Western Australian
Auditor General's Report

Local Government General Computer Controls

Report 23: 2020-21

12 May 2021

Office of the Auditor General
Western Australia

Audit team:
Jordan Langford-Smith
Kamran Aslam
Paul Tilbrook
Fareed Bakhsh
Steven Bertke
Ben Goodwin
Sayem Chowdhury
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

Local Government General Computer Controls

Report 23: 2020-21
May 2021

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT GENERAL COMPUTER CONTROLS

This report has been prepared for submission to Parliament under the provisions of section 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.

This is the second local government annual *Information Systems Audit Report* by my Office. The report summarises the results of our 2020 annual cycle of information systems audits across a selection of 50 local government entities.

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

CAROLINE SPENCER
AUDITOR GENERAL
12 May 2021

Contents

Auditor General's overview 2

Introduction 3

Conclusion 4

What we found: Capability assessments 5

What we found: General computer controls 7

Information security 8

Business continuity 11

Management of IT risks 11

IT operations 12

Change control 12

Physical security 13

Recommendations 14

Auditor General's overview

This is the second local government annual *Information Systems Audit Report* by my Office. The report summarises the results of our 2020 annual cycle of information systems audits across a selection of 50 local government (LG) entities.

Information systems underpin most aspects of LG entity 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 LG entities who may not have dedicated IT staff but rely on contractors to provide the necessary support.

In the 11 LG entities where we performed capability maturity assessments, none met our benchmark in all areas, with information security remaining a significant area of concern where no audited entities achieved our minimum capability maturity.

Throughout the report, we have included a number of audit case studies to help highlight the risks associated with weak information system controls. Included in the case studies are real life examples of how extremely poor general computer controls can result in system breaches, loss of sensitive and confidential information and financial loss. They serve as important reminders of the need to remain ever vigilant against constant cyber threats.

While legacy systems can take some time to replace or upgrade, not all controls require expensive technology investments. Well implemented processes and fine-tuning existing practices can achieve a good baseline to build resilience to internal and external threats. Educating staff on cyber risks and periodically testing their responses to simulated threats will give valuable feedback to entity executive and council.

I have chosen to not identify the audited LG entities given the nature of the findings, a custom extended from my Office's similar audits in the State sector. Over time, this practice may change to identify entities so as to provide an incentive to public entities to more promptly address identified control shortcomings.

Introduction

Local government (LG) entities rely on information systems to prepare their financial statements and to deliver important services to the public. Our general computer controls (GCC) audits assess whether LG entities' system controls effectively support the confidentiality, integrity and availability of their information systems and financial reporting. They are performed as an integral part of, and inform, our financial audit program.

This report presents a summary of the findings reported to 50 local government entities in 2019-20. For 11 LG entities we performed capability maturity assessments. A GCC audit with a capability maturity assessment is the most comprehensive information systems audit we undertake. We use the findings to inform our audit risk assessment and work program for the sector.

For our capability maturity assessments, we asked the 11 LG entities to self-assess against the provided capability maturity model. We then compared their results to ours (which were based on the results of our GCC audits). These assessments are a way to see how well-developed and capable entities' established IT controls are.

For the remaining 39 LG entities, the GCCs were examined by contract audit firms or by our financial audit teams who did not undertake the capability maturity modelling. Information system findings identified during these audits are included in this report.

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

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

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

Source: OAG

Figure 1: GCC categories

Throughout the report we have included real life case studies that illustrate the significant impact poor controls can have on LG entities. All case studies, except case study 7, are from metropolitan LG entities.

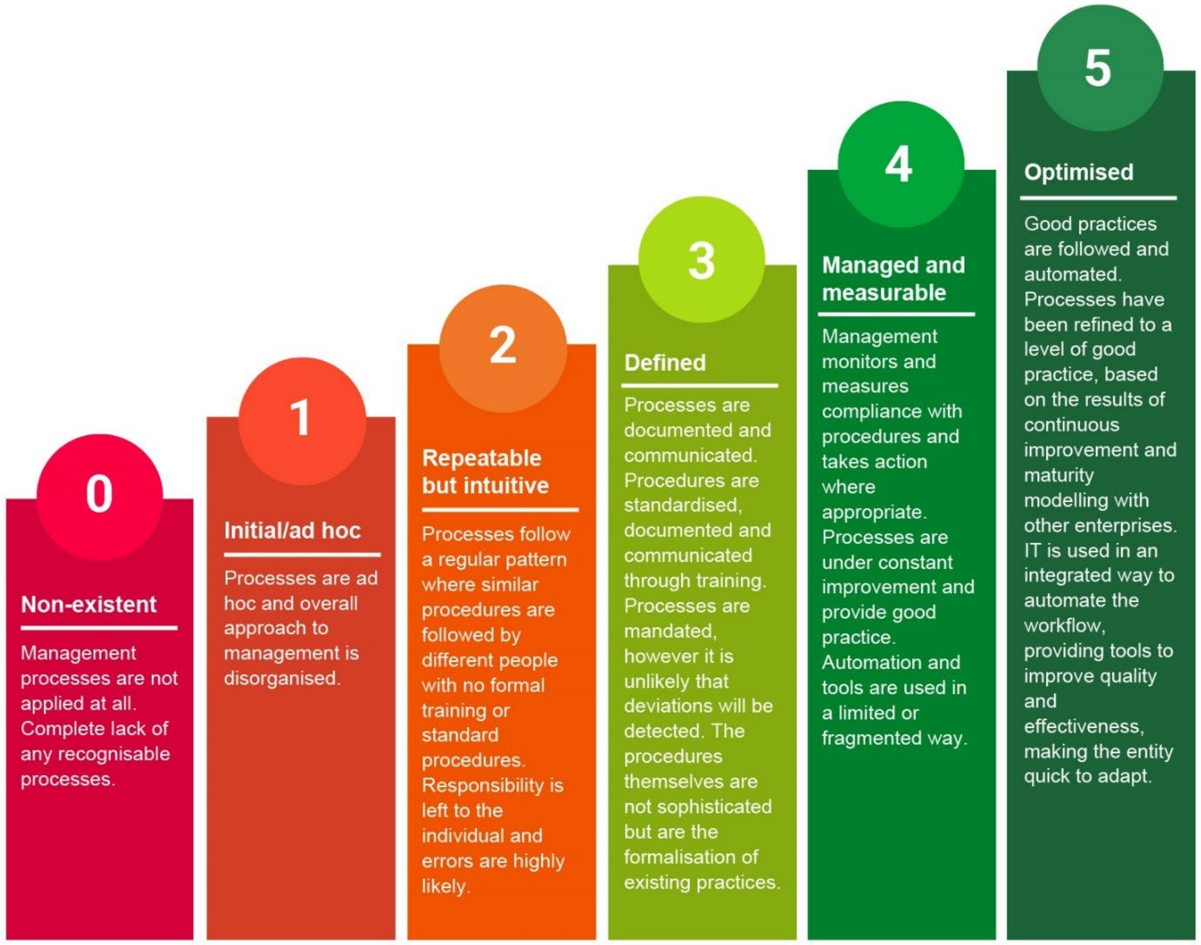
Conclusion

LG entities need to improve their general computer controls. We reported 328 control weaknesses to 50 LG entities, with 10% (33) of these rated as significant and 72% (236) as moderate. As these weaknesses could significantly compromise the confidentiality, integrity and availability of information systems, the LG entities should act promptly to resolve them.

Our capability assessment results show that none of the 11 audited LG entities met our expectations across 6 control categories, with 79% of the audit results below our minimum benchmark. We found weaknesses in controls for information security, business continuity, change management, physical security and IT operations. Entities also need to improve how they identify and treat information risks. Five of the entities were also included in last year's in-depth assessment and could have improved their capability by promptly addressing the previous year's audit findings but, overall, did not discernibly do so.

What we found: Capability assessments

We conducted in-depth capability assessments at 11 LG entities, 5 of which were also audited in 2018-19. We used a 0 to 5 rating scale[1] (Figure 2) 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.



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

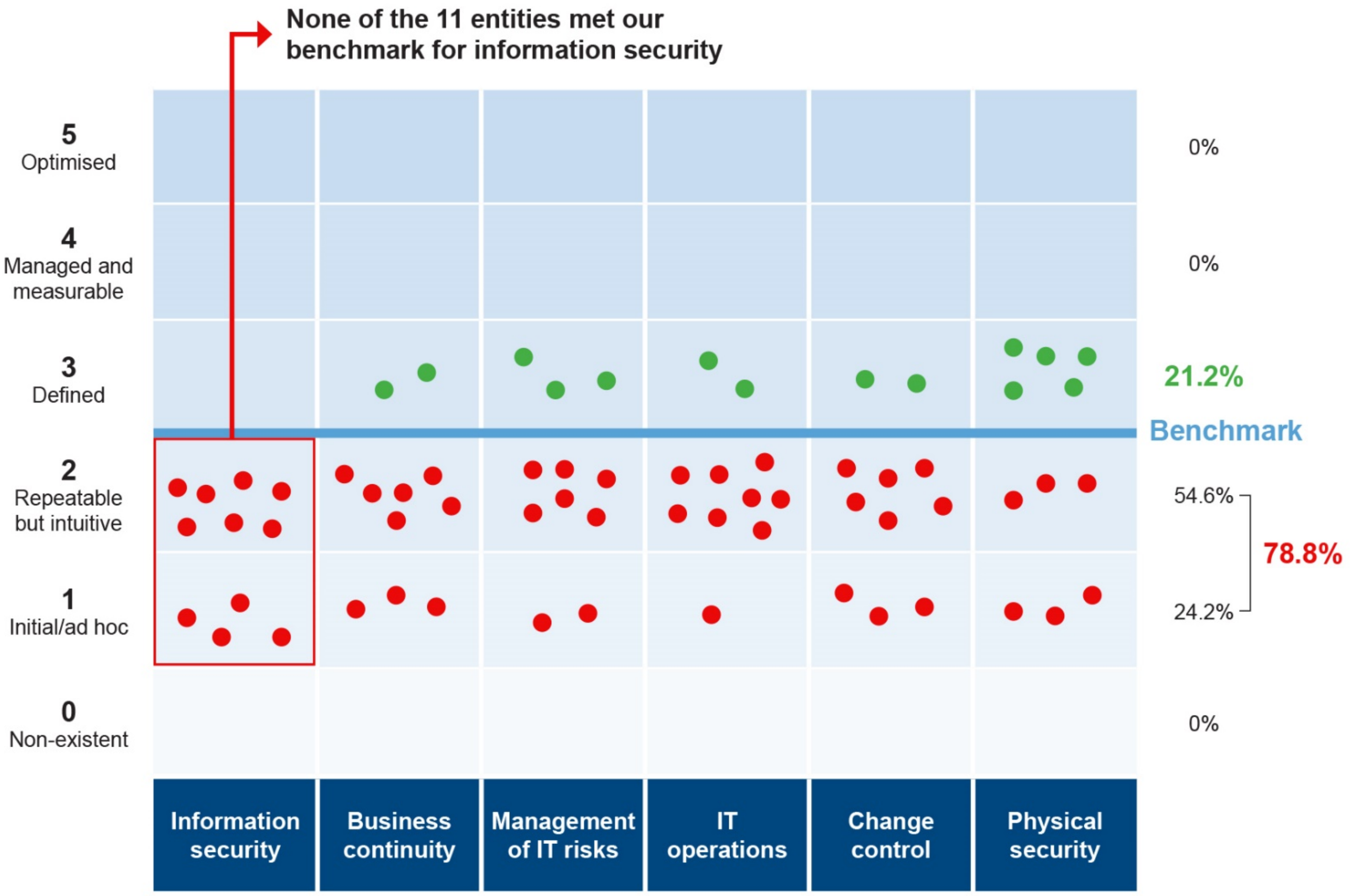
Figure 2: Rating scale and criteria

None of the 11 LG entities met our expectations across all control categories. In the area of information security, all 11 entities were below our benchmark.

Entities did not have adequate controls to effectively manage information security, change management, IT operations, physical security and business continuity. 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 3 shows the results of our capability assessments across all 6 control categories for the 11 entities we assessed in 2019-20.

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



Source: OAG

Figure 3: 2019-20 capability maturity model assessment results

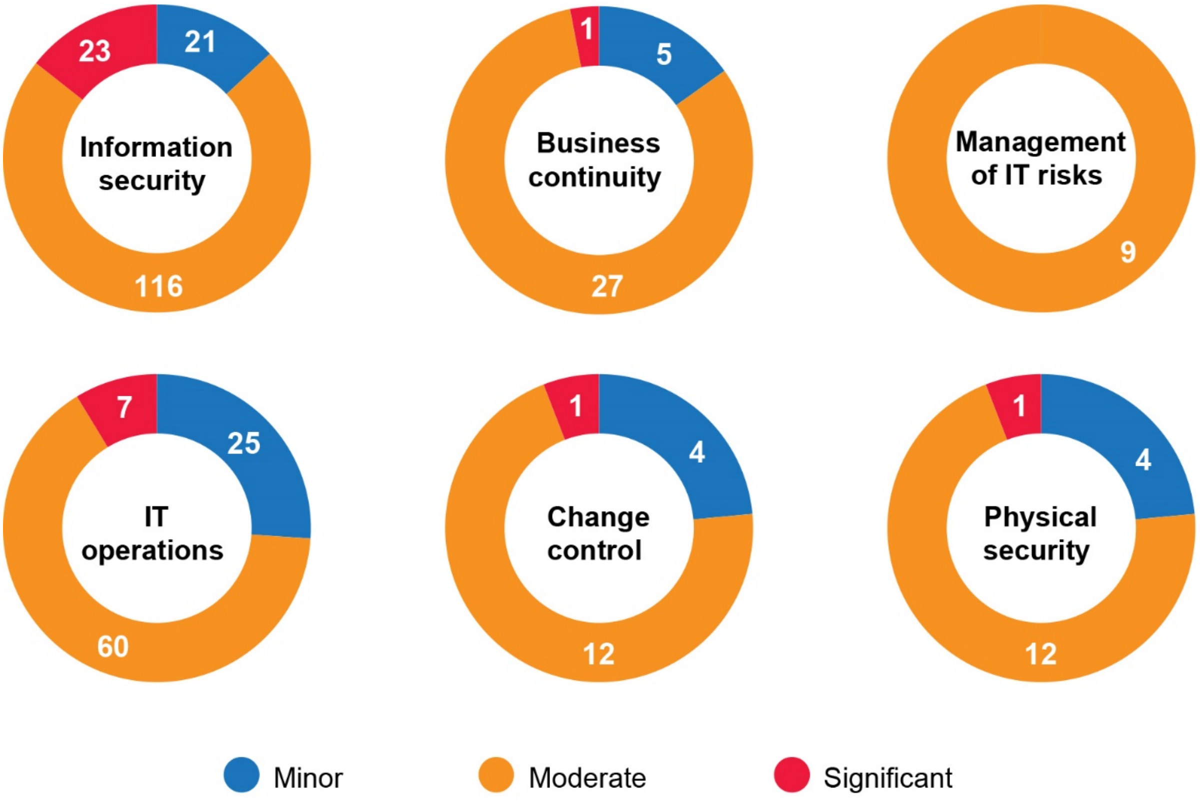
What we found: General computer controls

We reported 328 general control weaknesses to 50 LG entities, with 10% rated as significant requiring prompt action, 72% as moderate which should be addressed as soon as possible, and the remaining 18% as minor. Like last year, nearly half of all issues were about information security.

We reported these weaknesses to LG entities in a management letter. However, as management letters are often made public, we removed sensitive technical details which could increase the risk of cyber-attacks to entities. We reported these details separately through confidential letters to assist entities in addressing weaknesses. Entities generally agreed to implement our recommendations.

Figure 4 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.



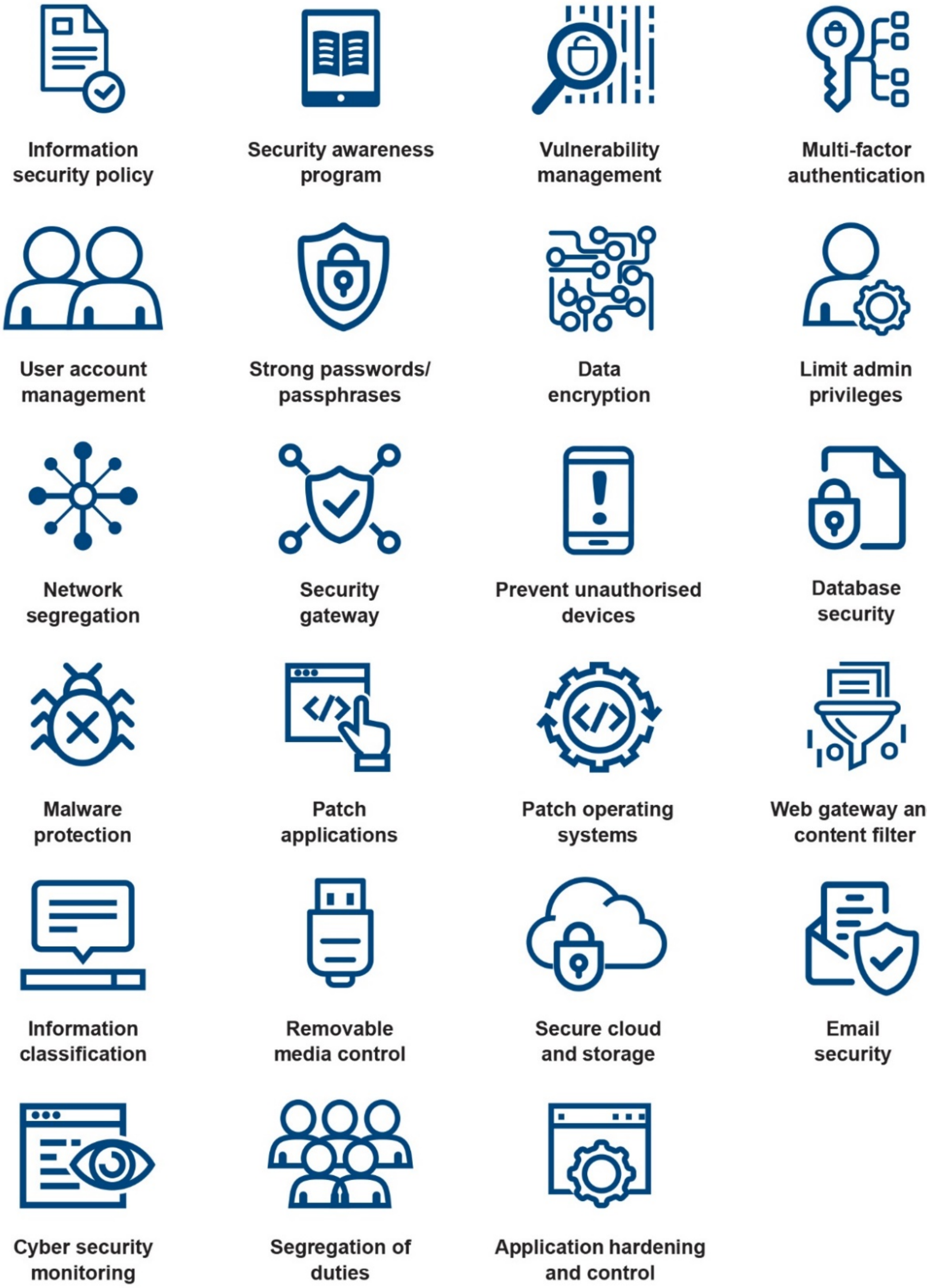
Source: OAG

Figure 4: 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.

Our GCC audits and capability maturity model include an assessment against better practice controls for information and cyber security. Figure 5 lists some of the important better practice controls for information security.



Source: OAG

Figure 5: Information security – Better practice controls included in our GCC audits

Many entities either lacked or had inadequate information security polices to inform staff of their responsibilities to protect entity information, which also includes the personal information of ratepayers. Staff and contractors were often not given sufficient training to understand the potential risks and threats to entity information. Case study 1 highlights the risks associated with a poor awareness of cyber threats.

Case study 1: Poor awareness and a lack of security controls results in a loss of confidential information

One entity we audited did not have an effective security awareness program to guide and educate staff on cyber and information security risks. A user's account details (username and password) were stolen because of a phishing attack which was not detected or prevented by the entity's security controls. The attack resulted in a fraudulent credit card transaction on the user's corporate credit card, which was immediately cancelled. Further investigation by the entity revealed the attacker downloaded 10GB of entity information in the form of sensitive emails.

If effective controls are not in place to detect and prevent attacks, this could result in loss of sensitive and confidential information. Along with technical controls, staff education and awareness are important to combat these threats. Without ongoing information security awareness training there is an increased risk that individuals will not understand the risks to the entity and their responsibilities to protect information. This may result in inappropriate actions which could compromise the confidentiality, integrity and availability of information.

Another common weakness was that entities did not have policies, procedures and processes to effectively manage technical vulnerabilities. Our vulnerability scans of key entity systems identified a range of critical and high severity vulnerabilities which had not been patched. These vulnerabilities can be exploited by malicious attackers to compromise entity systems.

Network segregation adds a layer of security to protect systems from cyber intrusions. It is most common to separate internal networks from external-facing systems. The network is divided into smaller zones with rules to restrict communication between areas and services. This strategy limits the impact of cyber intrusions by restricting attackers' ability to discover critical systems and gain access to sensitive information. We found many entities did not appropriately segregate their network, which makes it easier for an attacker to locate and access sensitive information once the network is compromised.

Case study 2 highlights the risks to information when networks aren't segregated.

Case study 2: Network security issues increase the risk of successful cyber attacks

One entity had not segregated its internet facing systems from the internal network. There was insufficient physical or logical segregation of its internal and external network. This meant that public facing and internal systems sat in the same network which is a serious situation.

Internet facing systems are under constant cyber threats, the current network design would allow a potential attacker or malicious software application (i.e. malware) full access to the network once the perimeter is breached. It would be difficult for the entity to contain any breach because communication between network segments was not controlled.

We also found that the entity did not have adequate controls in place to prevent or detect the use of unauthorised devices on the network. There is an increased risk that unauthorised devices could be used to attack internal systems or could result in the spread of malware to the entity's network and systems.

Multi-factor authentication (MFA) adds a layer of security to protect systems from unauthorised access. We found many entities did not have MFA for remote access to their network and allowed access with a username and password only (Case study 3). This leaves entities at risk of attacks such as phishing and password spraying.[2]

Case study 3: Information at risk due to poor remote access controls

At 1 entity we found the following issues relating to remote access into the network:

- MFA was not used to access the network and systems remotely over the virtual private network (VPN) and remote desktop services (RDS). MFA adds a layer of security to protect systems from unauthorised access and brute force attacks.
- There were no audit trails to detect whether staff working remotely had copied entity information to personal devices increasing the risk of information loss.

When remote access is not appropriately managed, there is an increased risk of inappropriate or unauthorised access to the entity's IT systems and information. In addition, without controls to prevent or monitor information copied to personal devices, there is an increased risk of unintentional or inappropriate disclosure of critical information.

We found many entities were not managing privileged access to their networks and systems. There were many instances where large numbers of staff were given the highest level of access privilege, allowing them to make changes to system configuration and information.

At several entities the highly privileged default administrator account had not been renamed and the password not changed for many years, even after staff turnover. When such an account gets compromised it can give an authorised user or malicious attacker complete control of the network.

Case study 4: Privileged access rights are not appropriately restricted and controlled

At 1 entity the allocation and use of privileged access rights to the network (active directory) were not appropriately restricted and controlled.

The entity had not changed the password for the default network administrator account since 2002, even though a number of IT staff who knew the password had left. We found instances where this account was used out of office hours and the entity was unable to explain this use.

We also found individuals assigned with the highest level of privileges which, were not appropriate for their role and responsibilities.

Without appropriate management of privileged access there is an increased risk that unauthorised or unintentional modifications of IT systems will occur. This could impact the confidentiality, integrity and availability of the entity's systems and information.

[2] Password spraying is a technique where cybercriminals try common passwords on user accounts to gain unauthorised access to systems. Each password is used on multiple accounts before attempting the next password.

Cybercriminals frequently use email scams to compromise entity system and information. Therefore, it is vital for entities to secure their email systems by implementing controls to check the integrity and authenticity of the emails (Case study 5).

Case study 5: Inadequate controls to secure emails and business information

At 1 entity we found there were inadequate controls to check the integrity and authenticity of emails. This means malicious users could impersonate genuine individuals to gain unauthorised access to systems and information. Without appropriate controls to secure emails the entity is at increased risk of successful cyber-attacks

The entity also did not monitor the use of public cloud storage as staff were using many different cloud storage services to share entity's business information. This puts the entity's sensitive information at risk.

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.

Weaknesses we found included:

- entities did not have up-to-date business continuity and disaster recovery arrangements in place. While many had developed continuity plans in response to COVID-19, they only covered the pandemic
- entities that did have continuity plans did not regularly test them.

An up-to-date business continuity plan, disaster recovery plan and incident response plan play a crucial part in enabling the entity to operate during a disruption and restore business services timely.

Management of IT risks

Entities should be aware of the nature of risks associated with IT and have appropriate risk management policies and practices in place such as risk assessments, registers and treatment plans.

Weaknesses we found included:

- no policies and procedures to document, assess, review and report IT risks
- key risks were not documented. This meant entities were unaware if appropriate controls were in place to protect their information
- entities had not reviewed their risk registers within a reasonable time.

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

IT operations include day-to-day tasks designed to keep services running, while maintaining data integrity and the resilience of IT infrastructure. We tested whether entities had formalised procedures and monitoring controls to ensure processes were working as intended.

Weaknesses we found included:

- a lack of user access reviews. Regular review of access ensures that only current authorised individuals have access to networks and key systems and the privileges assigned are appropriate for the tasks they perform
- no logging of user access and activity to key systems and sensitive information. This could result in malicious activity going undetected
- network logs not kept for adequate duration
- a lack of incident management procedures
- IT staff were not required to complete a background check (e.g. police clearance). These staff had highly privileged access to the entities IT systems and information.

Without appropriate plans and supporting procedures, IT operations may not be able to respond to business needs and recover from errors or failures.

The following case study highlights the risk to entities when user access is not appropriately controlled and monitored.

Case study 6: Shared generic accounts increase the risk of fraud

At 1 entity, staff could redirect payments for council rates, infringements, licence and application fees to another bank account by changing a file hosted on a shared server. Access to the server was not appropriately controlled because staff used a shared generic account to access and manage the server. This issue was further compounded because changes to the file and user activity were not logged and monitored. This meant that it would be difficult for the entity to identify and hold someone accountable, in the event of a fraudulent change.

Change control

We reviewed whether changes to IT systems were authorised, tested, implemented and recorded in line with management's intentions.

Weaknesses we found included:

- a lack of appropriate policies and procedures to implement changes
- change procedures were applied inconsistently
- a critical system was not covered by change procedures.

If changes are not controlled, they can compromise the integrity and availability of systems. As a result, systems will not process information as intended and entities' operations and services may be disrupted.

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.

The following case study highlights the risk to entities when changes are not controlled and monitored.

Case study 7: Poor monitoring of user activity and changes could result in incorrect rate statements

We discovered an instance where unauthorised changes were made to property valuations used to calculate rates. This resulted in the LG entity spending additional time and resources to identify the discrepancies and to ensure rate statements being issued for 2020-21 were correct. The entity had not implemented a process to regularly review audit logs to identify unauthorised changes made to rates, despite us raising this issue with them in 2 previous audits.

Without independent reviews of system and information changes, there is an increased risk of financial loss to the entity or incorrect fees being charged to customers because of erroneous or fraudulent data entry.

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 located at entity premises.

Weaknesses we found included:

- a lack of policies and appropriate environmental controls to protect IT infrastructure. This could result in system damage or malfunction due to heat or humidity and service outages
- no reviews of staff and contractors' access to server rooms. This increases the risk of unauthorised access to systems and information
- no backup power to maintain systems in case of power outage, increasing the risk of service outages.

Case study 8: Server rooms not well protected

One entity did not have an effective process to review who had access to the server room. We sampled 3 visitor access cards and found all allowed access to the building and server room. This had previously been identified by internal audit and entity management thought the issue had been resolved, but it had not been at the time of our audit. In addition, we found combustible materials such as non-essential equipment and cardboard boxes in the server room. Server rooms should be independent, restricted access rooms.

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 policies and practices are implemented for all control areas identified in figure 5 and continuously monitored.

2. Business continuity

   LG 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

   LG 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

   LG 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

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

Under section 7.12A of the *Local Government Act 1995*, the 50 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.

Auditor General’s 2021-22 reports

Number	Title	Date tabled
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
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
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