Western Australian
Auditor General's Report

Information Systems Audit Report 2020 – Local Government Entities

Report 27: 2019-20
25 June 2020

Office of the Auditor General
Western Australia

Audit team:
Jordan Langford-Smith
Kamran Aslam
Walber Almeida
Karla Cordoba
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 – Local Government Entities

Report 27: 2019-20
June 2020

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2020 – LOCAL GOVERNMENT ENTITIES

This report has been prepared for Parliament under the provisions of section 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 assistance provided by the staff at the entities included in our audits.

CAROLINE SPENCER
AUDITOR GENERAL
25 June 2020

Contents

Auditor General's overview

I am pleased to present our first local government Information Systems Audit report since the proclamation of the *Local Government Amendment (Auditing) Act 2017*. The report summarises the results of the 2019 cycle of information systems audits at 10 local government entities.

Our general computer control audits are a fundamental part of our financial audits. They help to provide assurance that the financial information generated by information systems is accurate, reliable and completely recorded. While local governments will differ in the size and scale, it is critical that they have effective controls to manage information systems.

The report has 2 parts:

- Information systems – security gap analysis
- General computer controls and capability assessment of local government entities.

The security gap analysis benchmarks the results of local government entities' security practices against a globally recognised standard. This standard provides a set of controls which entities can easily implement to protect critical information from internal and external threats. The standard provides useful guidance on how entities can address weaknesses and risks to their information security. My Office performed a similar exercise for State government entities in our 2013 Information Systems Audit Report.

We found that all 10 local government entities had significant shortcomings in their information security practices. Entities need to seriously consider these standards and the recommendations in this report to improve information security practices and protect the confidentiality, integrity and availability of information and systems.

The second part of this report outlines the results of our general computer controls audits and capability assessments. Overall, the level of maturity in the reviewed local government entities was low, with no entity meeting our minimum benchmark across all control categories.

Local government entities' information systems are integral for delivering key public services. However, most of the entities do not have a holistic view of activities that pose risks to their information systems. Entities should have visibility over their systems and take a strategic approach to address these risks.

International standards provide a good framework and starting point for entities to develop and implement sound practices in their operational and strategic security processes. My Office will continue to monitor and report on general computer controls and capability assessments of local government entities. We expect to see better results similar to the improvements made in the State sector in recent years as reported through our regular information system audit program.

Information systems – security gap analysis

Introduction

The objective of this security gap analysis was to determine whether local government entities are adopting adequate controls in managing their information security. We assessed the information security controls at 1 regional and 9 metropolitan local government entities of varying size to determine whether they met the requirements of International Security Standard 27002 (AS ISO/IEC 27002:2015). This standard provides a framework and set of controls to ensure IT environments are managed to preserve the confidentiality, integrity and availability of information. Most of these controls are globally recognised as good practice and require minimal effort to implement.

Conclusion

All audited entities had significant gaps in their management of information security when compared against the standard. We found that entities did not have good practices to manage information and cyber security. Entities did not have appropriate policies and processes to identify and guide information security practices and they often lacked ongoing monitoring processes to detect and respond to threats. These gaps in security controls seriously undermine the confidentiality, integrity and availability of information held by these entities.

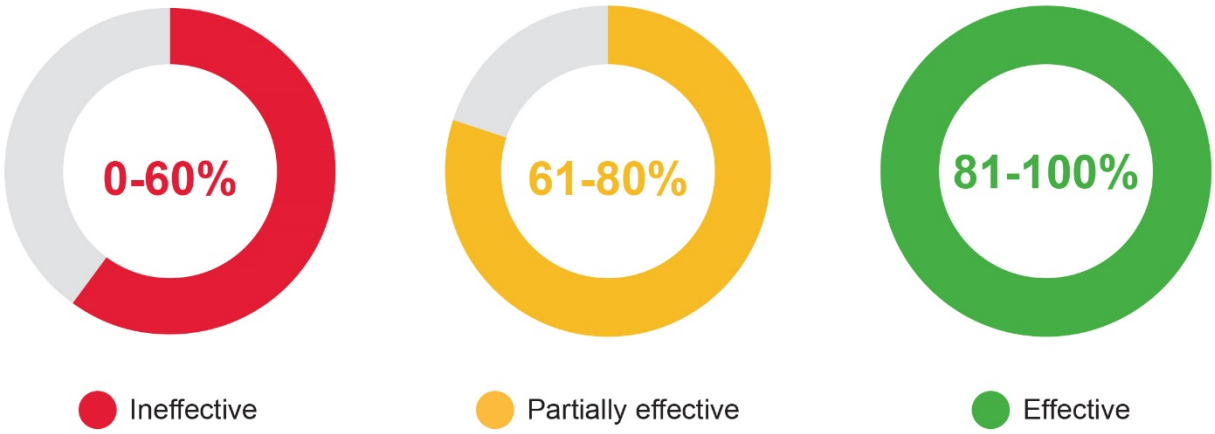
Background

Local government entities hold information, including confidential information about people and the community, which is fundamental to their operations and should be protected from external and internal threats. As IT systems and computing environments become more interconnected, the amount of information grows, along with the number and diversity of threats. Effective information security involves managing people, processes and technology to preserve the confidentiality, integrity and availability of information.

Entities can use the information security standard as a starting point to develop sound practices, or to assess their current controls. The standard has 14 areas with each area containing various controls that can be tailored to needs, size and complexity of entities.

In order to determine an overall rating for each area, we:

- determined which controls were applicable
- assessed and gave individual controls a score
- consolidated these scores to calculate an overall result which considered the number of effective controls in the area
- rated scores above 80 percent to be effective, scores from 61 to 80 percent as partially effective, and below 61 percent as ineffective.



Source: OAG

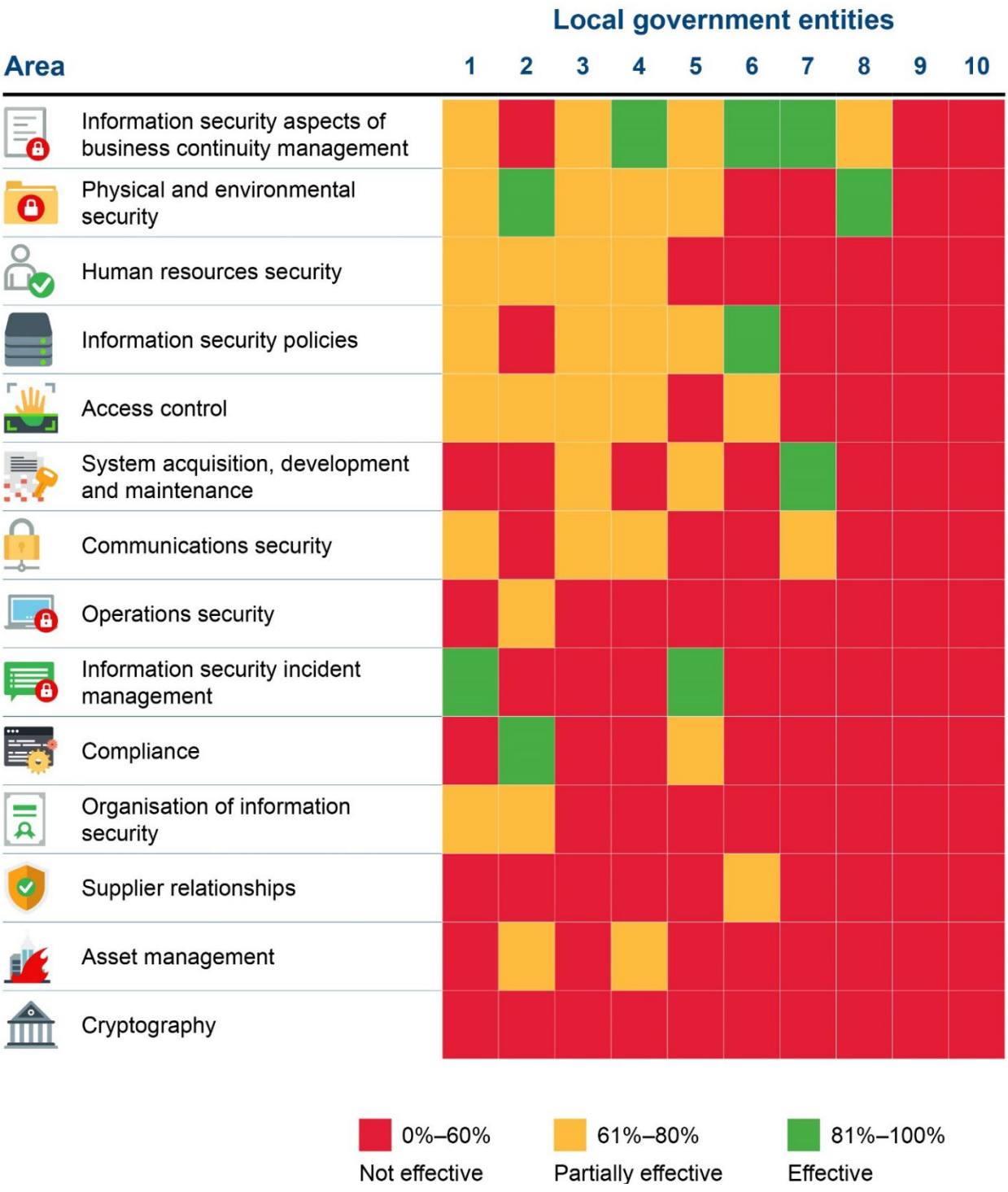
Figure 1: Scale to score entity controls

We evaluated if entities were effectively meeting information security best practices by comparing their controls against the 14 areas of the ISO 27002 standard. In performing this work, we also assessed if:

- entities had identified and defined the security requirements based on risks to their information systems
- appropriate controls were in place to mitigate information security risks
- mitigating controls were in place where practices did not align with international standards.

What we found

All of the audited entities had significant gaps in meeting the good practice standard across several control areas (Figure 2). Only 4 entities demonstrated that they were effective, or partially effective in at least 7 of the 14 areas. In order to protect the security of the information and systems of the audited entities, we have not named them in this report. We provided each audited entity with a copy of their gap analysis results.



Source: OAG

Figure 2: Results of security gap analysis for 10 local government entities

Each entity has unique security requirements based on their business needs. However, the majority of the entities had not assessed and identified their security requirements. Generally, security requirements can be identified through:

- assessing risks, taking into account the overall business strategy and objectives including vulnerabilities and threats to assets
- understanding legal, statutory and contractual requirements that apply to the entity and its contractors and service providers

- understanding the set of principles, objectives and business requirements for information handling to support operations.

Security policies did not provide direction and support for information security

Half of the entities did not have adequate policies outlining their approach for managing information security objectives. We found that policies did not contain guidance for key areas, including:

- roles and responsibilities for information security management
- access management
- protection from malware or malicious code
- use of IT assets and technical vulnerability management.

It is critical that entities take a strategic approach to information security by understanding the risks and implementing appropriate policies for the governance of security.

Additionally, none of the entities had a policy or a management approach on the use of cryptography controls, with all 10 entities rated as ineffective. A lack of guidance or direction for cryptography controls increases the risk that the confidentiality and integrity of information held by these local government entities could be compromised.

We also found 90% of the entities did not have good processes to check compliance with security requirements. For example, performing periodic internal reviews is a good way to ensure controls are working as expected. Without processes to detect policy breaches and non-compliance, entities cannot determine if their controls are operating effectively.

Poor controls risked network and operations security

Nine of the 10 entities did not have good practices to manage operational security. Without good practices, entities are at greater risk that internal and external threats will compromise their systems.

Operational security deals with day-to-day activities related to information processing and communication facilities. The weaknesses we found in controls over network and operations security included:

- a lack of change management processes. Changes may inadvertently introduce risks if they are not appropriately managed and tested prior to implementation
- network security appliances are not securely managed as they use insecure protocols. Insecure protocols that exchange information in plain-text can be used to compromise networks
- firewall events are only retained for limited periods and staff use shared generic accounts to administer firewalls. This makes it difficult to investigate and hold malicious users accountable as actions cannot be linked to them
- there were no processes to adequately assess and remediate security weaknesses. These weakness could be exploited to gain unauthorised access to entity systems and information
- a lack of controls to observe and review network activities. This could result in unauthorised or malicious activity going undetected
- data backup plans did not reflect current IT infrastructure. Also, entities were not testing the integrity of data on backups. Without appropriate backups and testing, entities risk

permanent data loss and may not be able to deliver their core services if systems or information are compromised

- inadequate segregation of networks. Weaknesses in a part of the network may enable malicious actors to access the entire network
- anti-malware controls were not installed on key servers. This could result in malware infections and compromise of systems and critical information.

Most entities had business continuity strategies but few had tested these

Three entities in the sample had good practices to manage business continuity and information security aspects during disaster situations. Four entities had not verified their capability to recover and ensure security of information during a serious interruption, and only partially met the standard. It is crucial to have well developed and verified business continuity and recovery strategies that address the security of information in crisis situations.

The remaining 3 entities had not adequately defined the information security requirements and plans in a disaster situation and consequently had inadequate business continuity and recovery strategies. This meant that a disaster or pandemic could disrupt their key services for prolonged periods and potentially compromise information security.

Poor access management controls resulted in inappropriate access

Half of the entities did not have good processes to manage access to systems and networks. The remaining half had partially effective controls to manage access. Some of the weaknesses we found include:

- a number of former staff still had access to systems. We found instances where systems were accessed inappropriately by former employees without an adequate explanation
- no formal process was in place to request and authorise access to systems
- weak password and authentication controls
- a lack of processes to review user access and privileges.

These control weaknesses significantly exposed entities to unauthorised access to systems and information.

Entities risked not effectively responding to security incidents

Only 2 entities had an appropriate plan to manage information security incidents. The remaining 8 entities did not have response plans, awareness programs and procedures for detecting security incidents and handling of forensic evidence to effectively manage security incidents. These controls are important to detect and appropriately respond to security incidents. Without robust and effective processes for responding to and managing security incidents, entities could face extended service outages and reputational damage in the event of an incident.

Information was at risk due to inadequate supplier management controls

The majority of the audited entities did not document or demonstrate their understanding of information security risks associated with the use of suppliers or contractors. Entities regularly employ contractors or procure systems to deliver key services. As part of this process, they may allow contractors to access information or store data on contractor managed systems. Even if entities use contractors, they are responsible for protecting their

information and managing how it is used. Understanding vendors, their security posture, services and systems is vital in maintaining effective information security controls.

Only 1 entity had partially effective controls to manage supplier risks. Without these controls there is an increased risk that entity information is exposed to unauthorised access and disclosure. In addition, by not embedding information security controls and practices into arrangements with suppliers and contractors, entities may have limited recourse in the event of an information security incident.

Physical and environmental security could be improved

Two entities met good practice standards in this area and 4 entities had partially effective controls. The remaining 4 entities were not managing the physical and environmental controls well. These entities have not formally defined the roles and responsibilities for managing the server room and their physical access controls were not operating effectively. For example, fire suppression systems were not installed, an excessive number of staff had access to server rooms, and access was not monitored. These weaknesses could result in unauthorised access to assets and accidental or deliberate damage to systems and information.

Information security controls were not considered over the lifecycle of information systems

Seven entities did not have good practices for managing their information and IT assets over the lifecycle of information systems. In particular, these entities did not have adequate plans and procedures to manage the acquisition, maintenance, disposal and re-use of IT and information assets. It is important to identify all assets that process information to ensure these are appropriately protected and the information on the assets cannot be inappropriately accessed, even after disposal.

We found that the majority of the entities had not defined how to classify information based on its value, legal requirements, criticality and sensitivity. As a result, appropriate security controls were not applied to information and assets based on these factors, increasing the risk to sensitive information.

Inadequate human resource security controls could threaten information security

Six entities did not have effective controls to ensure that information security risks were appropriately managed when staff were hired or terminated. The remaining 4 entities only had partially effective controls. Some of the weaknesses we identified include:

- no defined requirements for background checks before employing staff and contractors
- confidentiality and non-disclosure agreements not required for new staff
- inadequate induction and ongoing programs to inform staff and contractors of their information security responsibilities.

People play a fundamental role in maintaining information security. It is crucial that suitable people are hired, staff understand their responsibilities for information security and that the security of information is managed properly when staff leave the organisation. Poor practices for managing staff increase the risk of information or systems being compromised.

Recommendations

Local government entities should:

1. understand and assess the risks unique to their business activities and environment to inform their strategy for information security management
2. assess their controls against good practice standards to identify gaps and develop plans to improve information security. Entities can seek further guidance from other good practice standards. For instance, the Australian Cyber Security Centre maintains the *Australian Government Information Security Manual*[1] to assist entities in protecting their information and systems. The National Institute of Standards and Technology publishes *NIST Cybersecurity Framework*[2] to help organisations improve the management of cybersecurity risks
3. implement processes to continuously monitor and improve information security controls to ensure they meet entity needs.

Under section 7.12A of the *Local Government Act 1995*, the 10 audited entities are required to prepare an action plan addressing significant matters relevant to their entity for submission to the Minister for Local Government within 3 months of this report being tabled in Parliament and for publication on the entity's website. This action plan should address the points above, to the extent that they are relevant to their entity.

[1] https://www.cyber.gov.au/ism

[2] https://www.nist.gov/cyberframework

General computer controls and capability assessment results for local government entities

Introduction

In 2018-19, we audited the general computer controls (GCCs) at a sample of 1 regional and 9 metropolitan local government entities. Our GCC audits are integral to our annual financial audits of local government entities as they help to determine whether computer controls effectively support the confidentiality, integrity, and availability of information systems needed for annual financial reporting.

Information systems underpin most aspects of local government operations and services. It is important that entities implement appropriate controls to maintain reliable, secure and resilient information systems. These controls are equally important in smaller local government entities who may not have a dedicated IT department or staff, but may rely on contractors to provide the necessary support.

We use the results of our GCC work to inform our capability assessments of entities. We asked entities to self-assess their capability maturity across the 6 control categories using our assessment criteria. We then met with each of the entities to compare their assessment with ours, which was based on the results of our GCC audits.

Capability maturity models (CMMs) are a way to assess how well-developed and capable entities' established IT controls are. The model provides a benchmark for entity performance and a 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.

We focused on the following 6 categories to determine the maturity of entity control environments:

Source: OAG

Figure 3: GCC categories

Conclusion

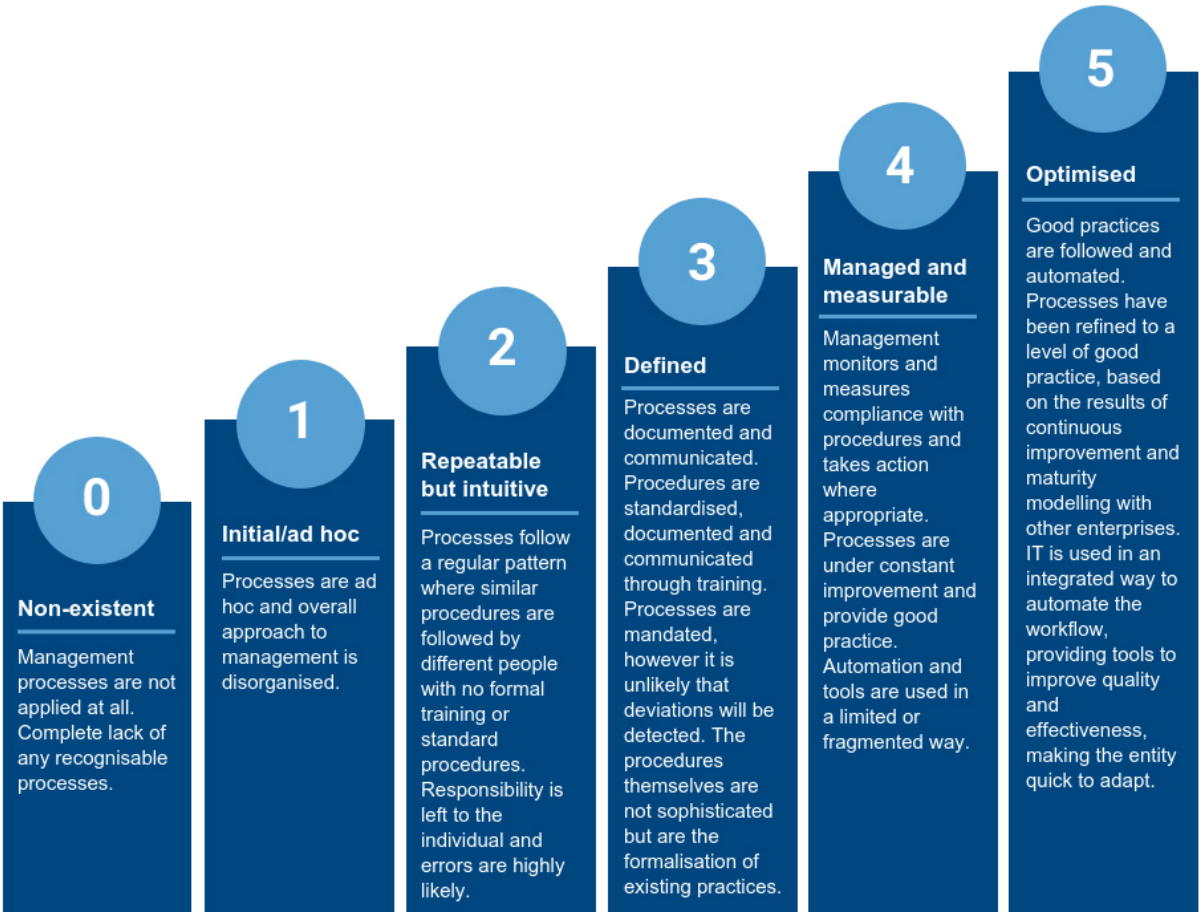
All 10 local government entities need to improve their general computer controls. We reported 150 control weaknesses across the 10 entities, with 13 of these weaknesses rated

as significant. As these weaknesses could significantly compromise the confidentiality, integrity and availability of information systems, the local government entities need to act promptly to resolve them.

Our capability assessment results show that none of the entities met our expectations across all control categories. We found weaknesses in controls for information security, business continuity, change management, physical security and IT operations, with many entities falling below our benchmark. Whilst some entities had good IT risk policies, others need to improve how they identify and treat information risks.

Audit focus and scope

We conducted GCC audits and capability assessments at 10 local government entities. We used a 6 point rating scale[3] from 0 to 5, detailed in Figure 4, to evaluate each entity's capability maturity level in each of the GCC categories. The model provides a reference for comparing entity results from year to year. We expect entities to achieve a level 3 (Defined) rating or better across all the categories.



Source: OAG

Figure 4: 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.

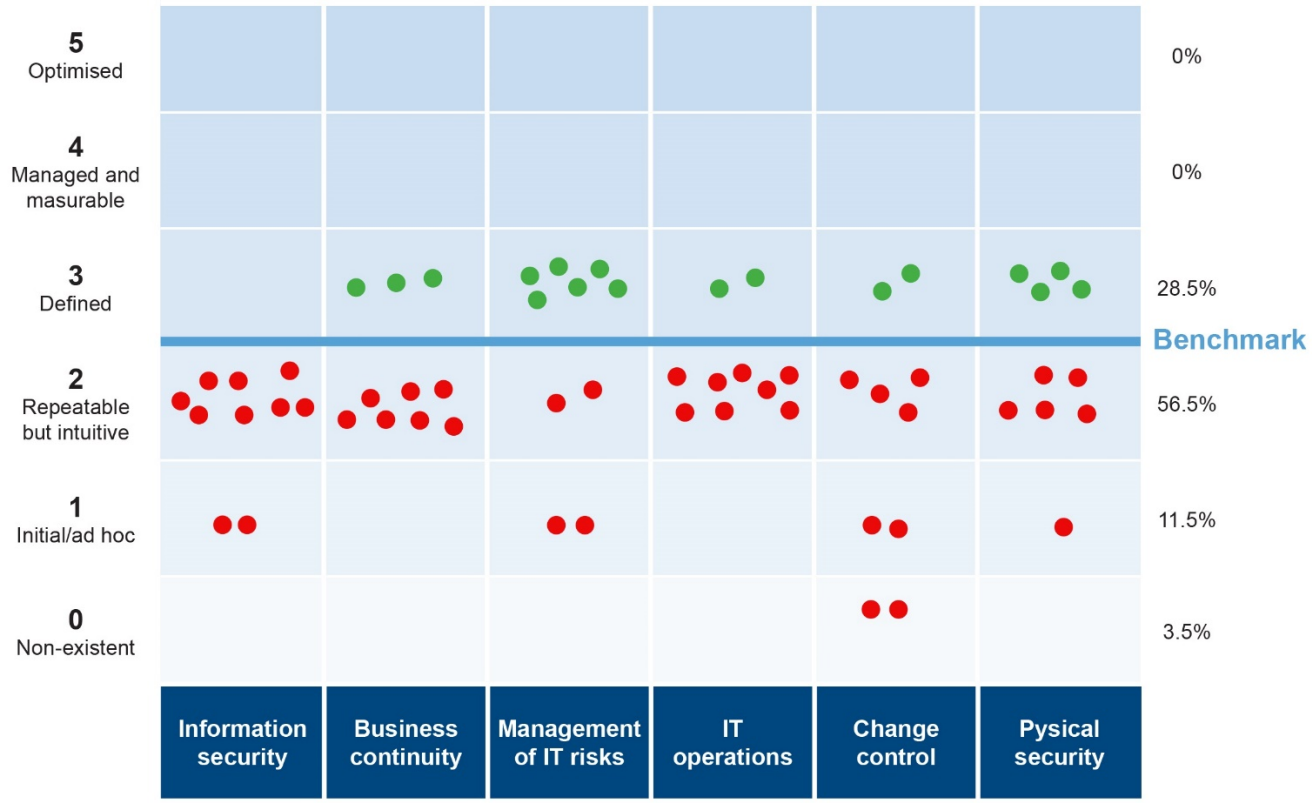
What we found

Capability maturity model assessment results

None of the local government entities we reviewed met our expectations across all control categories.

Entities did not have adequate controls to effectively manage information security, change management, IT operations, physical security and continuity of business. Poor controls in these areas left systems and information vulnerable to misuse and could impact critical services provided to the public. We have included specific case studies that provide more detail where we identified weaknesses in controls that could potentially compromise entities' systems.

Figure 5 shows the results of our capability assessments across all 6 control categories for the 10 entities we assessed.



Source: OAG

Figure 5: Capability maturity model assessment results

Information system controls

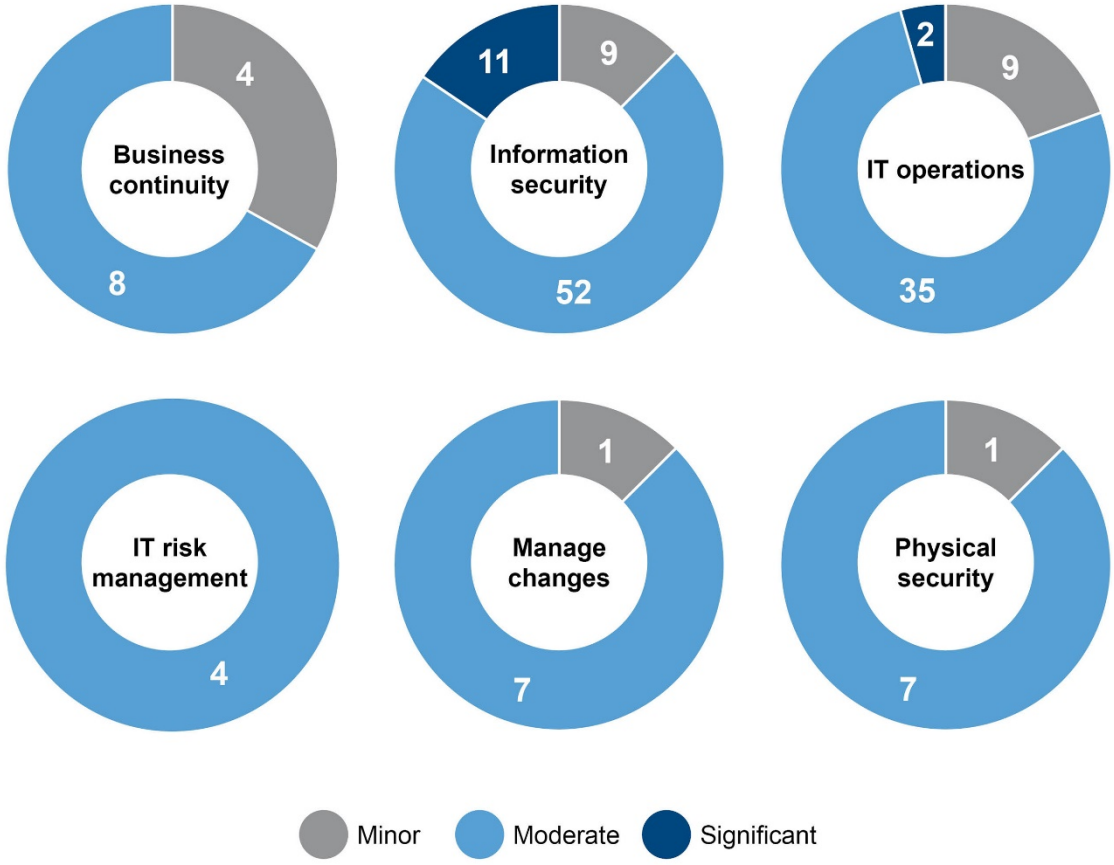
We reported information system control weaknesses identified during our GCC audits to local government entities in management letters. We identified 150 GCC control weaknesses across 10 entities, with 9% of the weaknesses rated as significant requiring prompt action, 75% as moderate which should be addressed as soon as possible, and the remaining 16% as minor. Nearly half of all issues were about information security which was also the category that had most of the significant findings.

Management letters issued to entities contained all the findings. However, we removed sensitive technical details which, if made public, could increase the risk of cyber-attacks for

those entities. We reported these details separately through confidential letters to each local government entity to assist them in addressing the weaknesses. Entities generally agreed to implement the recommendations included in our management letters.

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

While the majority of our findings are rated as moderate, a combination of these issues can leave entities with more serious exposure to risk.



Source: OAG

Figure 6: Distribution of ratings for GCC findings in each control category we reviewed

Information security

Good information security practices are critical to protect the information held in key financial and operational systems from accidental or deliberate threats and vulnerabilities.

We found that all 10 local government entities need to improve their practices for managing information security, with no entity meeting our benchmark. We reported 72 issues, nearly half related to the security of information and systems. It is concerning that 11 were rated as significant requiring prompt attention, as they seriously exposed the entity's systems and information to misuse.

Several entities had not clearly defined roles and responsibilities for information security. This, coupled with a lack of appropriate policies and practices, meant their approach towards security was inconsistent and ad-hoc.

A common weakness we found at most entities was a lack of processes to identify and patch security vulnerabilities in systems and ICT infrastructure. Our vulnerability scans of key entity systems identified a range of critical and high severity vulnerabilities which had not been

patched. These left the systems open to compromise. Our better practice guidance at Appendix 1 provides practical information to help entities manage their vulnerabilities.

The following case studies were selected to highlight the risks to entity information from systems not regularly being patched and inadequate access controls, including remote access.

Information and systems are at risk due to inadequate vulnerability management

One of the audited entities did not have appropriate processes to identify and patch security vulnerabilities leaving systems vulnerable to exploitation through unauthorised and inappropriate access. Weaknesses included:

- The entity did not perform regular vulnerability assessments to identify and address weaknesses in a timely manner.
- It also did not have a process to identify vulnerable devices or computers on the network. It is extremely important to have visibility over devices connected to the network, and their vulnerabilities. Our scans identified an unmanaged computer on the network which was still susceptible to well-known critical software vulnerabilities including EternalBlue, Petya and Bluekeep. Patches to address EternalBlue and Petya vulnerabilities were released by mid 2017.
- Over 340 critical and 1500 high severity vulnerabilities on a sample of 50 servers and workstations.
- The entity's security update processes did not include core network devices such as firewalls, routers and switches, leaving them outdated and exposed.

Without an effective process to identify, assess and address relevant vulnerabilities in a timely manner, there is an increased risk that systems will not be adequately protected against potential threats. These vulnerabilities could be exploited and result in unauthorised access to IT systems and information.

Source: OAG

Figure 7: Poor vulnerability management leaves an entity exposed to cyber attacks

Excessive privileges and poor controls to manage infringements and rates could result in fraud

One entity we audited did not have adequate controls in place to manage its rates and infringement receipting system. We identified the following issues:

- A large number of users had excessive privileges to access system functions. For example, we found a number of users who had high level access to a range of functions including receipting, rates accounting and infringements.
- Generic accounts were used to process infringements and rate payments. These generic accounts did not require network authentication and bypassed security controls to access information and resources. In the event of error or wrongdoing, the entity would not be able to attribute responsibility to a particular user.
- Former staff still had infringement books assigned, used to issue fines to the public.
- There was no process to reconcile infringements that had been cancelled, or numbers in the fine sequence that had been skipped. The entity could not provide any information or reasons for cancelled infringements or the missing numbers. This basic control is fundamental to ensuring revenue is fully collected and there is no inappropriate issuance or cancellation of fines by current or former staff.
- There was no visibility to determine if users directly accessed or modified the infringement and rates system database. Infringements or rates notices could therefore be altered without an auditable trace or log.
- The servers for the infringement and rates system were not patched and were exposed to serious software vulnerabilities including EternalBlue and WannaCry.

When combined, these weaknesses could result in a person inappropriately modifying rates or infringement information, or receiving payments without processing them through the system. Due to the use of generic accounts not linked to any person and the lack of monitoring controls, it would be difficult for this entity to identify inappropriate or fraudulent transactions and activities, or investigate who is responsible. In addition, vulnerabilities in the system could be exploited to compromise the confidentiality, integrity and availability of systems.

Source: OAG

Figure 8: Lack of controls to manage the rates and infringement system

Poorly controlled remote access exposes entity's systems and information

One local government entity we audited provided remote access to its staff and contractors but did not have appropriate controls to manage associated risks.

We found:

- Staff and contractors used their personal devices to remotely connect to the entity network and systems. However, the entity had not defined the minimum security controls that these devices needed.
- We identified 6 external contractors with domain administrator privileges to the entity's network. Three of these contractors were not working on any active projects and 2 had not used their access in 4 years.
- Remote access system settings were not secured and publically exposed sensitive information such as the underlying operating system version and internal network information. This could be used by people with malicious intent to compromise the entity network and systems.
- The entity did not require multifactor authentication for remote access. This provides an additional layer of security to the remote system from unauthorised access attempts.
- The remote access infrastructure contained security misconfigurations, unsupported systems and missing patches. These weaknesses could be exploited to gain unauthorised access to the entity systems.

Source: OAG

Figure 9: Internet accessible systems lack controls

Business continuity

Good continuity planning helps ensure that key business functions and processes are restored promptly after a disruption. Business continuity and disaster recovery plans should be regularly tested. This minimises the risk of extended outages which could disrupt the delivery of important services.

We found that 7 of the 10 audited entities did not have up-to-date business continuity and disaster recovery arrangements in place. Some plans had not been updated since 2013 and may not reflect current business practices and IT infrastructure. As a result, in the event of a disruption or disaster, entities may not be able to restore and continue business processes and functions.

Weaknesses in business continuity and disaster recovery planning could have a serious impact on the critical services local government entities deliver to the public. To ensure business continuity, entities should have an up-to-date business continuity plan, disaster recovery plan and incident response plan. The business continuity plan defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the disaster recovery plan. The incident response plan needs to consider potential incidents and detail the immediate steps to ensure timely, appropriate and effective response.

Management of IT risks

Six of the 10 local government entities we reviewed had good policies and procedures for managing IT risks. This was the control category where entities performed best. However, some common weakness at the other 4 included:

- a lack of risk management policies
- inadequate processes to review and report risks to senior management
- no risk registers for ongoing monitoring.

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.

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

IT operations

Only 2 of the 10 entities had adequately defined their requirements for IT service levels and allocated sufficient resources to meet these requirements. IT operations include day-to-day tasks designed to keep services running, while maintaining data integrity and the resiliency of IT infrastructure. In this area, we tested whether entities had formalised procedures and monitoring controls to ensure processes were working as intended.

Common weakness we found included:

- a lack of asset registers to track and monitor IT equipment which may lead to assets being lost or stolen and unintentional disclosure of information
- inadequate processes to ensure compliance with software licensing agreements. This could result in penalties for breaching licencing arrangements
- a lack of service level agreements with IT vendors and poor contract management practices leading to inadequate oversight of vendors or paying for services not provided
- inadequate retention and management of event logs. This means entities cannot track or identify malicious activities, nor they can investigate them
- a lack of access reviews which could result in inappropriate access.

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 studies highlight the risk to entities when devices and their events are not regularly monitored, and assets are not effectively managed.

No monitoring of inappropriate or malicious network activities

One entity had configured their network to log activities and events that occurred on their ICT infrastructure. However, there was no routine process to review those events.

The entity performed an informal review of logs and identified that a staff member had not complied with their acceptable use policies. Over a number of months, the staff member made several attempts (unsuccessfully) to access inappropriate websites featuring pornography. These websites are often carriers of malicious content and could put the entity's reputation at risk.

While it was good that there were controls in place to prevent access to inappropriate websites, and the entity took disciplinary action against the staff member, this case study highlights the importance of having formal processes for reviewing and monitoring logs to gain insights into inappropriate network activities. If proactive monitoring of important events is not is place, entities cannot detect any unauthorised or malicious activity or take timely corrective action. If it had not been for the informal review, the entity may not have identified inappropriate access attempts.

Entities can use centralised log management systems, such as Security Information and Event Management system, to analyse security events efficiently and effectively.

Source: OAG

Figure 10: Importance of regularly reviewing log events

Inadequate processes to manage IT assets

Another entity did not have appropriate processes to manage the lifecycle of IT assets. Issues we identified include:

- no policies relating to the disposal and re-use of assets
- computers donated to an external organisation without securely erasing data
- records of asset disposals were not maintained.

There is a high risk of unauthorised and unintentional disclosure of entity information if it is not securely removed from computers prior to disposal.

Source: OAG

Figure 11: Unauthorised disclosure of entity information

Insecure management of network devices

One local government entity did not manage its firewalls effectively. Issues we identified include:

- inappropriate firewall configuration which could allow external attackers to compromise the internal network
- individuals used shared generic accounts to administer the firewall which made it impossible to attribute actions to an individual
- backups of the firewall settings were not performed, leaving these vulnerable in the event of failure
- firewall security events were only retained for a short period (3 weeks) and alerts were not setup for critical events. This may make it difficult for the entity to detect or investigate security breaches, if required
- the firewall license for content filtering had expired, which allowed unrestricted access to all websites including those with inappropriate content.

The network and information systems are at a risk of compromise if network appliances are not managed appropriately.

Source: OAG

Figure 12: Increased risk of network compromise

Change control

We found that only 2 of 10 entities had appropriate processes to implement changes in their IT systems and infrastructure. We reviewed whether changes to systems were authorised, tested, implemented and recorded in line with management's intentions. Weaknesses we found included:

- a lack of formal system change management procedures. This increases the risk that changes, including those that may be harmful to systems and information, could be implemented without assessment
- no records of changes made to critical systems. This would make it difficult to investigate incidents that may have been caused by changes.

If changes are not controlled, they can compromise the security and availability of systems. As a result, systems will not process information as intended and entities' operations and services may be disrupted. There is also a greater chance that information will be lost and access given to unauthorised people.

We expected entities to have formal policies and procedures to ensure changes were risk assessed, tested, sufficiently documented and authorised prior to being implemented. This helps to ensure that changes to systems are consistent and reliable.

Physical security

Over half of the entities (6 of 10) did not have appropriate controls to protect their IT systems and infrastructure against environmental hazards and unauthorised access to server rooms. This means entities are at increased risk of unauthorised access and failure of information systems.

The following case study shows issues commonly faced by entities.

Server rooms are not well managed

At 1 entity, the primary server room was shared with the records area. All entity staff had access to this room and server racks were not locked. There was no fire suppression system or extinguishers installed in this area. Additionally, there were no controls to monitor the temperature or humidity of the server room.

Server rooms in shared areas present a risk of unauthorised access and outages due to deliberate or accidental damage to equipment. A lack of environmental controls in the server room, including fire management, could also result in system damage, malfunction due to heat or humidity and service outages.

Source: OAG

Figure 13: Information systems at risk of disruption

Recommendations

1. Information security

   To ensure security strategies align with, and support, business objectives senior executives should implement appropriate frameworks and management structures.

   Management should ensure good security practices and controls are implemented and continuously monitored.

2. Business continuity

   Local government entities should have an appropriate business continuity plan, disaster recovery plan and incident response plan to protect critical services and systems from disruptive events. These plans should be tested on a periodic basis to ensure unexpected events do not affect business operations.

3. Management of IT risks

   Local government entities need to identify threats and risks to their operations arising from information technology. These should be assessed and treated within appropriate timeframes. These practices should become a core part of business activities and have executive oversight.

4. IT operations

   Local government entities should use good practice standards and frameworks as a reference to implement good controls for IT operations. Entities should have appropriate policies and procedures in place to manage incidents, IT risks, information security and business continuity.

   Additionally, entities should ensure IT strategic plans and objectives support their overall business strategies and objectives.

5. Change control

   Change control processes should be well developed and consistently followed when applying patches, updating or changing 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

   Local government entities should develop and implement physical and environmental control mechanisms to prevent unauthorised access or accidental or environmental damage to computing infrastructure and systems.

Appendix 1 – Better practice guidance to manage technical vulnerabilities

Vulnerabilities are flaws in operating systems, devices and applications that attackers could exploit to gain unauthorised access to systems and information. Local government entities should have continuous monitoring processes to understand security weaknesses and gaps in their systems, devices and applications. Vendors generally provide patches to address flaws in applications and systems. Entities should implement appropriate processes and assign responsibilities to identify and treat these flaws.

The following table outlines some guiding principles entities should consider to address vulnerabilities. This is not intended to be an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre.[4]

Principle	Our expectation
Stocktake of assets	Entities should have visibility of all their ICT assets on the network including servers, workstations, printers, software applications, IoT and other network devices (switches, routers, firewalls).
Identify vulnerabilities	Regular vulnerability scans must be performed to identify security weaknesses. Where it is not possible to scan all assets at once, entities should prioritise and group assets to scan them in stages. Scans should be regular (e.g. continuous or monthly) as extended time gaps between scans leave the systems exposed for longer periods.
Understand the exposure	Each vulnerability poses a threat but some are more severe than others. Vulnerabilities generally have a severity rating based on impact and how easily they can be exploited. Entities should perform risk assessments to understand the exposure and take appropriate action.
Test and patch vulnerabilities	Entities should test patches before deploying them to live production systems. Ideally vulnerabilities should be patched as soon as possible, in line with their severity and impact levels. Entities should define appropriate timeframes to patch vulnerabilities based on their severity.
Apply mitigating controls if patching is not possible	In some instances, vulnerabilities cannot be addressed as they could affect the operations of a system (usually legacy systems), or a patch may not yet be available. Based on a risk assessment, mitigating controls should be applied with considerations to: • virtual patches • segregating or isolating unpatched systems • upgrading systems that no longer receive security updates.

[4] https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches

Principle	Our expectation
Don’t forget the network devices – and printers	Network devices such as firewalls, routers and switches - and printers - are equally important. Vulnerability management processes must include them as well. Entities should regularly update the firmware and software for these devices.
Verify the patches	Entities should establish a process to verify that patches have successfully fixed the vulnerabilities. Some patches may fail to install or could require further configuration to fully address the weakness. Running another scan after applying patches can identify and report such instances.

Source: OAG

Figure 14: Better practice guidance to manage technical vulnerabilities

Auditor General's reports

Report number	2019-20 reports	Date tabled
26	Western Australian Public Sector Audit Committees – Better Practice Guide	25 June 2020
25	WA's Transition to the NDIS	18 June 2020
24	Opinion on Ministerial Notification	16 June 2020
23	Opinion on Ministerial Notification	29 May 2020
22	Regulation of Asbestos Removal	21 May 2020
21	Audit Results Report – Annual 2019 Financial Audits	12 May 2020
20	Local Government Contract Extensions and Variations and Ministerial Notice Not Required	4 May 2020
19	Control of Monies Held for Specific Purposes	30 April 2020
18	Information Systems Audit Report 2020 – State Government Entities	6 April 2020
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

Report number	2019-20 reports	Date tabled
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