to business can have serious impacts on the critical services entities deliver to the public. To ensure business continuity, entities should have an up-to-date business continuity plan (BCP), disaster recovery plan (DRP) and incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure a timely, appropriate and effective response.

Entities should test these plans on a periodic basis. Such planning and testing helps entities assess and improve their processes to recover information systems in the event of an unplanned disruption to business operations and services. 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 benchmark

Common weaknesses we found include:

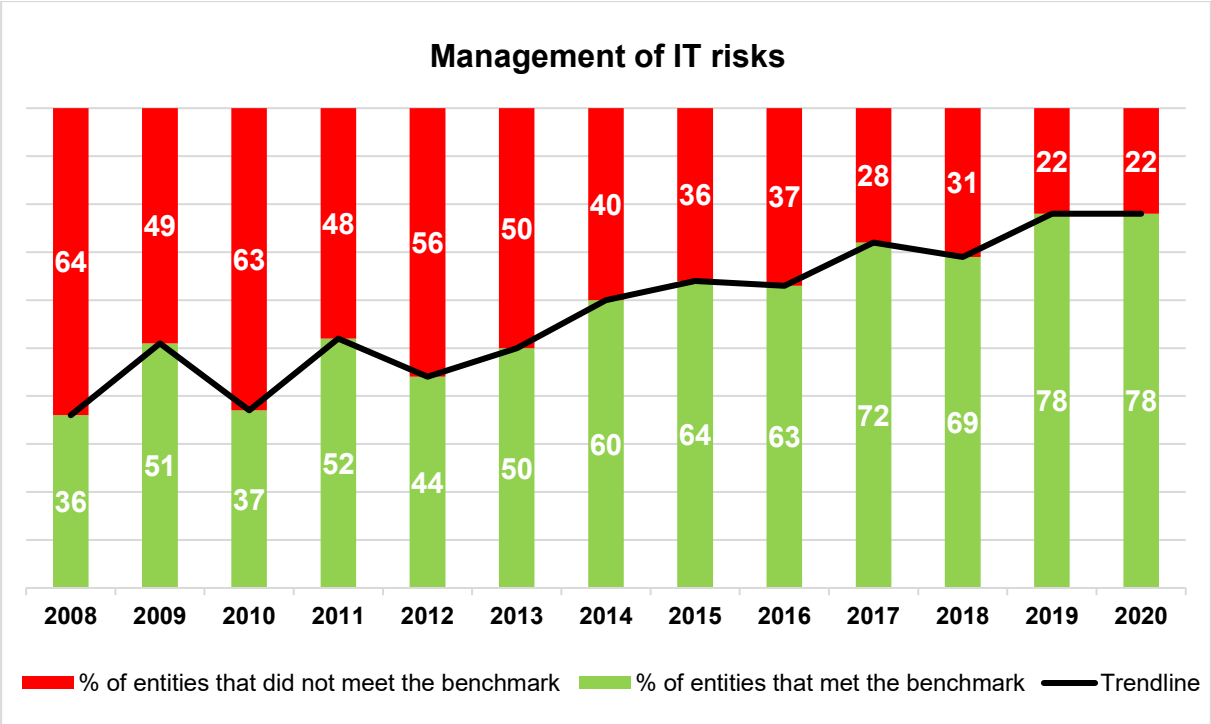
- **Lack of business continuity planning** – no business continuity plans or they were still in draft. An up-to-date business continuity plan plays a crucial part in enabling the entity to restore its key business functions in case of a disruption. The scope of a business continuity plan should also cover all business-critical areas, including IT.
- **No backup testing procedures** – no formal procedures to verify that systems and data can be recovered from a backup.
- **Inadequate IT disaster recovery plans that did not cover key systems** – in an event of disruption there could be delays in recovering key systems and key services.
- **Lack of disaster recovery plan testing** – without appropriate testing of disaster recovery plans, entities cannot be certain if the plan will work when needed.

Without appropriate business continuity planning there is an increased risk that key business functions and processes will not be restored promptly after a disruption. This could cause extended outages and disrupt the delivery of important services.

Management of IT risks

Consistent with last year, 78% of entities met our expectations for managing their IT risks. There has been steady improvement in this category, with 42% more entities meeting the benchmark since our first assessment in 2008.

All entities should have risk management policies and practices that identify, assess and treat risks that affect key business objectives. Entities should be aware of the nature of risks associated with IT and have appropriate risk management policies and practices such as risk assessments, registers and treatment plans.



Source: OAG

Figure 8: Management of IT risks – percentage of entities that met benchmark

Common weaknesses we found include:

- **Inadequate processes to identify, assess and treat IT risks** – without these processes, entities cannot manage their IT risks in an effective manner.
- **Lack of IT risk register** – risk registers are not maintained for ongoing monitoring and mitigation of identified risks.
- **IT risks are not reported to senior management** – key IT risks will go unnoticed if senior management is not aware of them.

Without appropriate IT risk policies and practices, entities may not identify and mitigate threats within reasonable timeframes. Entities may not meet their business objectives when risks are not identified and appropriately managed.

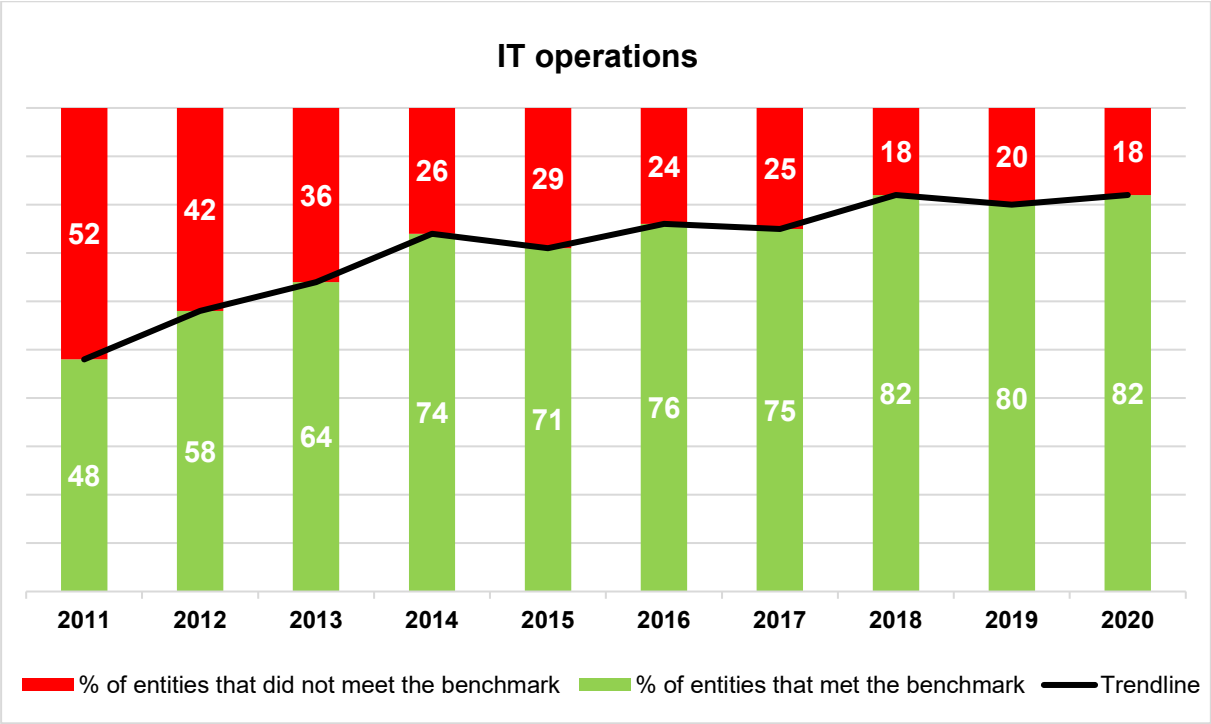
IT operations

There has been steady improvement in the IT operations category since we added it to our assessment criteria in 2011. This year, entities continued to improve with 82% reaching our benchmark.

Effective management of IT operations is key to maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures. We assessed whether 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 within entities were adequate and met good practice. Other tests included if:

- policies and plans were implemented and working effectively
- repeatable functions were formally defined, standardised, documented and communicated

- effective preventative and monitoring controls and processes had been implemented to ensure data integrity.



Source: OAG

Figure 9: IT operations – percentage of entities that met benchmark

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

Common weaknesses we found include:

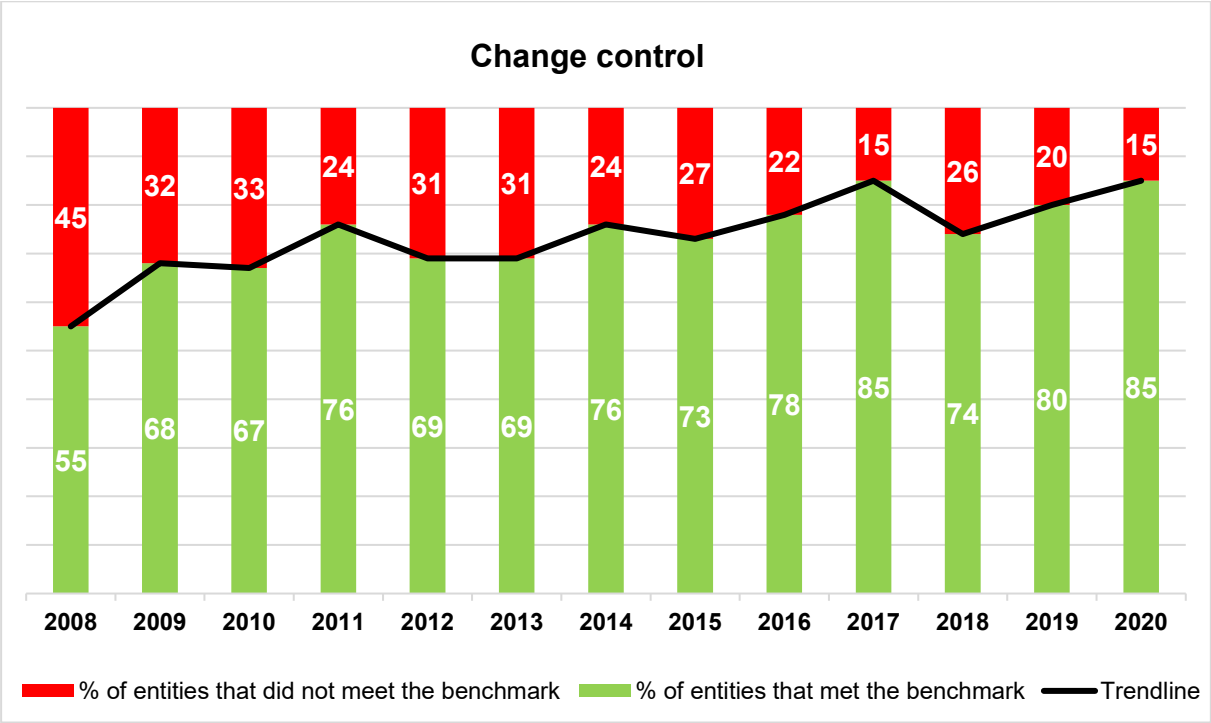
- **Failure to review policies and procedures** – outdated policies and procedures may be less effective in supporting the entity's goals.
- **Inadequate staff termination processes** – failure to consistently apply the pre-exit checklist procedures to staff terminations result in an increased risk of unauthorised access and loss of confidential information.
- **Ineffective IT asset management** – incomplete and inaccurate IT asset registers. Entities should implement processes to monitor and record the movement of IT assets to reduce the risk of asset theft or loss.
- **Lack of supplier performance management** – no supplier performance reviews to ensure value for money. Without an appropriate supplier performance review process, the entity may fail to identify non-compliance with its service agreements.
- **Inadequate monitoring of events** – system logs provide an opportunity to detect suspicious or malicious behaviour in key business applications. Entities did not have effective policies and procedures for monitoring event logs.

These types of findings can mean that IT service delivery may not meet business requirements or expectations. Without appropriate IT strategies and supporting procedures, IT operations may not be able to respond to business needs and recover from errors or failures.

Change control

Entities' change control practices continue to improve with 85% meeting our benchmark in 2019-20.

We examined if system changes are appropriately authorised, implemented, recorded and tested. We reviewed any new applications acquired or developed to evaluate if the changes were made in line with management's intentions.



Source: OAG

Figure 10: Change control – percentage of entities that met benchmark

Common weaknesses we found include:

- **No formalised change management process** – without standard procedures, changes made to IT infrastructure could adversely affect operations and cause down time.
- **Not following change processes** – change management processes are not applied consistently as some changes to critical systems do not follow the formalised process. Failure to comply with the change management process could result in unplanned downtime.

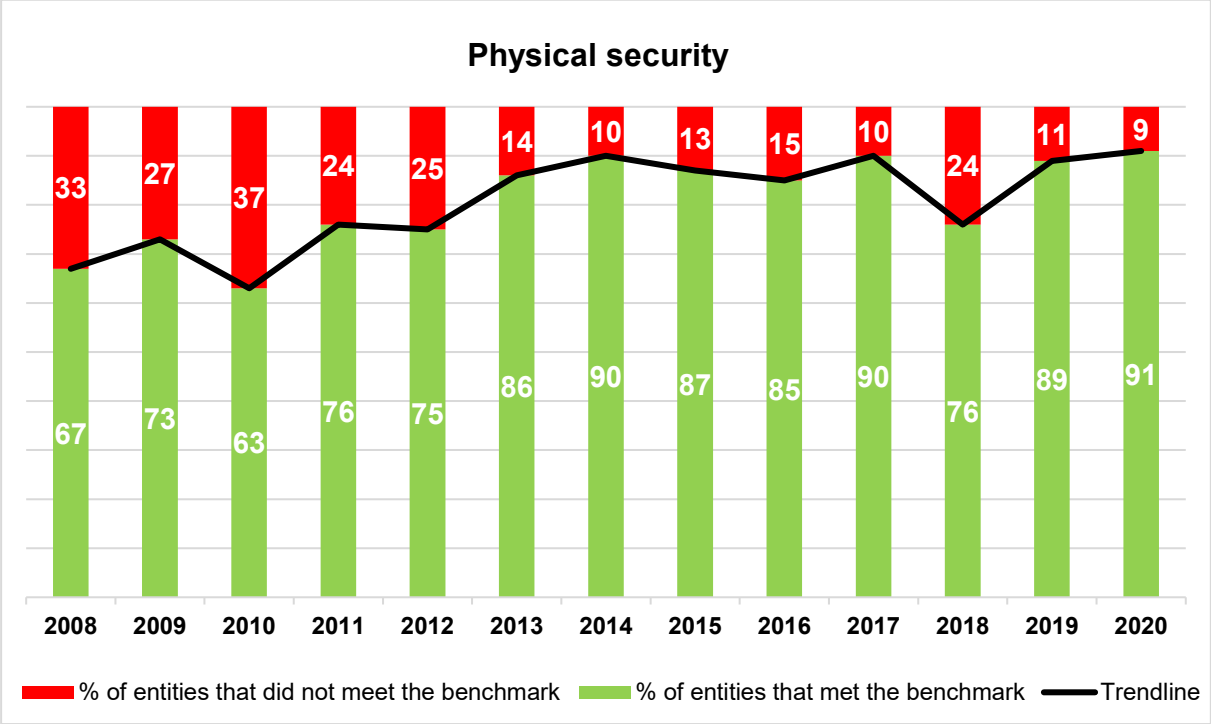
An overarching change control framework is essential to ensuring changes are made consistently, reliably and efficiently. When examining change control, we expect entities to be following their approved change management procedures.

There is a risk that without adequate change control procedures, systems will not process information as intended and entities' operations and services will be disrupted. There is also a greater chance that information will be lost and access given to unauthorised persons.

Physical security

Ninety-one percent of entities met our expectations for the management of physical security. Twenty-four percent more entities are now meeting the benchmark since our first assessment in 2008. This is also an area of better performance for many entities.

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 benchmark

Common weaknesses we found include:

- **Excessive users can access server rooms** – there is an increased risk of system outages and compromise without a process to review and limit access to server rooms.
- **Combustible materials are stored in server rooms** – business-critical infrastructure is at risk when combustible materials are stored inside server rooms.
- **Lack of fire suppression system** – there is an increased risk of system damage if an appropriate fire suppression system is not installed.

Recommendations for general computer controls

1. Information security

Executive managers should:

a. ensure good security practices are implemented in the following areas:

i) patching and vulnerability management

ii) application hardening and control

iii) strong passphrases/passwords and multi-factor authentication

iv) limit and control administrator privileges

v) segregate network and prevent unauthorised devices

vi) secure cloud infrastructure, databases, email and storage

vii) cyber security monitoring, intrusion detection and protection from malware

b. conduct ongoing reviews and monitoring of user access to information to ensure they are 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 an up-to-date business continuity plan, disaster recovery plan and incident response plan. These plans should be tested on a periodic basis.

3. Management of IT risks

Entities should:

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

b. ensure that 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 ensure appropriate policies and procedures are in place for key areas such as IT risk management, information security, business continuity and change control. In addition, entities should ensure IT strategic plans and objectives support overall business strategies and objectives. Entities should reference good practice standards and frameworks when implementing their own policies and procedures.

5. Change control

Well-developed change control processes should be consistently followed for changes to computer systems. Thorough planning and impact assessment of all changes should 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 damage to computing infrastructure and systems.

Remote access

The COVID-19 pandemic prompted organisations to quickly make changes to accommodate staff working remotely. Many organisations that previously didn't allow remote access to internal networks had to implement or accelerate the implementation of remote access systems. This increased challenges for security teams as transformation brought new opportunities for attackers to exploit system vulnerabilities and human error. A recent report[2] shows an increase in cybercrime due to working from home arrangements.

We assessed remote access management controls as part of our general computer controls audits to establish if entities were addressing information and cyber security risks.

We identified common weaknesses in the following areas:

Policies

Entities allowed staff to use personal computers to carry out their work. However, they did not have any policies to govern the use of personal devices or remote access. There were no minimum baseline security requirements that personal computers had to meet in order to access entity resources remotely. Some examples of the baseline controls we would expect to see include anti-malware, supported operating systems, patching and a secure internet.

Personal computers and networks present an attack surface that could be used by malicious actors to compromise entity networks and systems.

Data loss prevention

Entities did not restrict users from copying sensitive information to personal devices, and there were no audit trails to check if unauthorised download of information had occurred. If entities do not know where important information is stored, it will limit their ability to protect that information. This situation creates a risk of unintentional or inappropriate exposure of information. Entities deal with a range of sensitive and confidential information including information about members of public. It is imperative that effective controls are in place to protect such information from unauthorised disclosure and theft. This includes ensuring that hard copy information is appropriately secured.

Penetration tests

Penetration testing is when an entity simulates a cyberattack to test the effectiveness of their defences. We found entities had not completed this testing on their remote access systems to gain assurance that controls were effective to protect them from cyberattacks. This could put their systems at risk of compromise.

Multifactor authentication

Multifactor authentication (MFA) requires 2 or more pieces of evidence before granting access to systems. We found entities did not implement MFA to strengthen access. This means users could access the entities' systems and

[2] https://www.baesystems.com/en-media/uploadFile/20210428003949/1434665245766.pdf

networks with only a username and password, leaving the organisation vulnerable to phishing and password compromise.

Monitoring

Entities were not capturing and monitoring important events to understand if malicious activity was occurring on their systems and networks. IT staff and contractors also use remote privileged access to IT infrastructure, and entities do not have visibility of their actions. Event logs from a variety of sources including network devices, security appliances, remote access systems and endpoints must be monitored to identify malicious activity.

A 2020 study[3] found that the average time to detect and contain a security breach is 280 days. When a breach does occur, remote access logs will often play a key part in its detection, containment and future investigation.

Case study 5: Limited retention of security logs

One audited entity retains its remote access logs for 1 month only. Given the time it takes to detect a security breach on average, this limits the entity's ability to effectively investigate cyber intrusion or data breaches.

Access reviews

Entities did not have effective review procedures to ensure only authorised users had remote access. We identified staff accounts that were not disabled after the staff member had left the entity. This increases the risk of unauthorised or inappropriate access to key systems and information.

We also identified entities using generic accounts for remote access. Use of generic accounts limits accountability as it becomes difficult to attribute unauthorised activities to individuals.

Regular review procedures ensure that remote user accounts including highly privileged accounts, are still appropriate and their ongoing use is appropriate.

[3] https://www.ibm.com/security/data-breach

Recommendations for remote access

State government entities should:

1. develop appropriate policies to govern the use of personal devices. This should include a minimum-security baseline that personal devices must meet before accessing entity systems and networks
2. restrict users from copying sensitive information to personal devices, and ensure audit trails exist to identify instances of unauthorised download of information
3. implement and maintain an effective vulnerability management process to address potential security vulnerabilities before they are exploited. Develop a patching baseline to make sure all local and cloud-based systems and applications are patched in a timely manner
4. review and harden the internet-facing infrastructure including remote access systems and applications
5. implement multi-factor authentication to strengthen access controls
6. implement security monitoring processes that correlate logs from key network, security and application systems
7. develop effective processes for granting administrative access to remote access systems. Maintain oversight over administrative activity, keep the number of system administrators to a minimum and make sure this level of access is only granted to appropriate staff
8. implement processes to ensure only valid users can access internal systems remotely. This includes an effective off boarding process that removes remote access upon employee or third-party contractor termination, as well as regular reviews to identify unneeded accounts.

Auditor General's 2020-21 reports

Number	Title	Date tabled
28	Western Australian Public Sector Financial Statements – Better Practice Guide	14 June 2021
27	Opinion on Ministerial Notification – Port Agreements	11 June 2021
26	Audit Results Report – 2020 Financial Audits of Universities and TAFEs	2 June 2021
25	Delivering Essential Services to Remote Aboriginal Communities – Follow-up	2 June 2021
24	Opinion on Ministerial Notification – DPIRD Capability Review	18 May 2021
23	Local Government General Computer Controls	12 May 2021
22	Opinion on Ministerial Notification – Hospital Facilities Services	6 May 2021
21	Regulation and Support of the Local Government Sector	30 April 2021
20	Opinions on Ministerial Notifications – Policing Information	28 April 2021
19	Opinion on Ministerial Notification – Bennett Brook Disability Justice Centre	8 April 2021
18	Regulation of Consumer Food Safety by the Department of Health	1 April 2021
17	Department of Communities' Administration of Family and Domestic Violence Support Services	11 March 2021
16	Application Controls Audits 2021	8 March 2021
15	Opinions on Ministerial Notifications – Tax and Funding Information Relating to Racing and Wagering Western Australia	26 February 2021
14	Opinion on Ministerial Notification – Hotel Perth Campaign Reports	24 February 2021
13	Opinion on Ministerial Notification – Release of Schedule of Stumpage Rates	24 February 2021
12	Grants Administration	28 January 2021
11	COVID-19 Relief Fund	21 December 2020
10	COVID-19: Status of WA Public Testing Systems	9 December 2020

Number	Title	Date tabled
9	Western Australian Registry System – Application Controls Audit	26 November 2020
8	Regulating Minor Pollutants	26 November 2020
7	Audit Results Report – Annual 2019-20 Financial Audits of State Government Entities	11 November 2020
6	Transparency Report: Major Projects	29 October 2020
5	Transparency Report: Current Status of WA Health's COVID-19 Response Preparedness	24 September 2020
4	Managing the Impact of Plant and Animal Pests: Follow-up	31 August 2020
3	Waste Management – Service Delivery	20 August 2020
2	Opinion on Ministerial Notification – Agriculture Digital Connectivity Report	30 July 2020
1	Working with Children Checks – Managing Compliance	15 July 2020

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