Western Australian
Auditor General's Report

Information Systems Audit Report 2020 – State Government Entities

Report 18: 2019-20
6 April 2020

Office of the Auditor General
Western Australia

Audit team:
Jordan Langford-Smith
Kamran Aslam
Walber Almeida
Karla Cordoba
Sheau Lan Gan
Jake Davey
Fareed Bakhsh
Nomin Chimid-Osor

National Relay Service TTY: 13 36 77
(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 2020 – State Government Entities

Report 18: 2019-20
April 2020

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2020 – STATE GOVERNMENT ENTITIES

This report has been prepared for submission to Parliament under the provisions of sections 24 and 25 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.

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

CAROLINE SPENCER
AUDITOR GENERAL
6 April 2020

Contents

Auditor General's overview

I am pleased to present our annual *Information Systems Audit Report.* The report summarises the results of the 2019 annual cycle of information systems audits for State government entities and tertiary institutes in the Western Australian public sector.

This report presents the results of our general computer control audits and capability assessments. The capability and maturity of entities' general computer controls is such an important organisational imperative that it deserves the prominence of a dedicated report. Case studies are presented to share lessons from across the sector, including my Office. In future years, we may expand this report to provide more detailed information about common weaknesses found and approaches to addressing shortcomings.

The report contains a number of important findings and recommendations. All public sector entities should consider the recommendations and case studies in the report to see how they can be applied to their operations.

It is pleasing to see the number of entities assessed as having mature general computer controls across all categories of our assessment increased from 13 to 15, with many capability areas improving. However, information security and business continuity showed little improvement, with many entities failing to meet the benchmark for minimum practice. This is of significant concern given the value of personal and corporate information entities hold. It is my view that entities need to be as vigilant in protecting their personal and corporate information, by implementing the same level of controls including monitoring and protection, as for other valuable assets, such as cash, bank account access and other physical assets. Maturity across all sectors and entities has a way to go in this regard.

We use a rating scale to assess the maturity of entity controls across 6 categories. While the model has worked well over the last 12 years, my Office is looking at modernising and enhancing the model in future years. We hope this will help entities continue to develop and maintain robust controls that will sustain improved levels of maturity in general computer control environments.

The Office of Digital Government's support to entities in addressing weaknesses and improving their capability is an important central agency function, required for a modern public service where connectivity and security of State systems is a focus. During the last 12 months, following a request from the Office of Digital Government, I provided them with copies of entity management letters for our general computer controls audits, where entities consented for us to do so, in order to inform their work program.

Unfortunately, it can be difficult for entities to perfectly implement controls, and sometimes staff will ignore or circumvent them – either deliberately or inadvertently. That is why having mechanisms to detect problems, including monitoring controls, ongoing training and rotation of staff is vital. It is also critical to promote an organisational culture where staff understand the principles of information security and are encouraged to report shortcomings in the knowledge they will be addressed.

My Office is not ring-fenced from reality, or immune in this regard. In 2019 we discovered an instance where access controls for a business system were not effective. Consequently, human resource and other non-audit information was inappropriately accessed internally by staff who did not need to access it. Information on this matter is included in a case study in Appendix 1, which is provided to share the lessons learnt by our Office, including the value of various control mechanisms, as it was ultimately those controls that brought the breach to our attention.

In all entities, system controls are particularly important at times where entities are going through significant change to consolidate and modernise information and communications technology. These changes bring new challenges, particularly where information technology (IT) arrangements are outsourced. Our sector-wide controls audits have found that governance of outsourced IT arrangements needs improvement. Entities were not consistently ensuring that the systems implemented by vendors meet expectations around security standards, architecture and functionality. With a global trend to outsource IT services, entities have an increasingly important responsibility for ensuring that external service providers follow better practices.

In the current environment, controls around remote IT access infrastructure will also need to be an area of priority as entities increasingly support staff to work in more flexible ways in response to current public health measures for the COVID-19 virus. To assist entities with this, we have included some good practice security considerations in Appendix 2 around remote access.

Introduction

The objective of our general computer controls (GCCs) audits is to determine whether computer controls effectively support the confidentiality, integrity, and availability of information systems. Information systems are important for the delivery of essential services to the public. GCCs include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. In 2019, we focused on 6 categories of GCCs:

- information security
- business continuity
- management of IT risks
- IT operations
- change control
- physical security.

Conclusion

The number of entities that met our expectations across all control categories continued to improve in 2019, with 15 entities meeting the benchmark compared to 13 in 2018.

However, we continue to find a large number of GCC weaknesses which could compromise the confidentiality, integrity and availability of information systems. In 2019, we reported 522 GCC issues to 50 State government entities. This was a slight reduction from the 547 issues reported at 47 entities in 2018. However, entities are not addressing audit findings quickly, with 45% of the findings reported in 2019 relating to previously reported audit findings. One way entities can remain vigilant against the rapidly changing threats to information systems is by promptly addressing audit findings.

Controls over information security and business continuity are slowly improving, but they continue to be areas of concern. We found that 46% of the entities still don't have appropriate business continuity strategies and 43% lack controls to adequately manage information security. Poor controls in these areas leave systems and information vulnerable to misuse and may impact critical services provided to the public.

Our capability maturity model assessment indicated that entities are managing system changes and physical security relatively well. We also noted there was a slight improvement in the management of IT risks.

All entities need to pay more attention to information security and cyber risks, including procedures to classify information. These risks require the same attention as other critical business risks and building a culture of security is essential in effectively treating them.

Background

We use the results of our GCC work to inform our capability assessments of entities. Capability maturity models (CMMs) are a way to assess how well developed and capable entities' established IT controls are. The models provide a benchmark for entity performance and means for comparing results from year to year, and across entities.

The model we have developed uses accepted industry good practice as the basis for assessment. Our assessment of GCC maturity is influenced by various factors including the:

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

Audit focus and scope

We conducted GCC audits at 50 State government entities. This is the 12th year we have assessed entities against globally recognised good practice.

We provided 37 of the 50 entities with capability assessments and asked them to self-assess. We then met with each of the entities to compare their assessment and ours, which was based on the results of our GCC audits. There were thirteen entities where we did not perform a capability assessment as the audits were fully outsourced or IT control testing was performed by our financial audit teams.

We use a 0-5 rating scale[1] to evaluate each entities' capability maturity level in each of the GCC categories. We have included specific case studies where information security weaknesses potentially compromise entities' systems.

0 Non-existent	Management processes are not applied at all. Complete lack of any recognisable processes.
1 Initial/ad hoc	Processes are ad hoc and overall approach to management is disorganised.
2 Repeatable but intuitive	Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.
3 Defined	Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated, however it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 Managed and measurable	Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimised	Good practices are followed and automated. Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the entity quick to adapt.

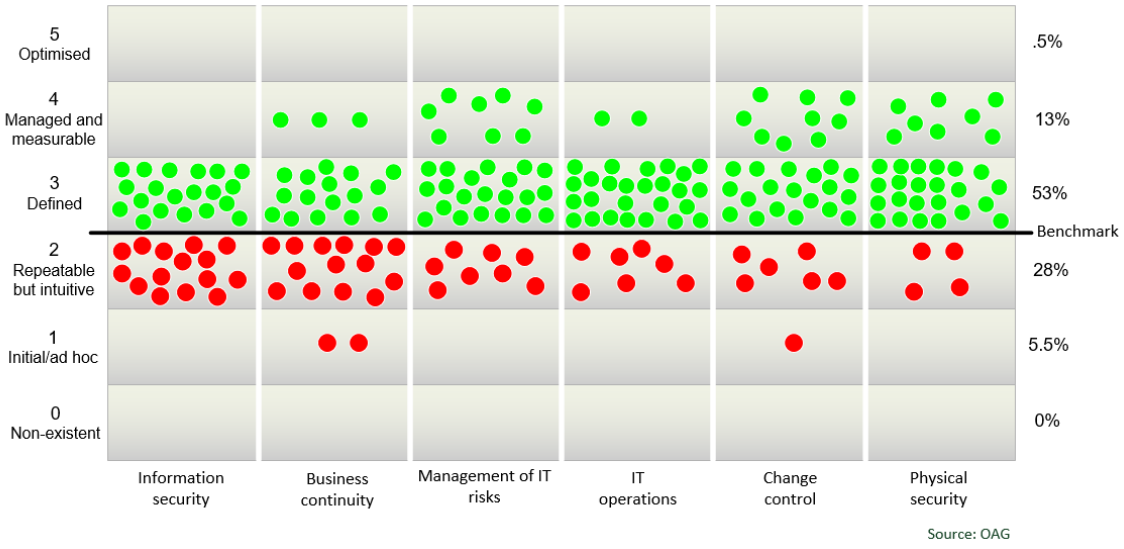
Source: OAG

Table 1: 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.

Findings

While entities improved their controls in 2019, they still need to focus on information security and business continuity controls. Figure 1 summarises the results of our capability assessments across all 6 control categories for the 37 entities we assessed. We expect entities to achieve a level 3 (Defined) rating or better across all the categories.



Source: OAG

Figure 1: Capability maturity model assessment results

Note: Business continuity and information security categories had the most amount of weaknesses.

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

Category	2019 %		2018 %
Information security	57	↑	47
Business continuity	54	↑	50
Management of IT risks	78	↑	69
IT operations	80	↓	82
Change control	80	↑	74
Physical security	89	↑	76

Source: OAG

Table 2: Percentage of entities rated level 3 or above

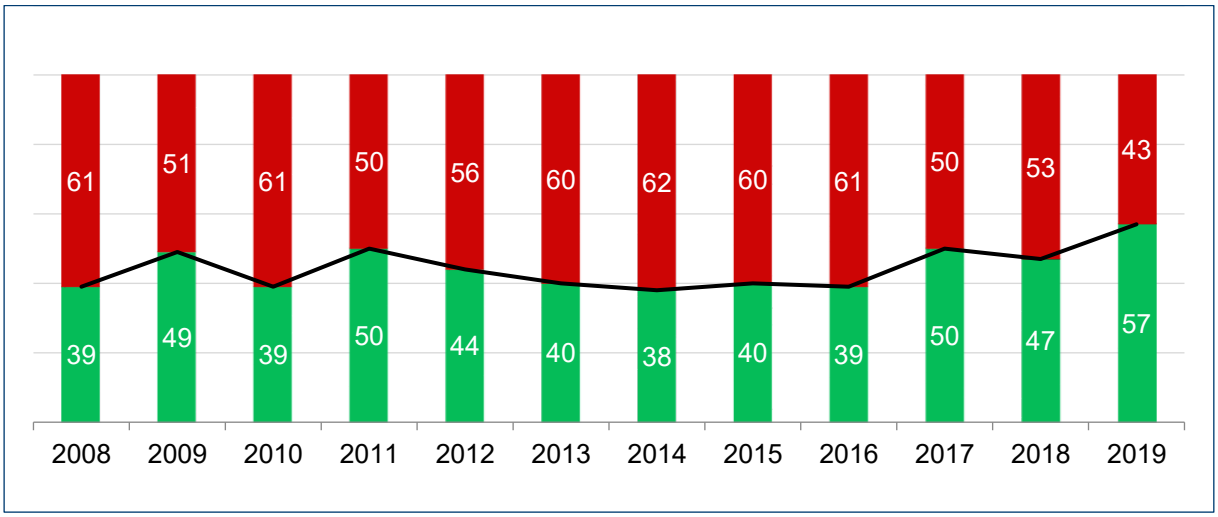
Entities improved their controls across 5 of the 6 categories in 2019. While information security and business continuity show improvement, we continue to find many entities with weaknesses in these areas. Robust controls over business continuity and disaster recovery are particularly important due to risks of large scale disruption associated with pandemics, natural disasters, or the compromise of information systems.

Only 4 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 (7 years at level 3 or higher)
- Racing and Wagering Western Australia (6 years at level 3 or higher)
- Western Australian Land Information Authority (4 years at level 3 or higher)
- Curtin University (4 years at level 3 or higher).

Information security

The number of entities who met our benchmark for information security increased from 47% to 57% in 2019. However, a large number of entities are still not managing this area effectively. The trend across the last 12 years shows slight improvement, but this is not enough to adequately address the risks associated with information security.



Source: OAG

Figure 2: Information security – percentage of entities that met benchmark

Note: Green represents the percentage of entities that met the benchmark and red represents the entities that did not meet the benchmark.

Weaknesses we found included:

- inadequate or out-of-date information security policies
- no review of highly privileged access to applications, databases and networks
- lack of processes to identify and patch security vulnerabilities within IT infrastructure
- no information security awareness programs for staff
- lack of staff training and development in information security
- information classification policy or procedures not in place
- weak password controls without multifactor authentication.

The following case studies demonstrate the risks to entity information when information is not securely managed.

Cloud based finance system with a high risk of unauthorised access

An entity that recently migrated their finance system to the cloud had not implemented appropriate controls. This meant the system had a high risk of unauthorised and inappropriate access. Issues we found included:

- insecure authentication with weak default passwords and no requirement for multifactor authentication for the internet accessible system
- over 190 users had access to sensitive information which included bank account details
- 11 former staff could still access the system due to the weak authentication mechanism
- 16 vendor staff had full administrator privileges to the system, 13 of which didn't need this access
- inadequate and limited audit and security event logs which did not correctly identify users that access the system
- 21 staff with conflicting system roles that allowed them to override management controls for segregation of duties.

By using the above vulnerabilities, we were able to obtain privileged access to all functions in the finance system. The system also did not have appropriate security trails to provide suitable evidence for any forensic investigations.

When combined, these weaknesses could result in a person inappropriately entering and approving an invoice for payment, modifying payee details to their own bank account and processing fictitious journals. Due to the lack of monitoring controls, it would be difficult for this entity to identify and investigate inappropriate or fraudulent transactions and activities.

Source: OAG

Figure 3: Poor information security controls leave entity exposed to fictitious or fraudulent transactions

Payment files are not secure

At 1 entity, we found that plain-text payment files used for processing EFT payroll payments to employees, could be accessed and modified by an excessive number of users. The entity also did not regularly check if there were changes to these payment files.

These weak controls increase the risk that a person with access to the payment file could inappropriately change payment information.

Source: OAG

Figure 4: Lack of controls to protect payment files

Multifactor authentication is important

Many entities' critical systems are accessible over the internet but do not require additional controls such as multifactor authentication. Multifactor authentication adds a layer of security and is a good safeguard against unauthorised access to systems and information.

We also found some entities did not require multifactor authentication for remote access into their network and IT systems, increasing the risk of unauthorised access to entity IT systems and information.

Source: OAG

Figure 5: Internet accessible systems lack controls

Information security is critical to maintain the integrity and reliability of information held in key financial and operational systems, and to protect them from accidental or deliberate threats and vulnerabilities. It is therefore important that entities appropriately manage the confidentiality, integrity and availability of government information and services.

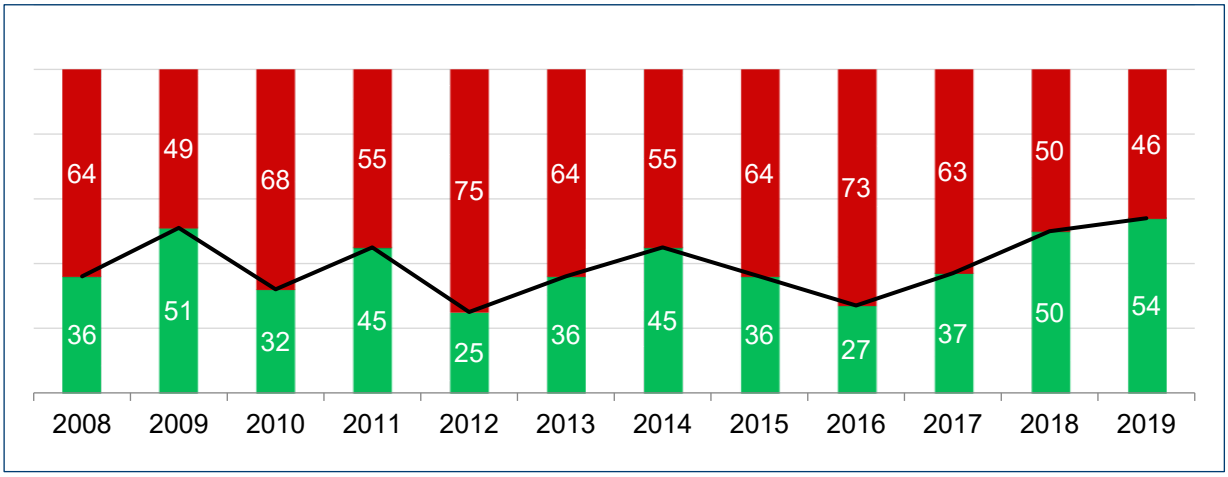
The OAG's own case study highlights the lessons learned from an incident involving inappropriate access to human resources information (see Appendix 1).

Business continuity

We found many entities 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 for recovering 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 6: Business continuity – percentage of entities that met benchmark

Weaknesses we found included:

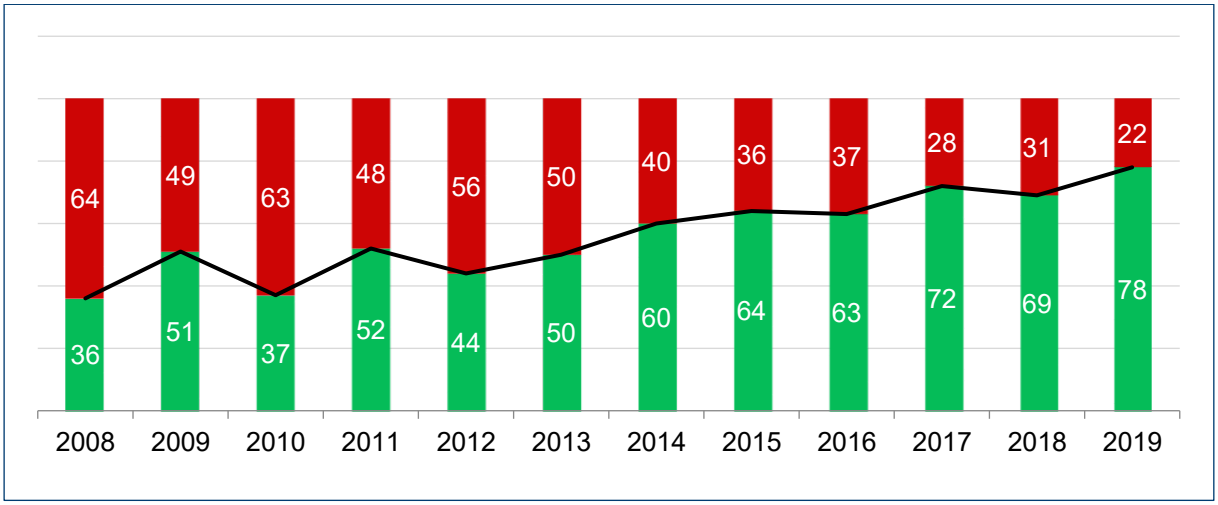
- lack of BCPs or DRPs
- DRPs which did not cover all key systems
- inadequate business impact analysis to prioritise business functions and recovery requirements
- old and redundant DRPs with some not reflecting current information and communication technology (ICT) infrastructure
- untested DRPs and entities not knowing if they can recover systems
- backups were not tested or stored securely.

Without appropriate 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

Seventy-eight percent of entities met our expectations for managing IT risks, a 9% improvement from last year and a 42% increase from our first assessment in 2008.

All entities should have risk management policies and practices that identify, assess and treat risks affecting 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 7: Management of IT risks – percentage of entities that met benchmark

Common weaknesses we found included:

- lack of approved risk management policies
- inadequate processes for identifying, assessing and treating IT related risks
- no risk registers for ongoing monitoring and mitigation of identified risks.

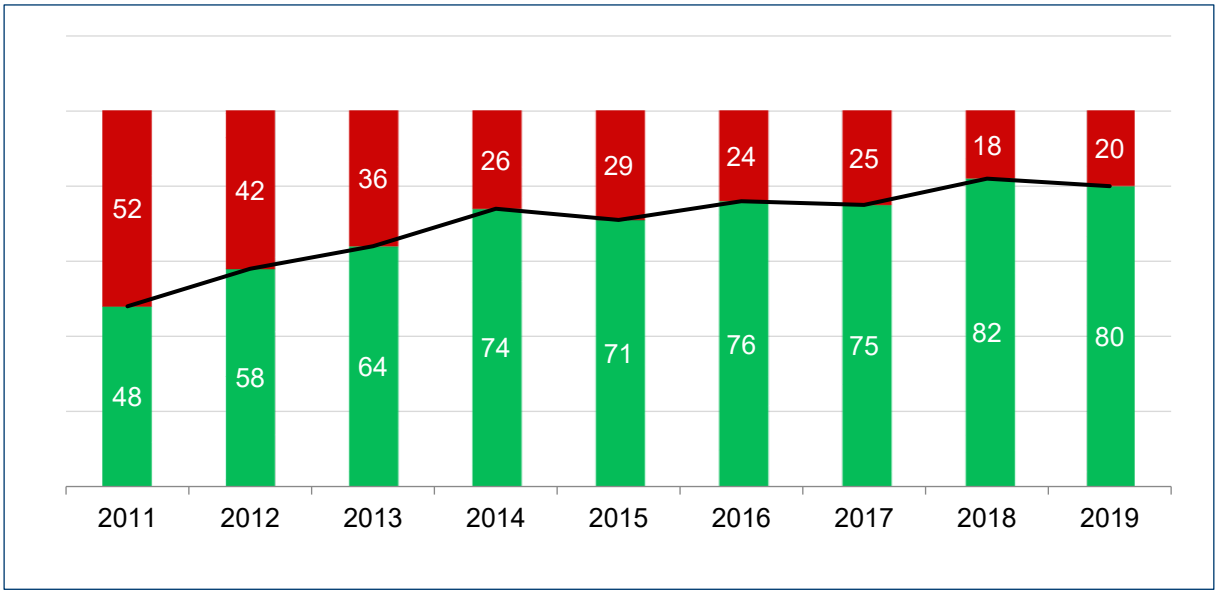
Without appropriate IT risk policies and practices, entities may not identify, and mitigate threats within reasonable timeframes. When risks are not identified and treated properly entities may not meet their business objectives.

IT operations

While there was a slight decline in 2019, many entities' IT practices and service level performance met our benchmark. Overall, there has been a steady improvement since 2011 when we first added this area to our assessment.

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 and segregation of duties.



Source: OAG

Figure 8: IT operations – percentage of entities that met benchmark

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

Weaknesses we found included:

- lack of service level agreements with IT vendors and inadequate contract management
- weak governance over IT operations
- IT strategies not in place
- lack of access reviews and segregation of duties across finance, payroll and network systems
- inappropriate processes to monitor cyber security events
- asset registers not maintained and IT equipment unable to be located.

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.

The following case study demonstrates the risks to entities when IT services are not procured appropriately.

Poor ICT procurement planning

One audited entity did not have effective processes for procuring ICT services. We found instances where ICT services were procured without going to tender. In this case, there were multiple contracts with a single vendor which were below the tender threshold($250,000). However, in aggregate over the year, the committed spend with this vendor was $2.5M which is well above the tender threshold.

Poor ICT procurement practices increases the risk that entities will breach State Supply Commission requirements for procurement or not achieve value for money in its procurement.

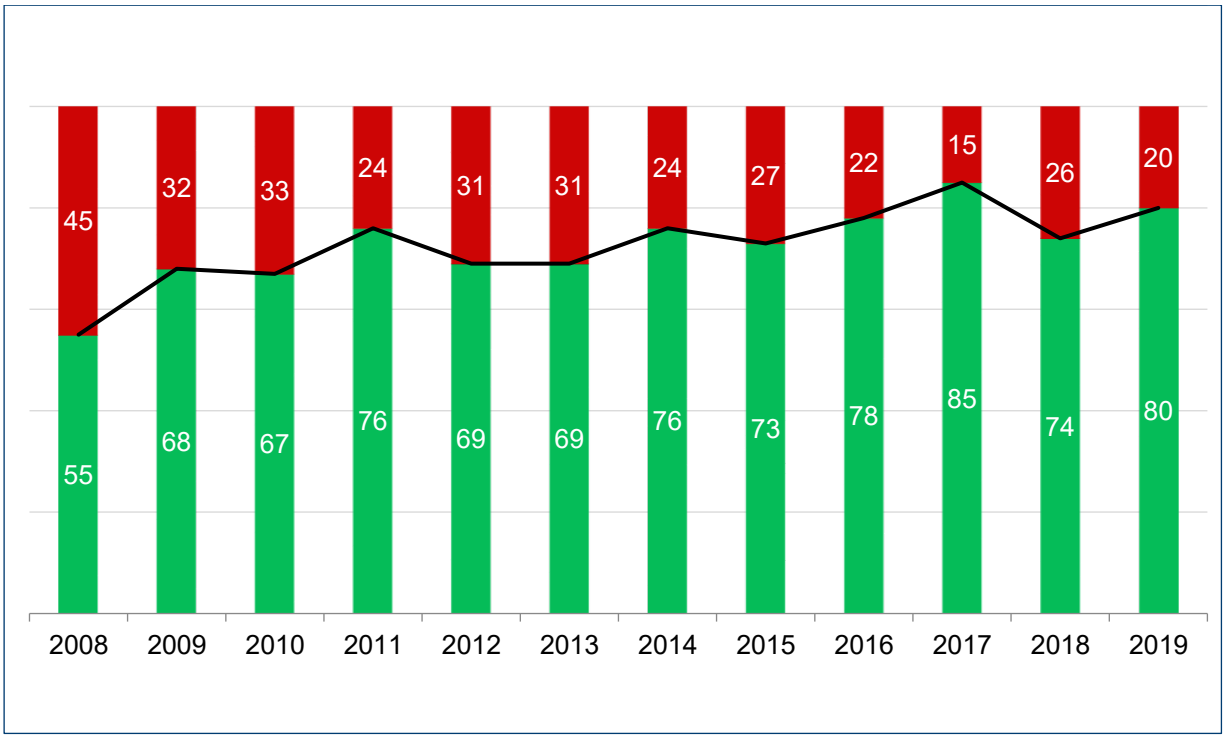
Source: OAG

Figure 9: Poor procurement planning can result in poor value for money

Change control

Entities' change control practices have slowly improved since 2008. In 2019, 80% of entities met our benchmark.

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

Weaknesses we found included:

- no formal system change management policies in place
- changes to critical systems not logged or approved
- changes to systems and critical devices not documented
- no risk assessments performed for major changes to infrastructure.

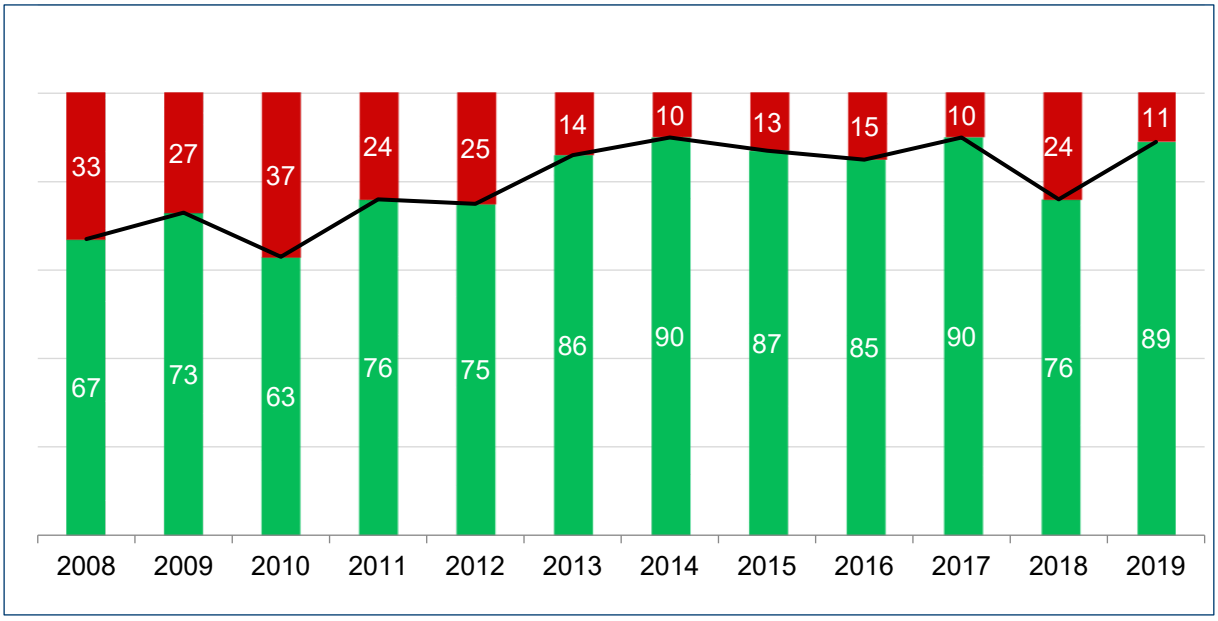
An overarching change control framework is essential to ensuring changes are made consistently, reliably and efficiently. When examining change control, we expect entities to be following their approved change management procedures.

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

There was a 13% increase in performance in this category as 89% of entities met our expectations for the management of physical security.

We examined if 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 had the ability to access or use computer systems.



Source: OAG

Figure 11: Physical security – percentage of entities that met benchmark

Weaknesses we found included:

- no reviews of staff and contactors' access to server rooms
- lack of humidity controls in the server room
- no fire suppression system installed in the server room.

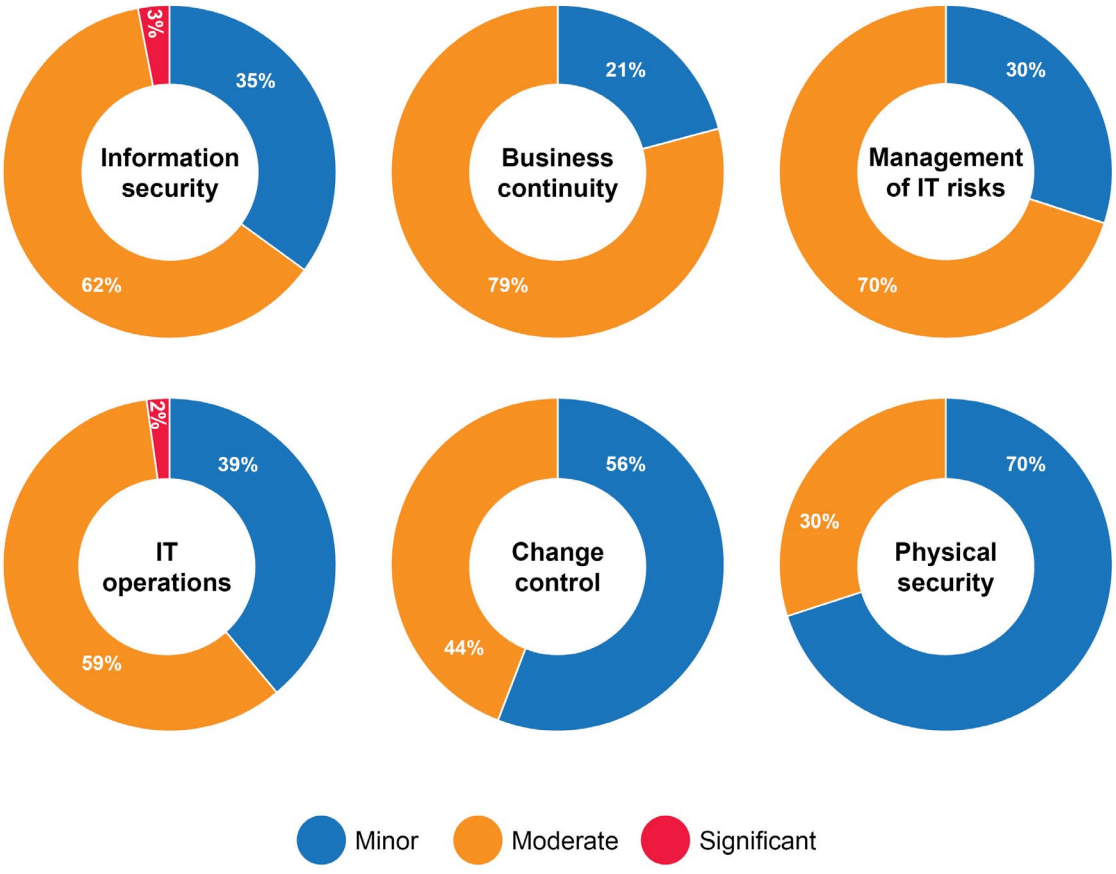
Inadequate protection of IT systems against various physical and environmental threats increases the potential risk of unauthorised access to systems, and information system failure.

The majority of our findings require prompt action

We rated the majority of our findings as moderate as they are of sufficient concern to warrant action being taken by the entity as soon as possible. However, combinations of issues can leave entities with more serious exposures to risk.

Figure 12 summarises how we rated the significance of our findings.

Although we did not rate many findings significant, of particular concern are higher risk findings in the information security and change control areas, as these leave systems directly exposed or can introduce vulnerabilities.



Source: OAG

Figure 12: Distribution of ratings for GCC findings in each control category we reviewed

Recommendations

1. **Information security**

   Executive managers should:

   a. ensure good security practices are implemented, up-to-date, regularly tested, and enforced for key computer systems

   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 information and cyber security awareness and 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 ensure that IT risks are identified, assessed and treated within appropriate timeframes and that these practices become a core part of business activities and executive oversight.

4. **IT operations**

   Entities should ensure that they have appropriate policies and procedures 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 use good practice standards and frameworks as a reference when implementing their own policies and procedures.

5. **Change control**

   Change control processes should be well developed and consistently followed for changes to computer systems. All changes should be subject to thorough 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 damage to computing infrastructure and systems.

Appendix 1 – OAG case study

An internal information access breach was identified at the Office of the Auditor General (the Office) in 2019. While the breach itself was a relatively unremarkable incident, as these breaches are all too common in the digital age, they can have reputational and operational impacts. As such, even a risk-aware entity such as ours can never be complacent about regularly testing the implementation and ongoing effectiveness of access controls.

We share the incident with Parliament and entities to illustrate the importance of contemporary controls that are actively implemented, monitored, and documented in policies and procedures. Staff should be continually trained in using these controls and periodic, executive-level assurance should be obtained to confirm they are functioning as intended.

Incident

The incident involved internal staff inappropriately accessing OAG human resource and other non-audit information in our records management system. In this case, parent file access controls were not automatically inherited by the subsequent new file levels for some records in that system over a period of time.

Detection, investigation and reporting

The incident was detected as a result of changes to personnel and work practices. The Office undertook an internal investigation and, for accountability and transparency purposes, informed Parliament through the Joint Audit Committee, comprising members of the Public Accounts Committee and Estimates and Financial Operations Committee, within a matter of weeks.

Once we investigated and understood the root cause, we promptly addressed the weakness in the internal file access controls. While it is disappointing that a business system control was not effective, and was taken advantage of, this experience provided a critically important learning opportunity for the Office, including the importance of rotating employees so that processes are tested and scrutinised with fresh eyes. An organisational culture of employees speaking up if something does not look right, and executive leaders willing to support action, is critically important. All staff are responsible for information security in their entity, and should inform management immediately if they identify a security weakness.

Actions taken

Key actions the Office took following this incident included:

- acceleration and re-prioritisation of initiatives to improve our information security and monitoring controls, including extensive reviews with periodic independent assurance
- increased executive visibility, awareness and dialogue around information security and internal control mechanisms
- a renewed focus on rotating employees within and between business units
- increased communication with staff around their shared responsibilities relating to information security, and further compulsory training
- increased investment in capability and leadership of the IT branch
- in the absence of a whole-of-government information classification policy, we are in the process of implementing our own information classification policy and procedures.

Appendix 2 – Security considerations for remote working arrangements

In response to the spread of the Coronavirus (COVID-19), entities in all sectors across Australia are encouraging staff to work remotely from home. Rapid transition to these arrangements can introduce risks and challenges for entities who may not have previously implemented large-scale remote working arrangements. It is important that entities manage and address these risks, as well as staff security behaviour, to prevent people from exploiting the current situation to compromise systems and information.

The following table outlines some guiding principles entities should consider when rolling out remote working technology and procedures. This is not intended to be an exhaustive list. Entities can obtain further guidance from the Australian Cyber Security Centre[2] and the Office of Digital Government has recently issued some considerations for remote work.

Principle	Our expectation
Prioritise and simplify	Each entity needs to assess their unique risks associated with remote working arrangements and address critical risks as a priority. These risks will be different for each entity depending on the functions staff perform remotely and the types of information being accessed. Entities should ensure that procedures and technology for remote working are simple and easy to follow. Complex processes can introduce vulnerabilities that could result in undesired outcomes.
Engage with staff	Increase staff awareness by clearly communicating expectations including policies and any occupational health and safety requirements. The business continuity plan may come into effect and it is also important that staff understand how the plan impacts their day to day working procedures. Staff should have easy access to a forum or group where they can seek answers to their queries related to working from home and security.
Remote access technology	The technology used for remote access needs to be secure. The security controls that entities select will depend on the method of remote access, such as: • virtual private network (VPN) • web applications • remote desktop access Remote access servers should enforce technical controls in line with security policies.
Security of network	The majority of the remote workers will use internet to access entity resources. Entities should implement appropriate policies to secure remote access originating from untrusted networks.

[2] https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19

	VPN is one of the better methods of securing remote access because it uses encryption to protect the confidentiality and integrity of communication over the network.
Physical security	Remote working locations may not be as secure as office environments. Entities need to understand the risks associated with this and define and implement appropriate controls to protect information. For example, implementing encryption on portable devices is a simple method to improve security. Entities also need to ensure the security of sensitive hard copy documents is maintained.
Multi-factor authentication	Remote access into entity systems and networks must be secured by strong authentication controls. Entities should implement multi-factor authentication for all remote access.
Bring your own device (BYOD) policies	A risk based policy should define the requirements for personal devices if they are allowed to access entity resources. Personal devices are generally not as secure as those provided by entities and attackers could exploit this weakness as more people work from home. Considerations should be given to: • encryption • access levels • segregated network zone for personal devices • security patch levels • malware controls.
Patch systems	All systems should be patched with latest updates. This applies to all the internet facing infrastructure and client applications.
Stay vigilant	Stay alert and educate staff on the risks especially phishing emails and text messages themed around COVID-19.

Source: OAG based on Australian Cyber Security Centre guidance

Auditor General's reports

Report number	2019-20 reports	Date tabled
17	Controls Over Purchasing Cards	27 March 2020
16	Audit Results Report – Annual 2018-19 Financial Audit of Local Government Entities	11 March 2020
15	Opinion on Ministerial Notification	28 February 2020
14	Opinion on Ministerial Notification	31 January 2020
13	Fee-setting by the Department of Primary Industries and Regional Development and Western Australia Police Force	4 December 2019
12	Audit Results Report – Annual 2018-19 Financial Audits of State Government Entities	14 November 2019
11	Opinion on Ministerial Notification	30 October 2019
10	Working with Children Checks – Follow-up	23 October 2019
9	An Analysis of the Department of Health's Data Relating to State-Managed Adult Mental Health Services from 2013 to 2017	9 October 2019
8	Opinions on Ministerial Notifications	8 October 2019
7	Opinion on Ministerial Notification	26 September 2019
6	Opinions on Ministerial Notifications	18 September 2019
5	Fraud Prevention in Local Government	15 August 2019
4	Access to State-Managed Adult Mental Health Services	14 August 2019
3	Delivering Western Australia's Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

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
F: 08 6557 7600
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for
Western Australia