The Council of the City of Cockburn

City of Cockburn

Audit Risk and Compliance Committee

Minutes

For Tuesday, 16 July 2024

These Minutes are confirmed

Presiding Member's signature

P. Corke.

Date: 17 September 2024

Table of Contents

Minutes

In Attendance

Elected Members
Cr P Corke (Presiding Member)
Cr K Allen
Deputy Mayor C Stone
Cr M Separovich (Deputy Member)
Independent Member Mr A Kandie

Guests
Cr T Dewan
Cr C Zhang

Ms C McGowan	Director, Office of the Auditor General
Mr J Ward	Engagement Partner, KPMG
Ms G Okafor	Manager, KPMG

Staff

Mr D Simms	Chief Executive Officer
Mr D Arndt	Director Planning and Sustainability
Mr M Foley	A/Director Infrastructure Services
Ms K Jamieson	A/Director Community and Place
Mr S Rosita	A/Director Corporate and System Services
Mr B Fellows	Head of Information and Technology
Ms M Todd	Manager Legal and Compliance
Mr M Lees	System Support Officer
Ms S D'Agnone	Council Minute Officer

1. Declaration of Meeting

The Presiding Member declared the meeting open at 6:03pm and welcomed Ms Cait McGowan from the Office of the Auditor General, Mr Ward and Ms Okafor from KPMG.

“Kaya, Wanju Wadjuk Budjar” which means “Hello, Welcome to Wadjuk Land”

The Presiding Member acknowledged the Wadjuk Peoples of the Nyungar Nation who are the traditional custodians of the land on which the meeting was being held and paid respect to the Elders both past and present and extended that respect to First Nations Peoples present.

2. Appointment of Presiding Member (If required)

N/A

3. Disclaimer

The Presiding Member read the Disclaimer:

> Members of the public, who attend Council Meetings, should not act immediately on anything they hear at the Meetings, without first seeking clarification of Council's position.
>
> Persons are advised to wait for written advice from the Council prior to taking action on any matter that they may have before Council.

4. Acknowledgement of Receipt of Written Declarations of Financial Interests and Conflict of Interest (by Presiding Member)

Nil

5. Apologies & Leave of Absence

Apologies
Mayor Logan Howlett
Cr C Reeve-Fowkes
Independent Member Warwick Gately
Mr A Lees, A/Director Community and Place
Mr N Mauricio, A/Director Corporate and System Services

6. Public Question Time

Nil

(2024/MINUTE NO 0015) Suspend Standing Orders

Committee Recommendation
MOVED Cr P Corke SECONDED Deputy Mayor C Stone
6:05pm That Clauses 9.5 and 9.6 of the Standing Orders Local Law 2016 be suspended.

CARRIED 5/0

During suspension of Standing Orders, Mr Ward from KPMG gave a brief summary of the Audit Plan process and findings.

(2024/MINUTE NO 0016) Reinstate Standing Orders

Committee Recommendation
MOVED Cr P Corke SECONDED Cr M Separovich

6.19pm That Clauses 9.5 and 9.6 of the Standing Orders Local Law 2016 be reinstated.

CARRIED 5/0

7. Confirmation of Minutes

7.1 (2024/MINUTE NO 0017) Minutes of the Audit Risk and Compliance Meeting - 21/05/2024

Committee Recommendation
MOVED Independent Member A Kandie SECONDED Cr K Allen

That Committee confirms the Minutes of the Audit Risk and Compliance Meeting held on Tuesday, 21 May 2024 as a true and accurate record.

CARRIED 5/0

8. Deputations

Nil

9. Business Left Over from Previous Meeting

Nil

10. Declaration by Members who have Not Given Due Consideration to Matters Contained in the Business Paper Presented before the Meeting

Nil

En Bloc Resolution

6:21pm The following items were carried en bloc:

11.1.1	11.2.2

11 Reports - CEO (and Delegates)

11.1 Corporate and System Services

11.1.1 (2024/MINUTE NO 0018) Audit Plan for Financial Year ending 30 June 2024

Executive A/Director Corporate and System Services
Author A/Head of Finance
Attachments 1. Audit Plan 2023-2024 **(Confidential)**

Officer Recommendation/Committee Recommendation
MOVED Cr M Separovich SECONDED Deputy Mayor C Stone
That Council:

(1) RECEIVES the Audit Plan for auditing the Financial Year ending 30 June 2024 as attached to the Agenda.

CARRIED 5/0

Background

The attached External Audit Plan and Strategy document for Financial Year 2024 outlines the purpose and scope of the External Audit and explains the audit methodology and approach to be taken in completing the 2024 Financial Year Audit.

It provides the Audit, Risk and Compliance Committee (ARC) with the opportunity to review the audit focus areas, the auditor's procedures, and the agreed timelines.

The Audit Plan was prepared by KPMG in consultation with the City and approved by the Office of the Auditor General (OAG).

Given the OAG has indicated a preference that their audit plans, management letters and audit closing reports are not made publicly available, this Audit Plan has been made confidential (refer Confidential Attachment.1).

However, the OAG has no issue with the City highlighting key aspects from the Plan in this report.

The OAG tendered out and awarded the performance of the City's audit to KPMG for another financial year. This year will be the sixth year KPMG has audited the City.

Regulation 9 (2) of the *Local Government (Audit) Regulations 1996* states that the principal objective of the external audit is for the auditor to carry out such work as is necessary to form an opinion on whether the accounts are properly kept, and that the Annual Financial Report:

- is prepared in accordance with financial records
- represents fairly the results of the operations of the Local Government as at 30 June, in accordance with Australian Accounting Standards and the *Local Government Act 1995*.

As set out in the ARC Terms of Reference, its duties and responsibilities include discussing with the external auditor the scope and planning of the audit each year.

Submission

N/A

Report

KPMG will conduct an independent audit to enable the OAG to express an opinion regarding the City's 2023-2024 financial statements.

The audit is conducted in accordance with Australian Auditing Standards to provide reasonable assurance that the City's financial report is free of material misstatement.

A key aspect of the audit work is considering the effectiveness of management internal controls and assessing the appropriateness of the City's accounting policies, disclosures, and accounting estimates.

The audit approach outlined in the plan is summarised under the seven following areas:

1. Methodologies and activities
2. Materiality
3. Risk assessment
4. Approach to IT audit
5. Independence
6. Approach to fraud
7. Environmental, Social and Governance (ESG) reporting.

A key aspect of the audit planning process is the assessment of inherent audit risks, where the auditor considers the nature of the risk, likelihood of occurrence and the potential impact it could have on the City's financial report.

For the 2023-2024 Audit, KPMG have determined the following eight focus areas:

1 Management override of controls

Area of audit focus

- Management is in a unique position to perpetrate fraud because of its ability to manipulate accounting records and prepare fraudulent financial reports by overriding controls that otherwise appear to be operating effectively

2 Infrastructure Assets

Areas of audit focus

- Significant volume and value of individual assets
- Recording capitalised costs in the incorrect period

3 Property, plant and equipment

Areas of audit focus

- Significant volume and value of individual assets
- Inaccuracy of amounts recorded in the fixed assets register
- Recording capitalised costs in the incorrect period

4 Revenue recognition

Areas of audit focus

- High volume of transactions that management are required to process accurately
- Heightened area of focus for stakeholders

5 Employee costs and provisions

Areas of audit focus

- High volume of transactions that management are required to process accurately
- Existence and accuracy of payroll related costs
- Completeness and accuracy of related payroll liabilities

6 Contracts and Expenditure

Areas of audit focus

- High volume of transactions that management are required to process accurately
- Heightened area of focus for stakeholders

7 Landfill site – rehabilitation asset and liability

Areas of audit focus

- Accounting treatment can involve high levels of judgement and estimation uncertainty

8 Cash, cash equivalents and term deposits

Areas of audit focus

- High volume of transactions of significant value
- Significant value of term deposits
- Cash and cash equivalents may not be completely identified and recorded
- Cash equivalents may not be appropriately classified

The Audit Plan outlines why these have been chosen as focus areas and the planned audit procedures to be applied in reviewing and assessing them.

The standard has been revised, reorganised and modernised in response to the evolving environment, including in relation to information technology.

Interim audit work for the 2023-2024 audit was completed in June 2024 and the proposed timeline included in the Audit Plan sees end of year audit procedures commencing on 16 September 2024.

According to the Plan, the draft audit report will be presented at the ARC meeting scheduled for 3 December 2024.

The audit opinion from the OAG will be issued on 6 December 2024, accompanied by the management letter.

KPMG and the OAG will be attending the July ARC meeting to present and discuss the attached audit plan for 2023-2024.

Strategic Plans/Policy Implications

Listening & Leading
A community focused, sustainable, accountable, and progressive organisation.
• Best practice Governance, partnerships and value for money.

Budget/Financial Implications

The OAG have provided a quote for the completion of the audit, which is covered within the FY 25 Annual Municipal Budget.

Legal Implications

- *Local Government Act 1995* Sections 5.53, 5.54, 6.4, and Part 7 - Audit
- *Local Government (Audit) Regulations 1996* Regulations 9, 9A and 10
- *Local Government (Financial Management) Regulations 1996* Part 4 - Financial Reports.

Community Consultation

N/A

Risk Management Implications

It is a requirement under the *Local Government Act 1995* for Council to accept the City's Annual Report (including the Financial Report and Auditor's Report) by no later than 31 December each year.

Failure to do so will lead to statutory non-compliance.

Appropriate audit planning helps ensure this risk is mitigated.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

11.1.2 (2024/MINUTE NO 0019) Local Government 2022-23 Information Systems Audit Results

Executive A/Director Corporate and System Services
Author Head of Information Technology
Attachments 1. Local Government 2022-23 Information Systems Audit Results - Local Government 2022-23.pdf ⇩

Officer Recommendation/Committee Recommendation
MOVED Deputy Mayor C Stone SECONDED Cr K Allen
That Council:

(1) RECEIVES the Office of Auditor General's Performance Audit Report Office of Auditor General State Government 2022-23 Information Systems Audit, as attached to the Agenda.

CARRIED 5/0

Background

The Office of the Auditor General (OAG) has published for the past 16 years, reporting on State government entities' general computer controls.

The City of Cockburn (the City) has presented similar reports to the Audit, Risk and Compliance Committee (ARC) in the past, to give context and relevance of efforts ongoing in the public sector.

To ensure the City adopts best practice in this area, the City independently submits a report to the ARC on the OAG audit report recommendations, highlighting any specific opportunities for improvement from the OAG report, that can benefit the City's cyber security posture and specific computer controls.

Submission

N/A

Report

Purpose of the OAG Audit Report

560 findings were made in computer controls audit, performed across 58 public sector (state government) entities.

Significant matters identified by the OAG

The OAG audit report has identified that 55% of weaknesses identified in previous years, were unresolved during this audit period.

The OAG audit has also identified the matters summarised below:

- Only 11% of entities met the benchmark for Endpoint security.
- Human resource security benchmark was met by only 34% of entities.
- 49% of entities met business continuity benchmarks.
- 57% of entities met network security benchmarks.
- 61% of entities met information security framework benchmarks.
- 89% of entities met change management benchmarks.

While the OAG's audit report highlights significant failings and stagnant progress across many state government entities, the City's progress against many of the benchmarks has continued to improve.

The City has continued its programme of works in this space, to meet the expected and anticipated benchmarks.

Implication(s) for local government / the City

1. The OAG audit recommends implementing computer controls across all 10 key computer control areas, with emphasis on improving endpoint security as a priority.

   In the City's case, this entails following the City's cyber security plans with alignment to ISO27001 and continuing to implement the ASD Essential Eight security controls already underway.

2. The OAG audit recommends following OAG guidance to help strengthen security controls.

   In the City's case, following the OAG guidance documentation to ensure Essential Eight cyber security controls, which are a requirement of the WA Government Cyber Security Policy. Effective implementation of these controls will significantly strengthen an entities' general computer controls and help address findings listed in the audit.

City response to OAG audit

A copy of the OAG audit is in Attachment 1, and below are responses provided by the cyber security officer to recommendations contained in the OAG audit:

No.	OAG recommendation	City response
1.	Endpoint security computer controls implemented to protect workstations, server, and mobile devices.	The City already has endpoint security controls applied to servers and workstations. The City will continue to implement Essential Eight cyber security controls, which include endpoint security. Works underway include a large-scale workstation replacement programme, and upgrading to the latest version of endpoint security software. Actions in this space are expected for completion by 31 December, 2024.
2.	Access management, including phishing-resistant multi-factor authentication implementation.	The City has extensive multi-factor authentication controls applied. The City will continue to implement Essential Eight cyber security controls, which include access management controls. Current works include adding additional MFA controls to control web-based system access. The next round of actions in this area is for completion by 31 December 2024.
3.	Human resource security controls are implemented, including pre-employment screening, effective termination procedures (including returning of assets), and ongoing security awareness training programs.	The City has adequate security controls in place to meet these requirements. The City undertakes pre-employment reference checks, national police clearances and qualification vetting for onboarding. For offboarding the City sends correspondence to all stakeholders to ensure that access cards and IT access are deactivated as soon as possible after termination. The City's HR has a checklist to collect City-owned items (including swipe cards, credit cards, keys and IT equipment).
4.	Network security computer controls are implemented, including preventing unauthorised devices from connecting to corporate networks, adequately securing wireless networks, and regular independent penetration tests.	The City has implemented various network security controls including network segregation, Cyber security monitoring (SIEM) and secure wireless networks. The City will continue to implement Essential Eight cyber security controls, which includes network security computer controls. Specifically, the City is undertaking the next round of network segmentation, to further isolate and control unauthorised devices. The next round of actions in this area is due for completion by 31 December, 2024.
5.	Information security framework policies are maintained in line with	The City has selected to align its self with ISO27001, and the ASD Essential 8 frameworks.

	the WA Government Cyber Security Policy	
6.	Business continuity plans should be kept up to date and should be tested regularly.	The City is in the process of revising its business continuity plan (BCP). A draft will be presented to SLT and ELT by August 2024 with a planned cyber related test scenario to follow. IT is scheduled to refresh the City's Disaster Recovery Plan (DRP) following the move of its Enterprise Resource Planning (ERP) System, TechnologyOne to a cloud-based platform as this fundamentally changes the IT architecture. This is scheduled for completion in March 2025.
7.	IT Operations should implement IT incident and problem management processes, SLAs, supplier performance, and asset inventories.	The City has incident and problem management systems and processes in place. An IT services catalogue project has commenced, with an expected completion date of 30 June, 2025.
8.	Access controls to prevent unauthorised access, prevent damage to IT infrastructure, and to ensure third-party access to data centres is managed appropriately.	The City has numerous physical security controls in place to protect against unauthorised access and damage to IT infrastructure. These controls include fire suppression systems, server room access control, temperature and humidity controls and CCTV monitoring. The City is continuing to roll-out further access control systems to prevent unauthorised access, and to log, capture and alert on access attempts. The City will continue to review and improve security access controls in this area, with the next round due by December 31, 2024.
9.	Ensure that IT information and cyber security risks are identified, assessed, and treated within appropriate timeframes.	The City will continue to review and manage risks within the City's Risk Management System (RMSS) and service desk tool, within expected timelines specified for each risk.
10.	Change management systems and procedures should be used to control change within IT systems	The City has a defined and documented IT Change Management Standard in place. These processes include change evaluation and production, and procedures for implementing emergency changes.

Strategic Plans/Policy Implications

Listening and Leading
A community focused, sustainable, accountable, and progressive organisation.
• Best practice Governance, partnerships and value for money.
• Employer of choice focusing on equity, innovation and technology.

Budget/Financial Implications

N/A

Legal Implications

N/A

Community Consultation

N/A

Risk Management Implications

This is some text. OAG performance audits constitute the fourth line of defence in the OAG's 'Four Lines of Defence Assurance Model' which the City has adapted in the *City of Cockburn Enterprise Risk Management Framework*. The OAG has identified risks in its audit report and the City needs to manage these risks by implementing appropriate control measures.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

6:24pm Cr Zhang departed the meeting.

Office of the Auditor General
Serving the Public Interest

Report 16: 2023-24 | 27 May 2024

INFORMATION SYSTEMS AUDIT RESULTS

Local Government 2022-23

Office of the Auditor General for Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Paul Tilbrook
Information Systems Audit team

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.

Image credit: shutterstock.com/13_Phunkod

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government 2022-23 – Information Systems Audit Results

Report 16: 2023-24
27 May 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT 2022-23 – INFORMATION SYSTEMS AUDIT RESULTS

This report has been prepared for submission to Parliament under the provisions of section 24 of the *Auditor General Act 2006*.

Our information systems audits focus on the computer environments of entities to determine if their general computer controls effectively support the confidentiality, integrity and availability of information systems and the information they hold.

This is our fifth report on the findings from our audits of local government entities' information technology general computer controls.

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

Caroline Spencer
Auditor General
27 May 2024

Contents

Auditor General's overview

This report summarises the results of the 2022-23 cycle of local government entities' information systems audits performed between April 2023 and March 2024. As these audits focus on areas that may affect the confidentiality, integrity and availability of the entities' information and systems, they are an essential part of our financial statement audits.

Our audit results show entities have improved the maturity of their control capability since our first information system audits in 2019-20, with the biggest improvements in risk and change management. However, significant improvements are still needed in all other areas.

Information and cyber security remains the highest concern due to the number of weaknesses we continue to identify in the five related categories (access management, endpoint security, human resource security, network security and information security framework). Entities need to better protect themselves against external and internal threats to reduce the risk of security breaches. Internal threats can be notably reduced through fit-for-purpose human resource controls such as screening, onboarding and offboarding procedures, and cyber security education programs.

This year, we reported 473 (58 significant, 328 moderate, 87 minor) issues to 76 entities. Concerningly, a large proportion (45%) of significant issues were unresolved findings from last year.

I encourage all entities to take note of the findings and recommendations in this report and implement fit-for-purpose solutions.

2022-23 at a glance

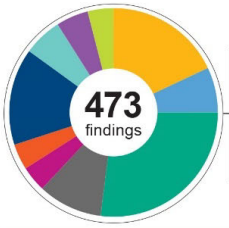
Auditing local government entities

(Prior year shown in brackets)

473 (PY: 324 at 53 entities) general computer controls findings at 76 entities

11 (PY: 12) capability maturity assessments

Key insights



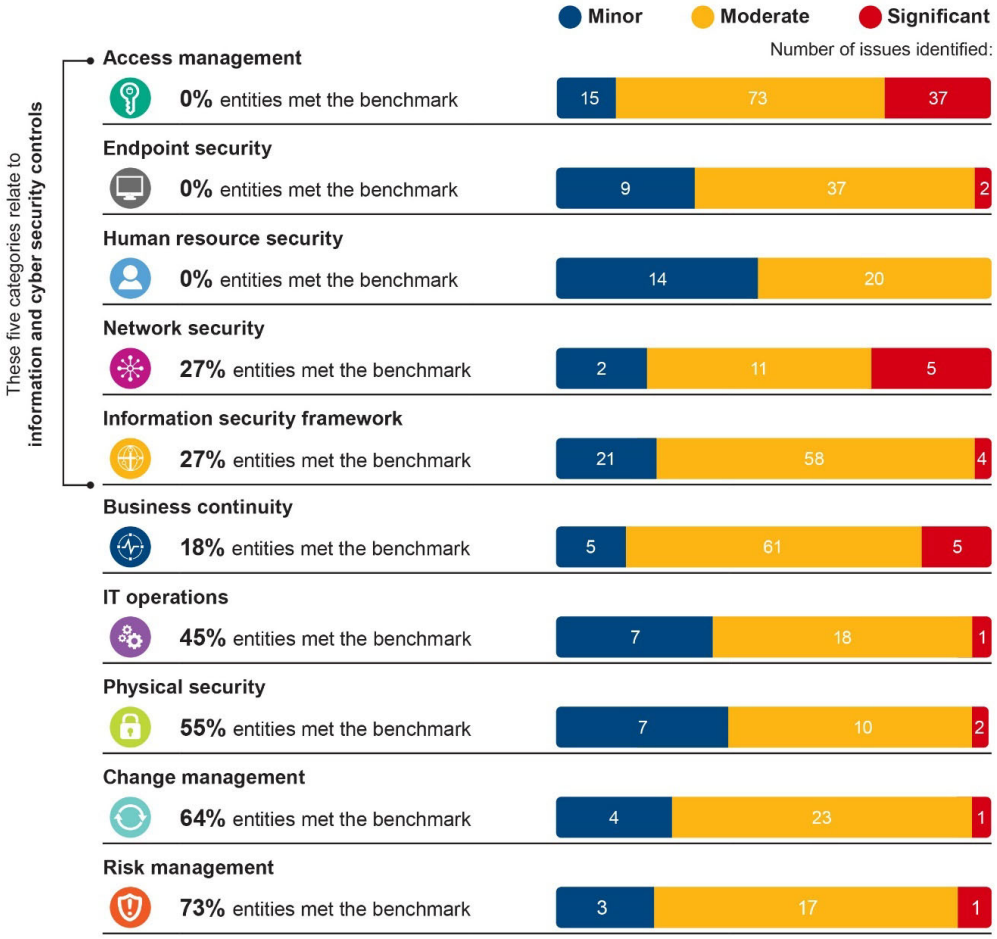
58 weaknesses were rated significant

328 moderate

87 minor

45% of the significant findings were unresolved issues from prior year

Snapshot of general computer controls findings and capability maturity assessments



Introduction

This is our fifth report on the findings from our audits of local government entities' information technology general computer controls (GCC)[1]. GCC audits are an essential part of our audits of local government entities' financial statements and are a requirement of the Australian auditing standards[2]. Our GCC audits determine if entities' information technology and related internal controls effectively support the integrity, availability and confidentiality of the information and systems used to prepare the financial statements.

The entities vary in the nature and complexity of the information technology they use to process and maintain their financial information. However, the ever-changing internal and external threat environment exposes all entities to the risk of compromise. Appropriate controls help entities to protect their information and systems.

In 2022-23, we reported GCC findings to 76[3] entities, compared to 53 entities last year[4]. Eleven of these entities were provided with capability maturity assessments. These assessments look at how well-developed and capable entities' established IT controls are. This report summarises the results of our GCC findings and capability maturity assessments.

Our GCC audits incorporate recognised industry better practices and consider various factors, such as:

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

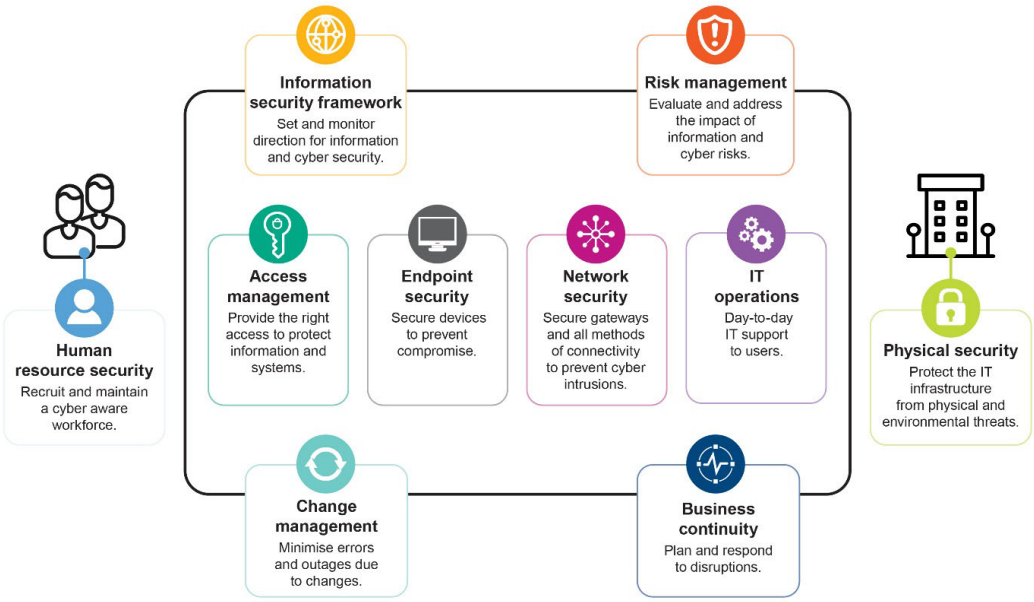
Figure 1 shows the 10 categories covered in our GCC audits.

[1] Our 2018-19 GCC and capability maturity assessments were done to inform our approach to assessing the sector's capability. 2018-19 results are not comparable to subsequent years and are therefore not shown.

[2] Auditing and Assurance Standards Board, *Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement*, AUASB, February 2020.

[3] Entities issued with GCC findings at 29 March 2024. Opinions of 10 local governments are not yet issued and their results are not included in this report. The entities are a mix of regional and metropolitan local governments.

[4] The number of entities issued GCC findings increased as auditing standards now require more consideration of IT and cyber security controls.



Source: OAG

Figure 1: General computer controls categories

Conclusion

In 2022-23, we reported 473 control weaknesses to 76 entities, compared to 324 weaknesses to 53 entities last year. The majority of these weaknesses were in categories that increase information and cyber security risks. Entities need to address these to protect their information and systems from security breaches.

While a number of entities addressed some prior year audit findings, most of the significant control weaknesses were not addressed. Entities should address these weaknesses as a priority and implement compensating[5] controls while progressing long term plans, such as migration to new platforms. Unresolved weaknesses can seriously impact the overall integrity of entities' IT environments and operations.

Our capability maturity assessments at 11 entities show improvement since our first assessments in 2019-20, with more controls meeting the benchmark. The biggest improvements have been in the categories of risk and change management, but significant improvement is still needed in all other categories.

This year's assessments showed some improvement in one of the five categories related to information and cyber security (network security) but only three entities met the benchmark. Categories of highest concern were access management, endpoint security and human resource security with no entities meeting the benchmark.

There was no material change in four categories (information security framework, IT operations, change management and IT risk management) while business continuity and physical security declined slightly.

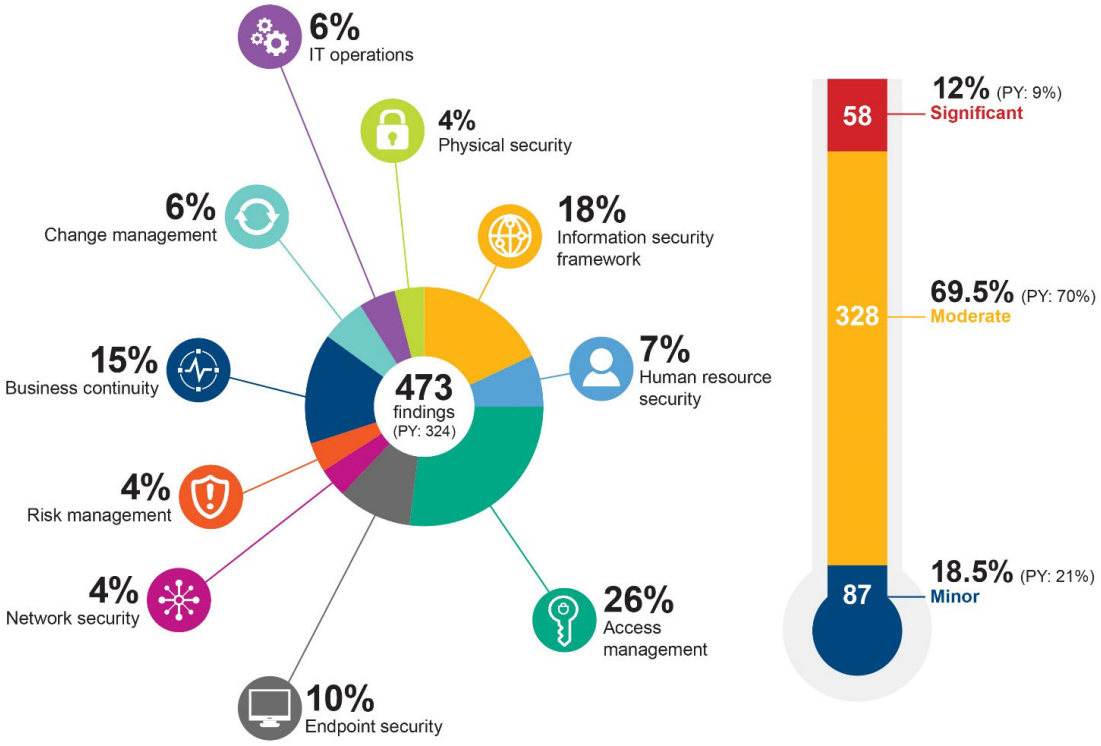
[5] Stop gap measures to address vulnerabilities where primary controls cannot be implemented due to limitations.

What we found: General computer controls

We reported 473 control weaknesses to 76 entities; 58 weaknesses were rated significant, 328 moderate and 87 minor. The increase in the number of entities issued GCC findings reflects changes in auditing standards[6] that require higher consideration of IT and cyber security controls.

There was a 3% increase in the number of significant findings compared to last year (Figure 2), which is mainly due to more entities issued findings this year. Although the majority of control weaknesses were rated moderate, these weaknesses combined significantly increase an entity's overall exposure to cyber threats.

Case studies throughout this report highlight the importance of good controls.



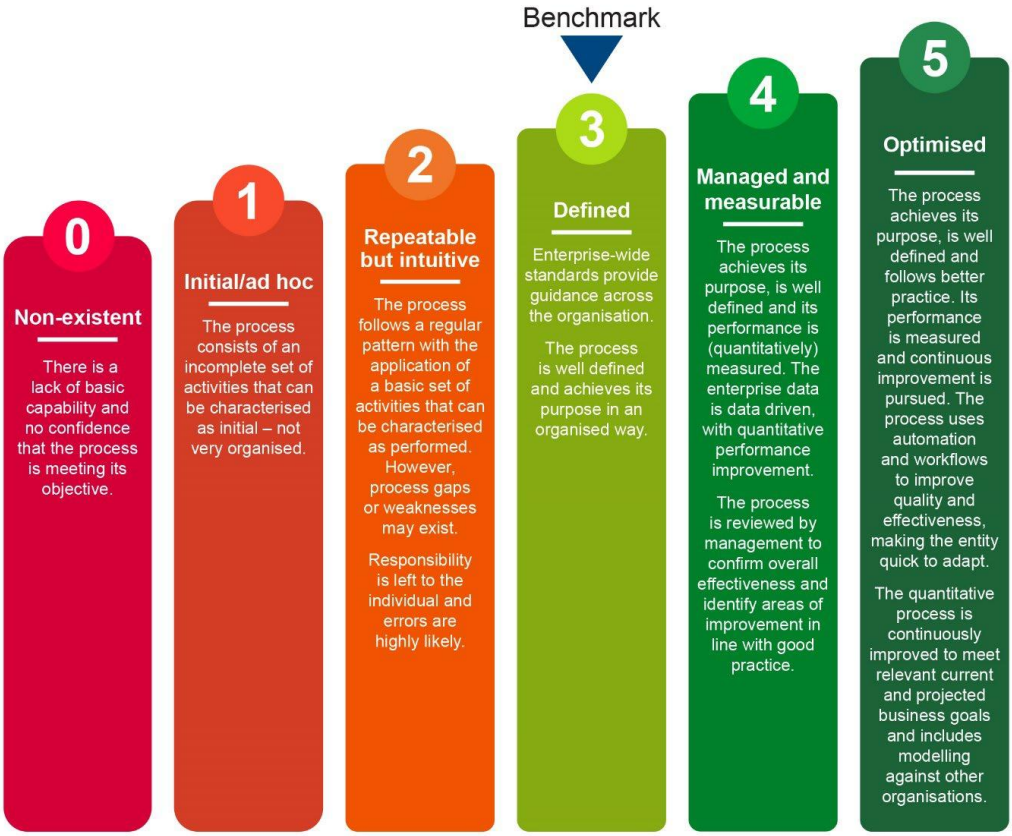
Source: OAG

Figure 2: Ratings and distribution of GCC findings in each control category

[6] Auditing and Assurance Standards Board, *The Consideration of Cyber Security Risks in an Audit of Financial Report*, AUASB, May 2021 *and* Auditing and Assurance Standards Board, *Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement*, AUASB, February 2020.

What we found: Capability assessments

We performed capability maturity assessments at 11 entities compared with 12 last year. This involved assessing the capability maturity level across the 10 GCC categories using a 0-5 rating scale[7] (Figure 3). To meet the benchmark, entities need to achieve a level 3 (Defined) rating or better.

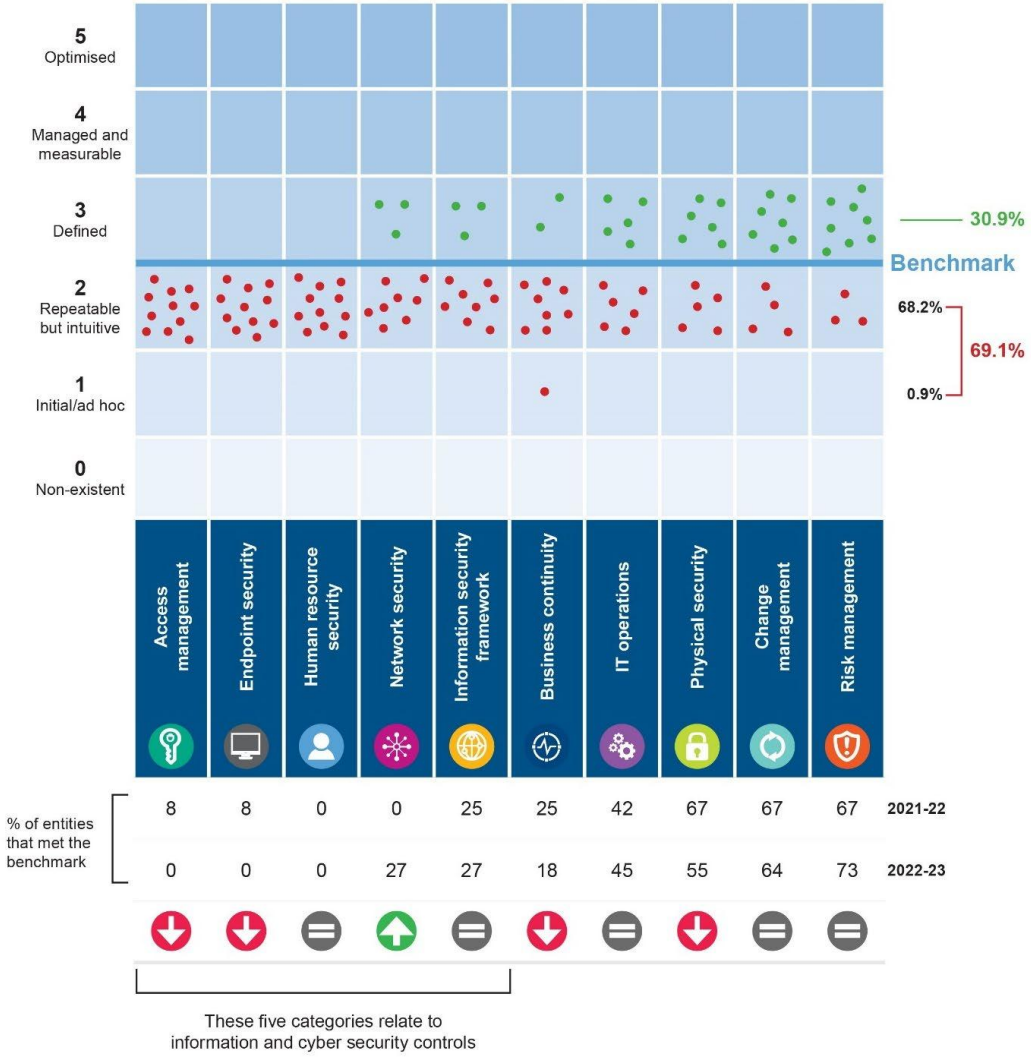


Source: OAG

Figure 3: Capability maturity rating scale and criteria

[7] The information within this maturity model assessment is derived from the criteria defined within the framework Control Objectives for Information Technologies 2019, released in 2018 by ISACA (an international professional association focused on IT governance).

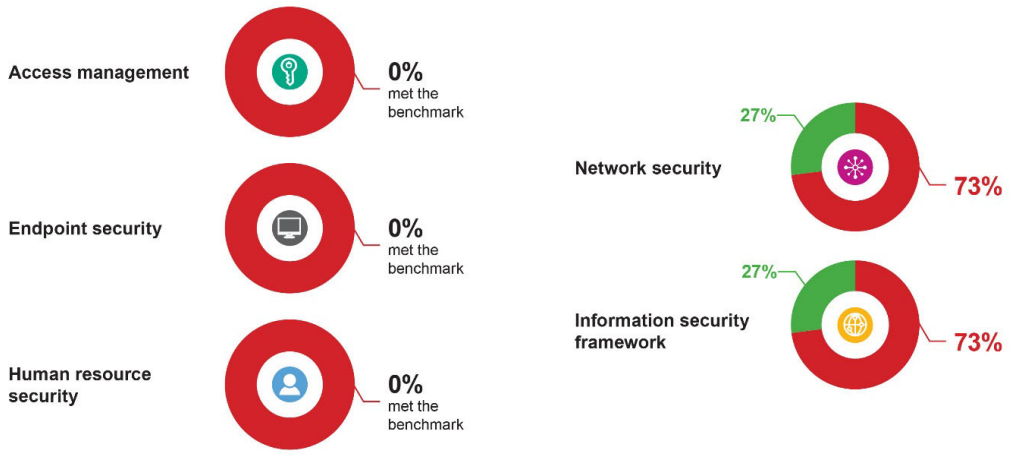
Figure 4 shows the results of our capability maturity assessments.



Source: OAG

Figure 4: Capability maturity assessment results

While there were improvements in network security this year, most entities were still not meeting the benchmark in the five information and cyber security categories (Figure 5). Entities must plan and implement fit-for-purpose controls to protect their operations and information from internal and external threats.



Source: OAG

Figure 5: Percentage of entities that met/did not meet the benchmark in the five information and cyber security categories

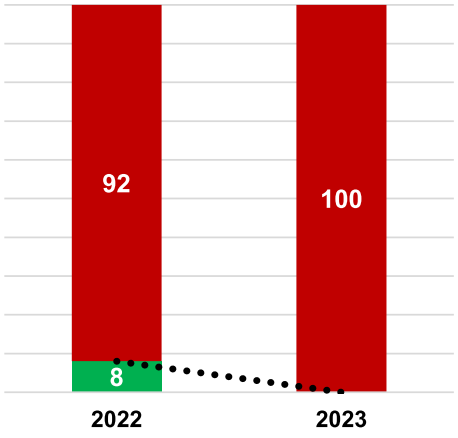
Entities continue to adopt digital technologies to improve engagement with their communities and deliver efficiencies in their service delivery. While there are many benefits to these digital technologies, there remains the ever-present and evolving nature of cyber security threats. Effective cyber security controls help entities manage risks, protect sensitive information and deliver services securely.

Entities are encouraged to implement the Australian Cyber Security Centre's mitigation strategies designed to protect against common cyber threats with a key focus on Essential Eight controls.

1. Access management

None of the 11 entities met the benchmark compared with one of 12 last year. This control category also had the highest number of significant GCC findings this year, mainly due to inappropriate or excessive administrative privileges within the finance systems. Poor access management controls increase the risk of security incidents, financial loss and reputational damage.

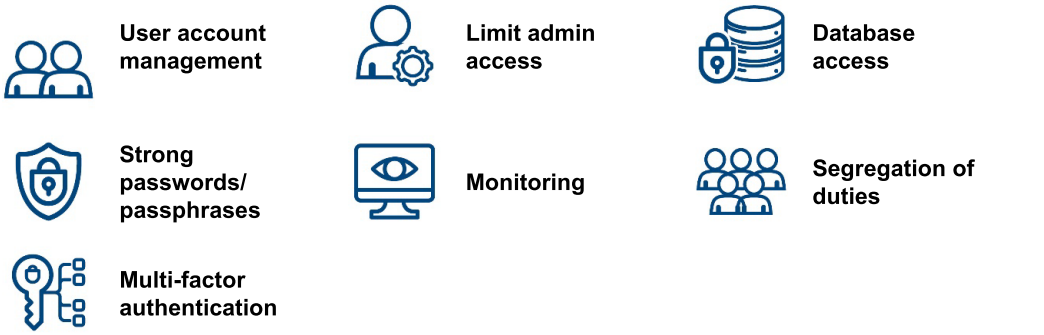
We assessed whether entities use the principle of least privilege to manage access, have strong authentication methods, monitor access and changes to data, and ensure key transactions cannot be performed end to end by the same individual (Figure 7).



Source: OAG

Figure 6: Percentage of entities that met/did not meet the benchmark

We have published a better practice guide[8] to help entities improve access management and protect information assets from unauthorised access. We encourage all public sector entities to adopt the principles in the guide.



Source: OAG

Figure 7: Key access management controls

Common weaknesses included:

- **Administrator privileges were not well managed** – excessive numbers of individuals were given administrator privileges. Administrators did not have separate non-privileged accounts for day-to-day tasks and administrator activity was not logged and monitored. Highly privileged accounts must be well managed as they can change system configurations, access rights and data.
- **Access and activity were not logged and monitored** – application, database and network access and activity were not appropriately logged or monitored to detect malicious activity. Entities should use fit-for-purpose tools to correlate and monitor activity from different systems (e.g. network, applications and databases).
- **Multi-factor authentication (MFA) was not used or not applied to all accounts** – a lack of MFA can increase the likelihood of unauthorised access.
- **Access was not reviewed** – entities did not review accounts to ensure they are required and have least privileges assigned to perform their function. Without a review of accounts (application, network, database, remote access, generic, system and administrator) there is an increased risk of unauthorised access.
- **Access was not appropriately approved** – access to key systems should be appropriately approved to prevent inappropriate access being granted.

The following case studies illustrate a range of control weaknesses in access management.

[8] Office of the Auditor General, *Digital Identity and Access Management – Better Practice Guide*, OAG, Perth, 28 March 2024.

Case study 1: Poor access controls increased the risk of fraud

At one entity, we found receipts had been deleted prior to end-of-day batch processing from the finance system. Poor access controls meant receipts could be deleted by any user without a trace to identify who deleted them. This could compromise the integrity of data and increases the likelihood of fraud.

Case study 2: Excessive superuser access

An entity had granted superuser access to almost all (24 out of 25) of its finance system users. This level of access allows users to inadvertently or maliciously change system configurations and potentially bypass system enforced expenditure authorisation and fraud prevention controls. This type of weakness increases the importance of manual controls as a last line of defence against error and fraud.

Case study 3: Excessive number of domain administrators

An entity granted the highest level of access rights (domain administrator) to 45 accounts, 40 of which also had database administrator rights to the finance and payroll system. Compromise of one account would give an attacker full access to the entity's systems. There is also a risk that unauthorised or unintentional changes of IT systems will occur.

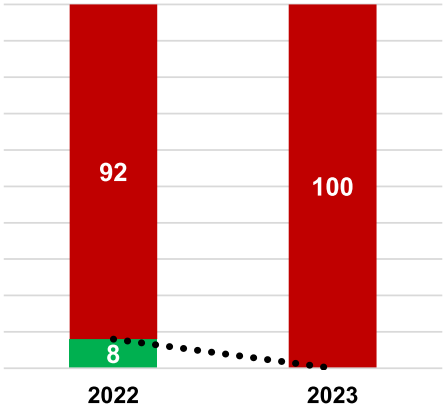
Case study 4: Lack of MFA

An entity is more vulnerable to being compromised through password guessing and phishing attacks, as it does not use MFA and uses single-sign-on for access to its network and finance application. This means a threat actor would gain access to all systems if the entity is compromised. While staff security awareness training can help reduce some risks, entities should prioritise MFA.

2. Endpoint security

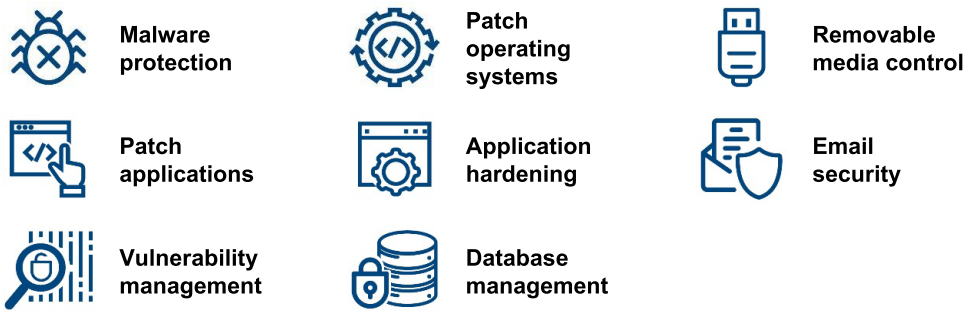
None of the 11 entities met the benchmark, compared with one of 12 last year.

Entities need to implement fit-for-purpose controls to protect endpoints (computers, servers, phones and network devices) from known threats (Figure 9).



Source: OAG

Figure 8: Percentage of entities that met/did not meet the benchmark



Source: OAG

Figure 9: Key endpoint security controls

Common weaknesses included:

- **Unauthorised applications are not prevented** – malicious applications could successfully compromise entities' systems and information.
- **Vulnerability management was ineffective** – systems that are not regularly scanned and patched to fix known vulnerabilities are more susceptible to compromise.
- **Unsupported systems** – key business systems and operating system software were no longer supported by vendors and were therefore not receiving updates designed to fix known vulnerabilities.

The following case study illustrates a common weakness in endpoint security.

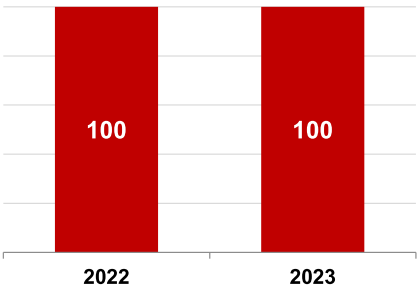
Case study 5: Ineffective application control

An entity only allowed applications and scripts to run from trusted locations. However, all staff could add applications and scripts to these locations to execute them. There is a higher likelihood of malware infections and compromise if unapproved applications are not blocked.

3. Human resource security

Similar to last year, none of the 11 entities met the benchmark in this category. Human resource security ensures employees, contractors and third-party vendors understand their responsibility to protect information during and after engagement.

Fit-for-purpose screening, onboarding and offboarding procedures, and cyber security education are key controls in this category (Figure 11).



Source: OAG

Figure 10: Percentage of entities that did not meet the benchmark

Figure 11: Key human resource security controls

Common weaknesses included:

- **Inadequate background screening** – without fit-for-purpose background screening processes, entities may engage unsuitable individuals (staff or contractors) to positions of trust, increasing insider threat risks.
- **Lack of security awareness training** – regular cyber security education creates a culture of awareness that helps prevent social engineering attacks such as phishing and business email compromise.
- **Exit procedures were not completed** – not completing exit procedures can contribute to unauthorised access to entities' premises, systems and information. This may also increase post-employment integrity risks such as the use or disclosure of confidential information.

The following case study illustrates weaknesses in human resource security.

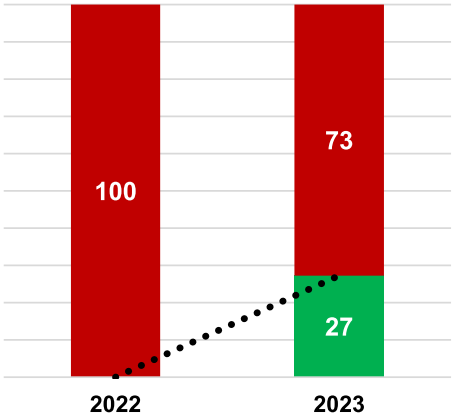
Case study 6: Staff and contractors were not aware of their information security responsibilities

An audited entity did not require its staff and contractors to understand and acknowledge acceptable use of IT resources. Contractors were also not required to sign any confidentiality agreements. There is a higher likelihood that individuals may not understand their information security obligations resulting in data breaches.

4. Network security

There was an improvement this year with three of the 11 entities meeting the benchmark, compared to none last year. The three entities improved their controls to manage and secure network infrastructure, segregated their network and had good monitoring.

Key controls to prevent and limit the extent of cyber attacks include securely configured network devices, network segregation, control over unauthorised connections and regular penetration testing to check that controls are operating as expected (Figure 13).



Source: OAG

Figure 12: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 13: Key network security controls

Common weaknesses included:

- **A lack of controls to block unauthorised devices on the physical network** – unauthorised devices can spread malware or be used to eavesdrop on communications or access sensitive information.
- **Firewall configurations were not reviewed** – reviews help to identify and promptly correct exploitable configuration weaknesses. Firewalls are important security systems that control and protect networks against cyber intrusions.
- **Networks were not segregated** – segregation controls to prevent lateral movement between network segments have not been implemented. Without proper network segregation a cyber breach would be difficult to contain.

The following case study illustrates a common weakness in network security.

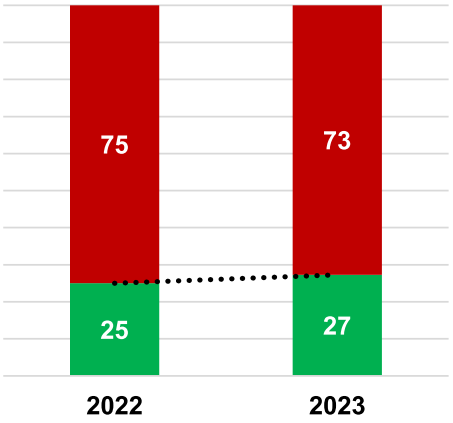
Case study 7: Publicly accessible network port allowed access

An entity did not prevent unauthorised devices from connecting to its physical network and had not segregated its network. We were able to connect a device to the entity's network, view all IT systems and infrastructure and access database, storage and CCTV servers. This entity is at high risk of compromise as unauthorised devices could be used to attack its systems or spread malware.

5. Information security framework

Three of the 11 entities met the benchmark compared with three of 12 last year. A structured approach ensures IT and security initiatives align with business objectives to protect systems and information against emerging threats.

We assessed whether entities had fit-for-purpose information and cyber security policies to govern and mitigate against current and emerging security risks (Figure 15).



Source: OAG

Figure 14: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 15: Key information security framework controls

Common weaknesses included:

- **Information and cyber security policies did not exist or were outdated** – without fit-for-purpose policies, entities' information security objectives are less likely to be achieved.
- **Lack of IT strategy** – an IT strategy is crucial for informing decisions about technology and cyber security investments and implementation. The strategy should align technology and cyber security initiatives with business objectives.

- **Data loss prevention controls were missing or inadequate** – the inadvertent or malicious leakage of information may go undetected and lead to reputational damage.

The following case study illustrates a common information security framework weakness.

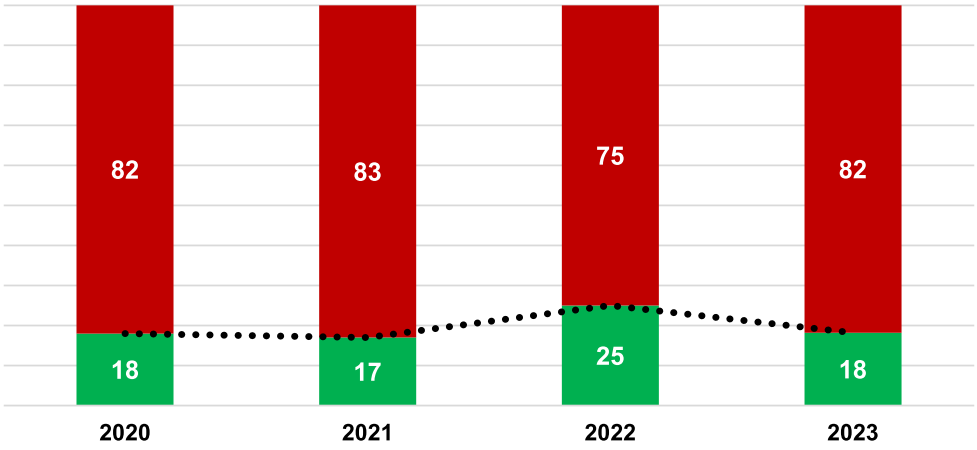
Case study 8: Assurance over cloud based services

An entity did not have a mechanism to know if its vendor's cloud security controls protected its information and systems. When key services are delivered through cloud systems, the cloud vendor must provide important security controls to protect the information and systems. Entities need adequate assurance and visibility that the vendor's controls operate effectively to deliver services in a secure manner.

Independent assurance reports such as a service organisation controls report (SOC2) provide insights into vendor management of cloud infrastructure and systems.

6. Business continuity

We saw a minor decline this year. Only two of the 11 entities met the benchmark in this category, compared with three out of 12 last year. Entities should have fit-for-purpose plans and procedures to guide their response to disruptive events (Figure 17). These should be based on a business impact assessment and agreed recovery objectives.



Source: OAG

Figure 16: Percentage of entities that met/did not meet the benchmark

Source: OAG

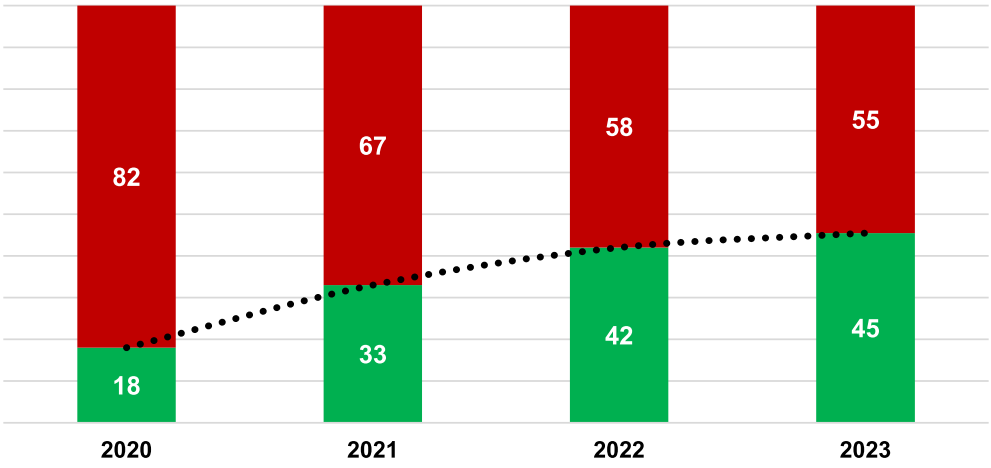
Figure 17: Key business continuity controls

Common weaknesses included:

- **Missing or outdated continuity plans** – delivery of services to the community may experience prolonged outages if adequate continuity plans do not exist.
- **Plans were not tested** – continuity plans must be regularly tested to confirm they can meet recovery expectations.
- **Lack of backup restoration testing** – entities should regularly restore their backups to ensure complete systems can be recovered to a common point. Business-as-usual recovery of files is not sufficient.

7. IT operations

There was no material change in IT operations this year with five of the 11 entities meeting the benchmark. We assessed if the entities had fit-for-purpose service desk processes and appropriately managed IT vendors and IT assets (Figure 19).



Source: OAG

Figure 18: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 19: Key IT operations controls

Common weaknesses included:

- **IT asset registers were poorly maintained and stocktakes not performed** – inadequate management of IT assets can result in loss or theft, leading to financial loss and reputational damage.

- **Service level agreements were not in place or monitored** – a lack of or poorly monitored service level agreements could result in substandard services.

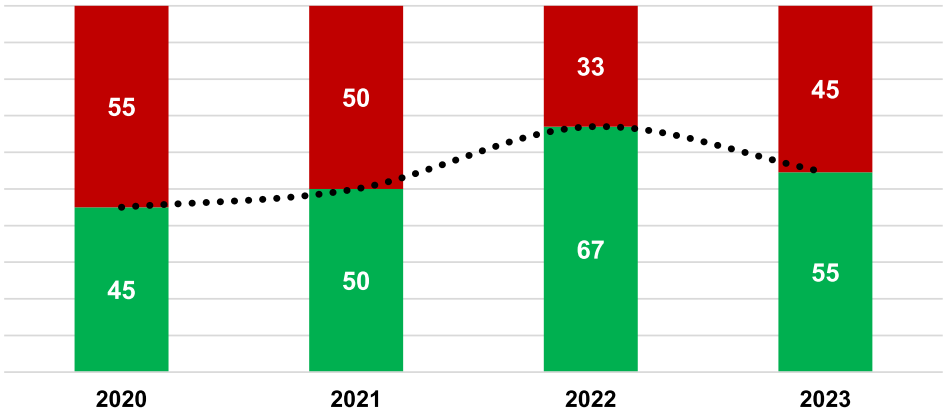
The following case study illustrates a common weakness in IT operations.

Case study 9: Supply chain risks

An entity's service agreement did not include information and cyber security requirements for the vendor to comply. Security expectations should be clearly documented in third-party agreements to reduce supply chain risk. Vendors may not adequately protect entity information and systems if requirements are not clearly documented in the service agreement. Threat actors will often target vendors to indirectly compromise entities, highlighting the importance of vendors' sound security practices.

8. Physical security

Physical security declined this year with only six of the 11 entities meeting the benchmark in this category, compared with eight of the 12 last year. The decline was due to a deterioration in server room access controls. We assessed if entities had controls to protect IT infrastructure from unauthorised access, deliberate damage and environmental hazards such as heat, fire and humidity (Figure 21).



Source: OAG

Figure 20: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 21: Key physical security controls

Common weaknesses included:

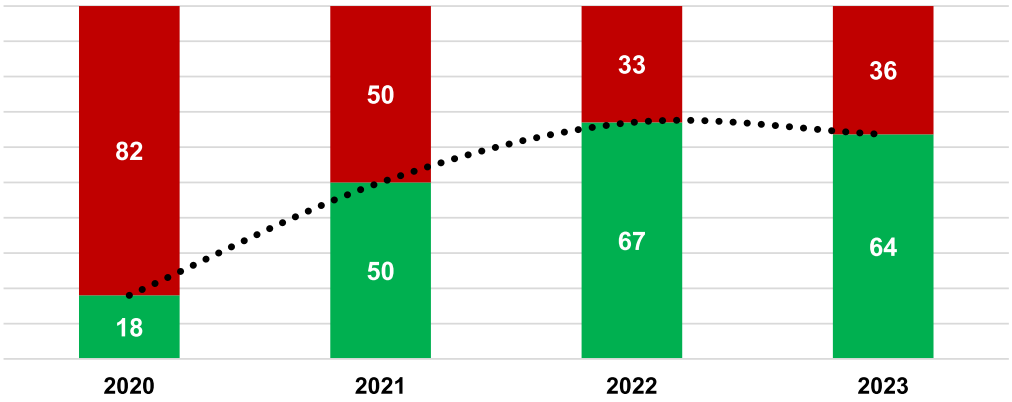
- **Access to equipment enclosures/rooms was not controlled** – access to equipment enclosures should be authorised, recorded and reviewed to reduce malicious or

unintentional damage to IT equipment. Additional controls may include access alarms or CCTV.

- **Dedicated server rooms were not well maintained** – server rooms need to be clear of unwanted material and cabled tidily to reduce the likelihood of damage to infrastructure.

9. Change management

There was no material change this year. Seven of the 11 entities met the benchmark, compared with eight of the 12 last year. Well managed change control processes reduce the likelihood of disruptions (Figure 23).



Source: OAG

Figure 22: Percentage of entities that met/did not meet the benchmark

Source: OAG

Figure 23: Change management controls

A common weakness was:

- **Change management processes were not documented or not followed** – this increases the chance of errors or delays when implementing changes and the likelihood of disruptions and outages.

The following case study illustrates a common weakness in change management.

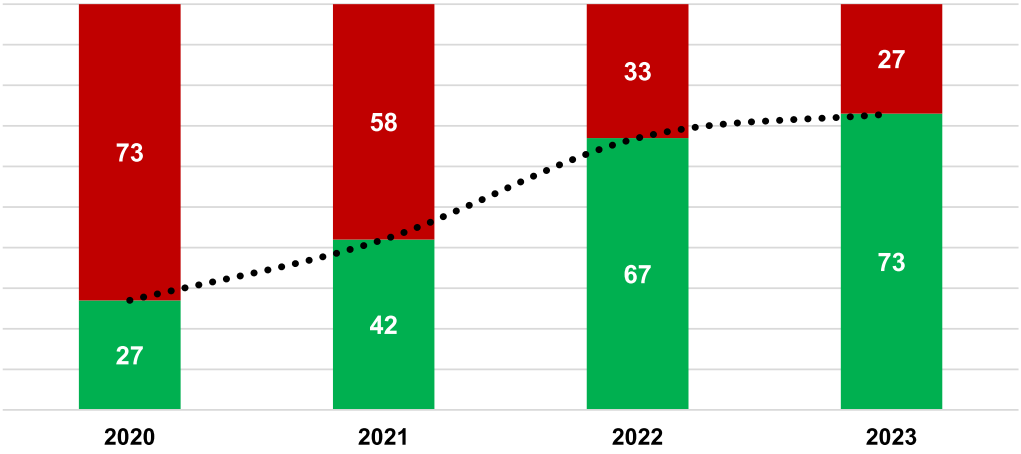
Case study 10: Changes were not appropriately assessed

At one entity, we found staff could approve their own change request. In some instances, the changes were poorly documented and lacked an impact and risk assessment. These

weaknesses increase the likelihood that changes will adversely impact the entity's operations.

10. Risk management

There was no material change this year. Eight of the 11 entities met the benchmark, compared with eight of the 12 last year. A fit-for-purpose risk management process helps entities prioritise information and cyber security risks.



Source: OAG

Figure 24: Percentage of entities that met/did not meet the benchmark

We reviewed risk management policies and processes and if they considered key cyber risks, threats and vulnerabilities (Figure 25).

Source: OAG

Figure 25: Risk management controls

Common weaknesses included:

- **IT risk registers not in place or not maintained** – IT risks may not be effectively managed without adequate documentation.
- **IT risks not reviewed –** timely review of risks is important to ensure mitigation strategies are cost efficient and operate effectively.

Recommendations

1. **Access management**

   To ensure only authorised individuals have access, entities should:

   a. implement effective access management processes

   b. regularly review active user accounts

   c. enforce strong passphrases/passwords and phishing-resistant multi-factor authentication

   d. limit and control administrator privileges

   e. implement automated access monitoring processes to detect malicious activity.

2. **Endpoint security**

   Entities should:

   a. implement effective controls against malware

   b. promptly identify and address known vulnerabilities

   c. control installation of software on workstations, servers and mobile devices

   d. prevent unapproved applications and macros from executing

   e. enforce minimum baseline controls for personal or third-party devices connecting to their systems

   f. implement controls to prevent impersonations and detect/prevent phishing emails

   g. review and harden server and workstation configurations.

3. **Human resources security**

   Entities should ensure that:

   a. pre-employment screening is conducted for key positions

   b. confidentiality/non-disclosure requirements are in place and understood by individuals

   c. termination procedures are in place and followed to ensure timely access cancellation and return of assets

   d. ongoing security awareness training programs are in place and completed by all staff.

4. **Network security**

   Entities should:

   a. implement secure administration processes for network devices

   b. regularly review their network security controls through penetration tests

   c. segregate their network

   d. prevent unauthorised devices from connecting to their network

e. adequately secure wireless networks.

5. Information security framework

Entities should:

a. maintain clear information and cyber security policies and governance structures to oversee and direct IT operations and cyber security

b. conduct regular assessments or gain comfort through assurance reports

c. obtain and review service organisation controls (SOC2) report or equivalent when they use software-as-a-service (SaaS) application for key systems including payroll and finance

d. classify information and implement data loss prevention controls.

6. Business continuity

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

7. IT operations

Entities should:

a. implement appropriate IT incident management processes

b. regularly monitor supplier performance

c. perform regular reviews of inventory assets

d. have formal service level agreements with suppliers.

8. Physical security

Entities should:

a. implement effective physical access controls to prevent unauthorised access

b. maintain environmental controls to prevent damage to IT infrastructure arising from heat, moisture, fire and other hazards

c. gain assurance that third-party providers manage their data centres appropriately.

9. Change management

Entities should:

a. consistently apply change control processes when making changes to their IT systems

b. assess and test changes before implementation to minimise errors

c. maintain change control documentation

d. implement controls to detect unauthorised changes.

10. Risk management

Entities should:

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

b. ensure IT, information and cyber security risks are identified, assessed and treated within appropriate timeframes

c. provide executive oversight and remain vigilant against the risks of internal and external threats.

In accordance with section 7.12A of the *Local Government Act 1995*, local government entities should prepare a report on any matters identified as significant in the local government's audit report[9]. The report should be given to the Minister for Local Government within three months of the local government receiving the audit report and published on the local government's website.

[9] An audit report includes the independent auditor's opinion and the auditor's management report (interim and final management letters) as described in regulation 10 of Local Government (Audit) Regulations 1996. Further information on what is an audit report is available on our website (https://audit.wa.gov.au/resources/local-government/faqs/#faq-21828).

Auditor General's 2023-24 reports

Number	Title	Date tabled
16	Local Government 2022-23 – Information Systems Audit Results	27 May 2024
15	State Government Advertising	15 May 2024
14	State Government 2022-23 – Information Systems Audit	12 April 2024
13	Provision of Supplementary Information to the Standing Committee on Estimates and Financial Operations – Opinions on Ministerial Notifications	5 April 2024
12	Digital Identity and Access Management – Better Practice Guide	28 March 2024
11	Funding for Community Sport and Recreation	21 March 2024
10	State Government 2022-23 – Financial Audit Results	20 December 2023
9	Implementation of the Essential Eight Cyber Security Controls	6 December 2023
8	Electricity Generation and Retail Corporation (Synergy)	8 November 2023
7	Management of the Road Trauma Trust Account	17 October 2023
6	2023 Transparency Report: Major Projects	2 October 2023
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Local Government 2021-22 – Financial Audit Results	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

Office of the Auditor General for Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for Western Australia

11.1.3 (2024/MINUTE NO 0020) OAG Report to ARC - Disaster Recovery Planning

Executive A/Director Corporate and System Services
Author Head of Information Technology
Attachments 1. Office of the Auditor General - Local Government IT Disaster Recovery Planning - 31 May 2024 ⇩

Officer Recommendation/Committee Recommendation
MOVED Deputy Mayor C Stone SECONDED Cr K Allen
That Council:

(1) RECEIVES the Office of Auditor General's Performance Audit Report Office of Auditor General State Government 2022-23 Local Government IT Disaster Recovery Planning, as attached to the Agenda.

CARRIED 5/0

Background

The Office of the Auditor General (OAG) has published for the past 16 years, reporting on state government entity's general computer controls.

The City of Cockburn (the City) has presented similar reports to the Audit, Risk and Compliance Committee (ARC) in the past, to give context and relevance of efforts ongoing in the public sector.

To ensure the City adopts best practice in this area, the City independently submits a report to the ARC on the OAG audit report recommendations, highlighting any specific opportunities for improvement from the OAG report that can benefit the City's cyber security posture and specific computer controls.

Submission

N/A

Report

Purpose of the OAG Audit Report

The purpose of the OAG report is to evaluate the effectiveness of ICT disaster recovery planning across local governments, ensuring that they are adequately prepared to recover from ICT-related disruptions and continue delivering critical services.

Important Matters Identified by the OAG

1. **Enhanced Preparedness:** Local governments need to improve their disaster recovery plans (DRPs) to ensure they are prepared for ICT disruptions. This involves clearly defining activation criteria, responsibilities, and procedures.

2. **Staff Training and Awareness:** The report highlights the need for better training and awareness among staff regarding their roles in disaster recovery. This can help mitigate the impact of ICT disruptions and facilitate quicker recovery.

3. **Improved Communication:** Effective communication plans are essential for coordinating disaster recovery efforts. Local governments must address any deficiencies in their current communication strategies to ensure clear and timely information flow during disruptions.

4. **Regular Testing:** The importance of regular testing of both individual components and integrated systems is emphasized. Local governments should conduct thorough and frequent tests to identify and rectify weaknesses in their DRPs.

5. **Comprehensive Recovery Planning:** Full recovery tests, including relocating and operating live systems from secondary locations, are necessary to understand the overall effectiveness of the DRP. Local governments must ensure their plans are robust and capable of handling real-life scenarios.

6. **Continuous Improvement:** The report implies that disaster recovery planning is an ongoing process. Local governments should continuously update and improve their DRPs based on lessons learned from tests and actual incidents.

Implication(s) for local government / the City.

The OAG report recommends that local government entities should:

1. Assess their recovery requirements and appropriately document detailed disaster.
2. Periodically test their recovery plans, to verify that key IT systems and information can be restored in line with entity expectations.
3. Review and update their IT vendor service agreements to include obligations for disaster recovery planning, testing and response. Any recourse if services are not met should also be documented.

City Response to OAG Audit

A copy of the OAG audit is in Attachment 2, and below are responses provided by the Information and Communications Technology Manager to recommendations contained in the OAG audit:

No.	Office of the Auditor General Recommendation	City Response
1.	Assess the recovery requirements and appropriately document detailed disaster.	The City currently has a Disaster Recovery Plan and environment that are fit for purpose, providing a strong foundation for ongoing operational continuity. The City is undergoing significant IT infrastructure changes, including replacing its virtual desktop computing environment with laptops and migrating its Enterprise Resource Planning (ERP) solution TechnologyOne, to a SaaS platform. These changes require a thorough reassessment of the City's disaster recovery requirements to ensure continued effectiveness. The shift to a primarily laptop-based environment later this year provides greater flexibility and mobility for staff, further enabling remote work. The disaster recovery plan must now also account for scenarios where staff are able to work in a highly mobile manner. This includes strategies for remote data backup and recovery and ensuring all laptops are equipped with the necessary software to access recovery systems from any location. Additionally, moving TechnologyOne to a SaaS platform significantly alters the server infrastructure, requiring the inclusion of the provider's disaster recovery capabilities and Service Level Agreements in the City's plan. Updating the Disaster Recovery Plan involves documenting detailed recovery procedures, clearly defining roles and responsibilities, and establishing a comprehensive communication strategy. By incorporating these changes, the City will enhance its preparedness and resilience, ensuring effective recovery from ICT disruptions and the continuation of critical services.
2.	Periodically test recovery plans, to verify that key	The City currently tests its ability to restore servers from backup every six months. Considering the OAG report and pending changes to

	IT systems and information can be restored in line with entity expectations.	server and desktop infrastructure, including the shift to a laptop-based environment and the migration of the TechnologyOne ERP solution to a SaaS platform, the City will review and update its Disaster Recovery Plan. This update will ensure the Plan continues to meet the City's business continuity requirements, incorporating additional testing procedures such as tabletop reviews to simulate disaster scenarios and validate recovery strategies for the new IT environment.
3.	Review and update IT vendor service agreements to include obligations for disaster recovery planning, testing and response. Any recourse if services are not met should also be documented.	The City's ERP solution, TechnologyOne, is moving to a SaaS platform, necessitating a thorough review of vendor agreements to ensure alignment with the City's Disaster Recovery Plan and Policies. As part of the Disaster Recovery Plan Review, all existing agreements with vendors will be scrutinised to ensure they adequately cover disaster recovery procedures and objectives. Additionally, the City will mandate that new agreements with vendors specifically address obligations for disaster recovery planning, testing, and response. This will include detailed documentation of recourse options if vendors fail to meet their disaster recovery obligations. By doing so, the City aims to ensure robust and reliable disaster recovery measures that support its business continuity requirements.

Strategic Plans/Policy Implications

Listening and Leading
A community focused, sustainable, accountable, and progressive organisation.
• Best practice Governance, partnerships and value for money.
• Employer of choice focusing on equity, innovation and technology.

Budget/Financial Implications

N/A

Legal Implications

Sections 7.1, 7.12A(3) and 7.12AJ of the *Local Government Act 1995* refer.

Community Consultation

N/A

Risk Management Implications

OAG performance audits constitute the fourth line of defence in the OAG's 'Four Lines of Defence Assurance Model' which the City has adapted in the *City of Cockburn Enterprise Risk Management Framework*.

The OAG has identified risks in its audit report and the City needs to manage these risks by implementing appropriate control measures.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil

6:26pm Cr Zhang returned to the meeting.

Office of the Auditor General
Serving the Public Interest

Report 17: 2023-24 | 31 May 2024

PERFORMANCE AUDIT

Local Government IT Disaster Recovery Planning

Office of the Auditor General for Western Australia

Audit team:
Aloha Morrissey
Paul Tilbrook
Adam Dias
Lyndsay Fairclough
Information Systems Audit team

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.

Image credit: shutterstock.com/Panya_photo

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Local Government IT Disaster Recovery Planning

Report 17: 2023-24
31 May 2024

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

LOCAL GOVERNMENT IT DISASTER RECOVERY PLANNING

This report has been prepared for submission to Parliament under the provisions of sections 24 and 25 of the *Auditor General Act 2006*.

Performance audits are an integral part of my Office's overall program of audit and assurance for Parliament. They seek to provide Parliament and the people of WA with assessments of the effectiveness and efficiency of public sector programs and activities, and identify opportunities for improved performance.

This audit assessed whether six non-metropolitan local government entities of varying sizes effectively plan and test their ability to recover their information technology systems following a disaster.

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

Caroline Spencer
Auditor General
31 May 2024

Contents

Auditor General's overview

Local government entities, like other public sector organisations, rely heavily on information technology (IT) systems to operate and deliver a vast range of services to their communities. This makes it increasingly important for all entities, regardless of their size, to have planned their response to disruptions such as cyber attacks and natural disasters.

My Office's previous information systems audits have consistently found issues with local government disaster recovery planning[1]. This audit was an opportunity to delve a little deeper into entities' preparedness. Encouragingly, all the entities we audited were aware of the importance of disaster recovery planning to recover their IT systems and most had developed plans. However, none were fully prepared.

Further, as all the entities we audited relied on third party vendors to manage and recover their IT systems, it is important that vendor service agreements clearly define what is to be delivered.

I encourage entities to use the better practice principles we have included in this report to improve disaster recovery planning across the local government sector. Timely recovery of IT systems after a disaster can reduce financial and reputational losses, and minimise delays in delivering services to the public.

[1] Office of the Auditor General, *Local Government 2022-23 – Information Systems Audit Results*, OAG, 27 May 2024, accessed 28 May 2024.

Executive summary

Introduction

This audit assessed whether six non-metropolitan local government entities of varying sizes effectively plan and test their ability to recover their information technology (IT) systems following a disaster.

We have anonymised findings throughout this report to not compromise the security and continuity of systems and information at the entities. Detailed findings were provided to each entity.

Background

There are 147 local government entities in WA who provide key services and facilities to their communities. This may include waste management, road repair or broader services such as administration of marinas, cemeteries, airports, medical centres and retirement homes. All entities depend to some degree on functioning IT systems. These systems can be disrupted by disasters such as damage to equipment, cyber attacks, fire or flood. Any such disruption may impact an entity's ability to provide its services.

Entities can best prepare themselves to deal with the impact of a disaster on their systems through the process of IT disaster recovery planning. Good planning should consider several elements, including how and when the plan should be activated, who is responsible, and a clear description of recovery procedures (Appendix 1). These steps are typically captured in a disaster recovery plan (DRP). DRPs generally focus on major disruptions and are not concerned with minor issues such as system glitches or brief losses of communications that occur as part of normal day-to-day operations.

Conclusion

None of the audited entities were ready to recover their IT systems following a disaster as they had not effectively planned or tested their DRPs. All acknowledged the importance of disaster recovery planning and most had developed DRPs. However, only one DRP was adequate and none had tested if their plans would work. Appropriate planning and testing help reduce the likelihood of prolonged system outages that can disrupt business operations, the delivery of services to the community, and be costly to fix.

All the audited entities used third party vendors to manage and recover their IT systems. However, none had adequate service agreements in place. The agreements did not clearly define entities' recovery expectations or vendors' obligations to prepare and test plans. In one case, the entity did not have a formal arrangement in place and relied on a verbal understanding. Clear and appropriate service agreements help ensure vendors understand an entity's needs and will prepare for and respond to a disaster as expected.

Findings

Entities did not appropriately document how they plan to recover their IT systems

Most entities did not fully document how they will respond to a disaster. Five entities developed DRPs, but only one of these included enough information to be effective. The others were missing key elements, such as:

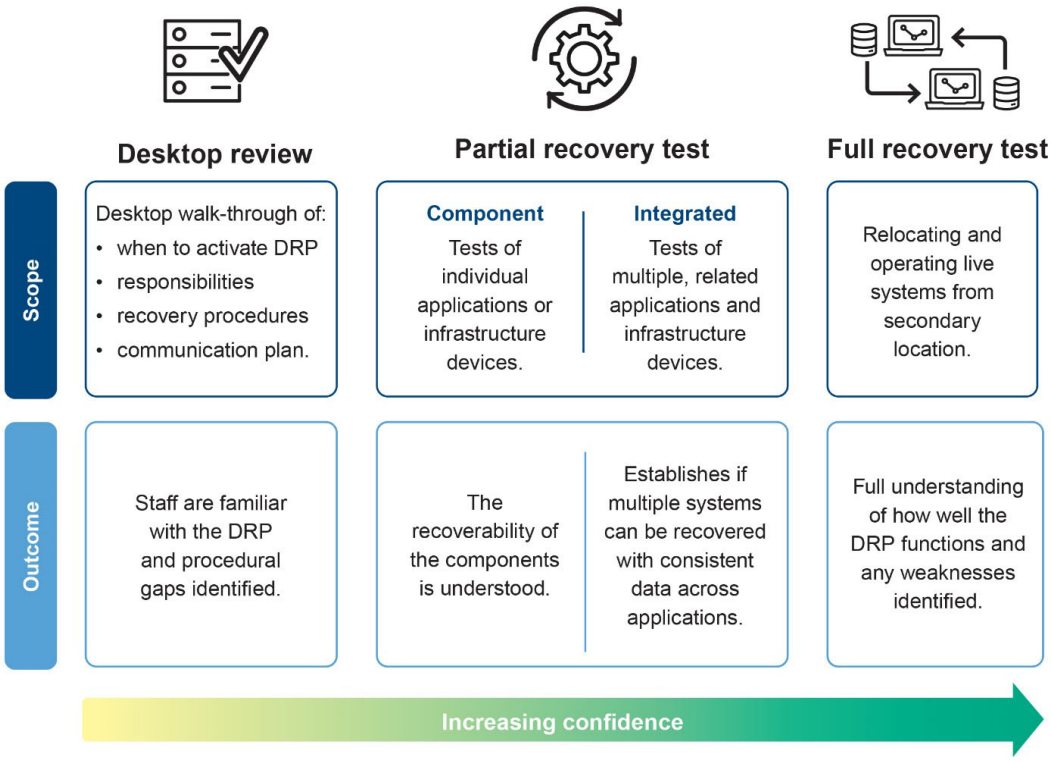
- roles and responsibilities
- when and how to activate the plan
- recovery objectives aligned to entity needs
- which business systems are most important, the associated IT systems and the order in which they need to be restored
- detailed recovery steps.

One entity did not document how it planned to recover its IT systems at all. Entities were aware of the need to recover their IT systems and all had developed high-level business continuity plans which included a requirement to recover IT systems. However, these plans did not have enough detailed information to help manage IT disasters and fully recover key systems. Disasters are inherently disruptive, stressful and unusual situations. If entities do not have a clear, documented plan, they may not be able to respond effectively and restore systems to provide needed services to the community.

Entities did not know if their plans would work as expected

The five entities with DRPs did not test if these plans would successfully recover IT systems and information to meet business needs. As part of day-to-day operations, all had restored individual data files from their backups. However, they had not tested if full IT systems recovery was possible or if recovered data was consistent across applications. Without periodic testing of system recovery, entities cannot be confident their recovery plans and the steps they contain are achievable, up-to-date and effective.

Entities did not determine the nature and frequency of the testing they needed. For example, testing can range from desktop exercises to the recovery of full systems and may include part or all of the DRP (Figure 1). As testing comes at a cost, can be disruptive to entity operations and can lead to accidental outages, entities need to determine the combination of levels of testing most appropriate for their business.



Source: OAG based on ISO/IEC 27031:2011[2]

Figure 1: Levels of disaster recovery testing

Service agreements with IT vendors were not adequate

Entities' agreements with IT vendors were not detailed enough to deal with disasters. All the entities relied on IT vendors to participate in disaster recovery planning and testing and to respond in case of disasters. Five had service agreements in place but these were missing all or some of the following:

- a clear description of the disaster recovery service required
- where the disaster recovery services are to be provided
- a description of the hardware required and delivery timeframes
- a clear requirement for the vendor to participate in disaster recovery planning
- how vendors are involved in testing (nature and frequency)
- timeframes for recovering from a disaster
- processes for monitoring, tracking and evaluating vendor performance
- recourse if expectations are not met.

[2] International Organization for Standardization and the International Electrotechnical Commission, *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*, ISO, 2011.

One entity only had a verbal understanding with its IT vendor. In response to the audit, the entity started developing a written agreement. If entities do not have clear and detailed agreements with their vendors, there may be misunderstandings about the service to be supplied. This could impact entities' ability to prepare for a disaster and prolong the restoration of IT systems after an event.

Case study 1: Inadequate service agreement could delay recovery

One entity had a single physical server running its IT systems. If a disaster damages this server, the entity's DRP requires the IT vendor to provide a replacement within 48 hours. However, the agreement with the vendor did not include the 48-hour timeframe nor outline hardware specifications for the replacement.

If the hardware requirements are not clearly stated, the vendor may not be able to deliver appropriate equipment in the required timeframe. This may prolong the entity's reliance on manual processes and increase the time needed to enter the backlog of information after restoration.

Recommendations

The six audited local government entities should:

1. assess their recovery requirements and appropriately document detailed disaster recovery plans. Consideration should be given to key elements as outlined in Appendix 1
2. periodically test their recovery plans, to verify that key IT systems and information can be restored in line with entity expectations
3. review and update their IT vendor service agreements to include obligations for disaster recovery planning, testing and response. Any recourse if services are not met should also be documented.

In accordance with section 7.12A of the *Local Government Act 1995*, the six audited local government entities should prepare a report on any matters identified as significant to them for submission to the Minister for Local Government within three months of this report being tabled in Parliament, and within 14 days of submission publish it on their website.

Response from the audited local government entities

Audited entities generally accepted the recommendations and confirmed that where relevant, they have amended plans and procedures or will improve practices for effective disaster recovery planning.

Audit focus and scope

This audit assessed whether six non-metropolitan local government entities of varying sizes across WA had effective plans to manage IT disruptions.

Our criteria were:

- Are plans aligned to current business needs?
- Are plans tested to verify effectiveness and continuous improvements?

We visited each entity and:

- reviewed their policies and procedures for disaster recovery planning and testing
- examined other relevant documents and records
- conducted interviews with key staff.

This was an independent performance audit, conducted under section 18 of the *Auditor General Act 2006*, in accordance with Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other ethical requirements related to assurance engagements. Performance audits focus primarily on the effective management including compliance with legislative and other requirements of entity programs and activities. The approximate cost of undertaking the audit and reporting was $230,000.

Appendix 1: Better practice principles – key elements of IT disaster recovery plans

The table below shows key elements of a disaster recovery plan to help guide an effective plan. These elements are not exhaustive and entities should assess their own needs as part of their preparation.

Key elements	Description
Purpose and scope	The purpose and scope of the plan should be defined and agreed with senior management. It should include: • details and location of the main technology supporting the business • an overview of the organisation and people that manage the technology • the security classification of systems • the relationship of this plan to other business continuity, incident response and cyber security response plans.
Roles and responsibilities	Cleary define the positions, teams and IT vendors with responsibilities for governance, incident escalation and IT disaster recovery. These should have the appropriate skills and knowledge, or contractual arrangements in place. Decision-making and spending authorities should also be clearly documented.
Contact details	Contact details for all key external and internal stakeholders.
Plan activation	Clearly document the circumstances and timeframes that cause the plan to be invoked.
Recovery objectives	Entities should assess the risks and effects a disaster will have to key IT systems. Plans should reflect the current business needs of the entity and outline: • critical business functions and their supporting IT systems. These should be listed in order of importance • recovery time objectives (RTO) - the timeframes in which the IT systems are to be recovered • recovery point objectives (RPO) - the amount of data which can be lost, measured in time.
Recovery procedures	A description of, or direction to, recovery procedures for: • networks, servers, applications and databases • security systems • data synchronisation within and between applications, including potential procedures to handle a backlog of information • data restoration • handover of services to users.
Communication plan	Plans should outline the method and frequency of communication to key stakeholders such as the public, enforcement authorities and other government departments.
Document control and storage	Plans should include clear approvals, version control and where the plan will be stored.
Testing	Plans need to be tested to ensure they can recover IT systems and will work as expected. They should detail the intended frequency, nature and scope of testing.

Source: OAG based on ISO/IEC 27031:2011[3]

[3] International Organization for Standardization and the International Electrotechnical Commission, *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*, ISO, 2011.

Auditor General's 2023-24 reports

Number	Title	Date tabled
17	Local Government IT Disaster Recovery Planning	31 May 2024
16	Local Government 2022-23 – Information Systems Audit Results	27 May 2024
15	Government Campaign Advertising	15 May 2024
14	State Government 2022-23 – Information Systems Audit	12 April 2024
13	Provision of Supplementary Information to the Standing Committee on Estimates and Financial Operations – Opinions on Ministerial Notifications	5 April 2024
12	Digital Identity and Access Management – Better Practice Guide	28 March 2024
11	Funding for Community Sport and Recreation	21 March 2024
10	State Government 2022-23 – Financial Audit Results	20 December 2023
9	Implementation of the Essential Eight Cyber Security Controls	6 December 2023
8	Electricity Generation and Retail Corporation (Synergy)	8 November 2023
7	Management of the Road Trauma Trust Account	17 October 2023
6	2023 Transparency Report: Major Projects	2 October 2023
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Local Government 2021-22 – Financial Audit Results	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

Office of the Auditor General for Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for Western Australia

11.2 Legal and Compliance

11.2.1 (2024/MINUTE NO 0021) Quarterly Risk Register Update

Executive Chief Executive Officer
Author Risk Advisor
Attachments
1. Risk Matrix ⇩
2. Strategic Risks ⇩
3. Risks Rated Substantial and Higher ⇩

Officer Recommendation/Committee Recommendation
MOVED Cr M Separovich SECONDED Deputy Mayor C Stone
That Council:

(1) RECEIVES the Quarterly Risk Register Update.

CARRIED 5/0

Background

This report provides an update to the Audit, Risk and Compliance Committee (ARC) on the City of Cockburn (the City) risk register for the period May 2024 and June 2024 (the Reporting Period).
A previous report was considered by the ARC on 21 May 2024.

The City's risk register is recorded in RMSS, the City's cloud-based online Enterprise Risk Management (ERM) solution.

This report links to the Corporate Business Plan 2024-28:

Outcome 5	Listening and Leading A community focussed, sustainable, accountable and progressive organisation
Objective 5A	Best practice governance, partnerships and value for money.
Sub-service	Enterprise risk management
Outputs	Provide an enterprise risk management framework Develop City's Business Continuity Framework.

Submission

N/A

Report

Risk Register

The risk level cited in this report to the ARC is the Residual Risk, which is the risk remaining after management has taken action to alter its severity by implementing risk treatment measures.

Table 1 below summarises the changes to the City's risk register during the Reporting Period.

Table 1: Changes to the City's risk register: May 2024 – July 2024

Residual Risk Level	May 2024	July 2024	Change
Low	101	109	+8
Moderate	119	121	+2
Substantial	9	10	+1
High	1	1	0
Extreme	0	0	0
Total	**230**	**241**	+11

The City's ERM policy and framework are aligned with the requirements of the Australian Standard AS ISO 31000:2018 *Risk management-Guidelines* (AS ISO 31000).

One of the pillars of AS ISO 31000 is improvement.

The City's risk register is a dynamic environment and, when identified, new risks are added to the register. Additionally, the risk register is subject to continual review to ensure that the risk information gathered reflects the credibility of the risks.

A review has resulted in the updated rating of this risk:

- RMSS Risk ID 152 *Tree canopy decline* – Decline in the extent of canopy cover across the City as a consequence of poor maintenance or the impacts of pests and disease.
  As a result of the Polyphagous shot-hole borer (PSHB) infestation in trees the level of this risk has increased from a Low 4 to a Substantial 12.

The City's risk register currently contains 11 risks rated Substantial and higher, including one risk rated High - all are operational risks.

The City's highest rank risk is ranked High and is climate change related. The elevated ranking of climate related risks is replicated across Australian local governments, with Disaster, Catastrophic Events and Climate Change and Adaptation ranked in the top 10 risks impacting local government. [JLT Public Sector Risk Report, JLT Risk Solutions Pty Ltd].

Attachment 1 to this report is the current City of Cockburn Risk Matrix.

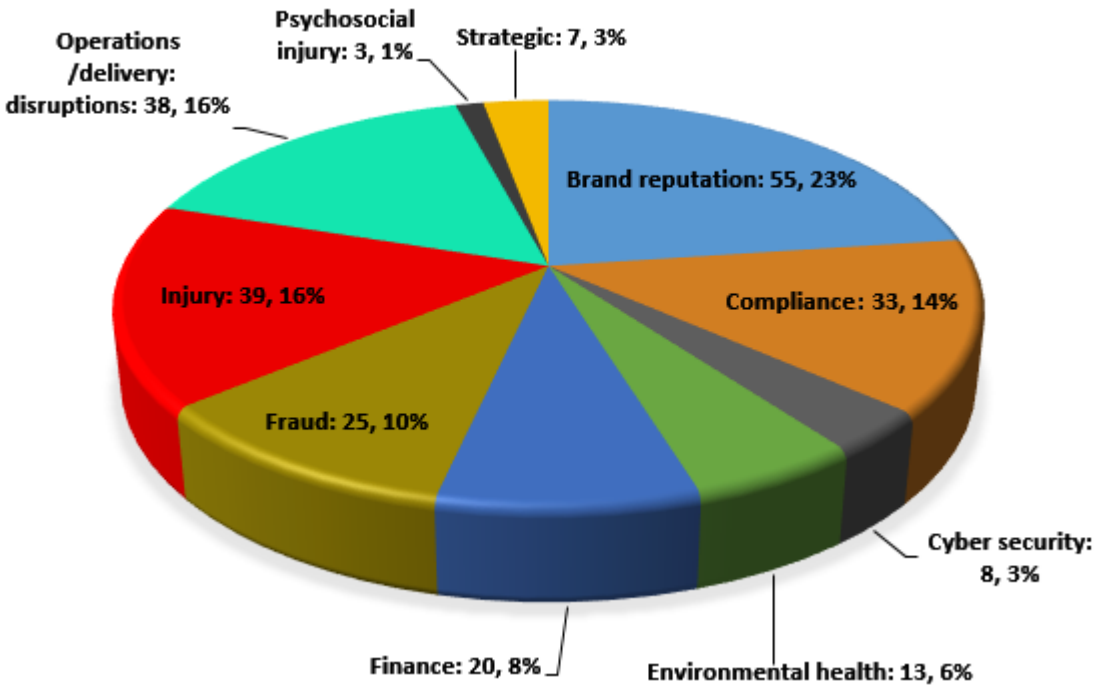
The Risk Assessment Matrix is used for risk analysis and evaluation, comprehending the nature of the risk, and determining the level of risk exposure (likelihood and consequence). It was used for re-evaluating the above risks.

There has been no adjustment to the risk assessment and acceptance criteria since the last report to the ARC.

Risk Register Categories

Figure 1 below illustrates the categories of the open risks in the City's risk register during the Reporting Period.

Figure 1: Total open risks, by category: 27 June 2024



The City's risk register comprises:

- Seven (7) Strategic Risks, whose owners are members of the Executive Leadership Team; and
- 234 Operational Risks, whose owners are Heads of Business / Managers of Service Units.

Risk Register Categories

Figure 2 below is a heat map of the open risks in the City's risk register during the Reporting Period.

Figure 1: Heat map of total open risks: 27 June 2024

		Likelihood				
		Rare 1	**Unlikely 2**	**Possible 3**	**Likely 4**	**Almost Certain 5**
Consequence	**Insignificant 1**	**Low 1 5 Risks**	**Low 2**	**Low 3 1 Risk**	**Low 4**	**Moderate 5**
	Minor 2	**Low 2 9 Risks**	**Low 4 69 Risks**	**Moderate 6 9 Risks**	**Moderate 8 2 Risks**	**Substantial 10 2 Risks**
	Major 3	**Low 3 18 Risks**	**Moderate 6 66 Risks**	**Moderate 9 29 Risks**	**Substantial 12 1 Risk**	**High 15**
	Critical 4	**Low 4 7 Risks**	**Moderate 8 15 Risks**	**Substantial 12 4 Risks**	**High 16**	**Extreme 20**
	Catastrophic 5	**Moderate 5**	**Substantial 10 3 Risks**	**High 15 1 Risk**	**Extreme 20**	**Extreme 25**

The following two attachments provide progress updates to the above risks.

Attachment 2 to this report is the Strategic Risks - Update as of 27 June 2024.

Strategic risks reflect the internal and external forces capable of threatening the City's ability to achieve its strategic objectives or affect its long-term positioning and performance.

This attachment outlines each strategic risk and provides progress and notes on the management of each risk.

There are currently 7 identified strategic risks, all ranked Moderate Risks, and there has been no change in this number the last report to the ARC.

Attachment 3 to this report is the Risks Rated Substantial and Higher - Update as of 27 June 2024.

This attachment outlines each risk rated Substantial and higher and provides progress and notes on the management of each risk.

The City's risk register currently contains 11 risks rated Substantial and higher, including one (1) risk rated High - all are operational risks.

Strategic Plans/Policy Implications

Listening and Leading
A community focused, sustainable, accountable, and progressive organisation.
• Best practice Governance, partnerships and value for money.
• Employer of choice focusing on equity, innovation and technology.

Budget/Financial Implications

N/A

Legal Implications

Local Government (Audit) Regulations 1996 regulation 17 CEO to review certain systems and procedures.

Community Consultation

N/A

Risk Management Implications

Risk management oversight and review is a function of the ARC.

The ARC is required to review the City's Strategic and Operational Risk as part of the City's risk management practices.

The ARCs oversight of the risk register review report supports continuous improvement of risk management processes.

Failure to adopt this report will result in a moderate risk to the City in its ability to support an integrated and effective approach to risk management and continually improve its risk management processes.

Advice to Proponent(s)/Submitters

N/A

Implications of Section 3.18(3) *Local Government Act 1995*

Nil.

City of Cockburn Enterprise Risk Management - risk assessment and acceptance criteria

Risk Assessment Matrix

Consequence / Severity

	Risk Category												Likelihood / Probability				
									Project				Rare 1	Unlikely 2	Possible 3	Likely 4	Almost certain 5
	Brand Reputation	Compliance	Cyber Security	Environmental Health	Finance	Fraud	Injury	Operations / Delivery Disruptions	Quality	Cost	Time	Psychosocial safety	Theoretically such an event is possible but not expected to occur during an operation / asset life / project.	Possible that such an event may occur once during operation / asset life / project.	Such an event may occur more than twice during an operation / asset life / project.	Such events may occur frequently during an operation / asset life / project.	Such events are expected to occur routinely during an operation / asset life / project.
Insignificant 1	Low impact. Low profile. No complaint.	Minor breach of policy / process requiring some response with little impact on other criteria.	Scanning or reconnaissance. Negligible effect on organisation.	An insignificant environmental event that can be immediately corrected under the control of the City.	< $50,000 or < 5% of OP. Little or no impact on asset.	Single opportunistic dishonest activity or asset misappropriation. Internal or external.	Minor first aid.	Little impact. Business as usual. < 5% variation against KPI.	Majority of milestones and objectives being achieved with minor variation to scope and/or quality reported. Minor impact absorbed through project.	< 5% of Project Budget or < $50,000 whichever is lower.	< 5% of Project Timeline or < 30 days, whichever is lower.	Activation of HR, WHS or Mental Health First Aider process.	Low 1	Low 2	Low 3	Low 4	Moderate 5
Minor 2	Low impact. Low profile. Low media attention. Possible complaint.	Compliance breach of policy / process requiring additional work or minimal damage control.	Low-level malicious attack, targeted reconnaissance, phishing, non-sensitive data loss. Causes spurious real time systems slowing for organisation.	A minor environmental event that can be corrected through system improvements within the City.	$50k ≤ to < $250k or 5% ≤ to <10% of OP. Minor loss or damage.	Theft of confidential or personal information, or intellectual property. Repetitive dishonest activity or asset misappropriation. Internal or external.	Medical treatment. No Lost Time Injury (LTI).	Minor impact. Easily dealt with. Still business as usual. 5 ≤ to < 10% variation against KPI.	Minor impact on milestones and objectives being achieved with minor variation to scope and/or quality reported. Disruptive impact on project deliverables expected.	5% ≤ to < 10% of Project Budget or $50k ≤ to < $250k, whichever is lower.	5% ≤ to <10% of Project Timeline or 30 ≤ to < 60 days, whichever is lower.	Unplanned absence of < 2 weeks.	Low 2	Low 4	Moderate 6	Moderate 8	Substantial 10
Major 3	Moderate impact. Moderate media attention. Public complaint.	Compliance breach requiring investigation, mediation or restitution and breach of legislation or regulations.	Malware, beaconing or other active network intrusion; temporary system / service disruption. Loss of confidentiality, integrity, or availability causes limited effect on organisation.	A moderate environmental event that can be remediated but requires multiple stakeholder input.	$250k ≤ and < $1m or 10% ≤ to < 25% of OP. Major damage to asset.	Falsifying financial or procurement records to obtain an improper or financial benefit. Internal or external.	Medical treatment with LTI and / or work restriction > 2 weeks.	Some objectives affected. Can continue business as usual, with minor controls executed. 10 ≤ to < 25% variation against KPI.	Major impact on milestones and objectives being achieved with minor variation to scope and/or quality reported. Serious impact on project deliverables expected.	10% ≤ to < 25% of Project Budget or $250k ≤ to < $1m, whichever is lower.	10% ≤ to < 25% of Project Timeline or 60 ≤ to < 90 days, whichever is lower.	Unplanned absence of > 2 weeks, or Workers' Compensation case.	Low 3	Moderate 6	Moderate 9	Substantial 12	High 15
Critical 4	Damage to reputation. Public embarrassment. High media attention. Several public complaints. Third party legal action.	Compliance breach involving external investigation or third party actions resulting in tangible loss or reputation damage to the City and breach of legislation or regulations.	Exfiltration or deletion / damage of key sensitive data or intellectual property. Loss of confidentiality, integrity, or availability causes some adverse effect on organisation.	A significant environmental event where rehabilitation involves multiple stakeholders and various levels of the community and government.	$1m ≤ and < $5m or 25% ≤ to < 50% of OP. Significant loss of asset.	Persistent planned or systematic dishonest activity or asset misappropriation. Internal or external.	Partial disablement or severe injury, or reportable to WorkSafe.	Some major objectives cannot be achieved. Business can still deliver, but not to expected level. 25 ≤ to < 50% variation against KPI.	Major impact on milestones and objectives being achieved with significant variation to scope and/or quality reported. Critical impact on project deliverables expected.	25% ≤ to < 50% of Project Budget or $1m ≤ to < $5m, whichever is lower.	25% ≤ to < 50% of Project Timeline or 90 ≤ to < 120 days, whichever is lower.	Extended leave from chronic unmanaged work related issues.	Low 4	Moderate 8	Substantial 12	High 16	Extreme 20
Catastrophic 5	Irreversible damage to reputation. Very high level of public embarrassment. Very high media attention. Many public complaints.	Compliance breach involving regulatory investigation and / or third party actions resulting in tangible loss or significant reputation damage to the organisation and breach of legislation or regulations.	Sustained disruption of essential systems and associated services. Loss of confidentiality, integrity or availability causes serious adverse effect on organisation.	A severe environmental event requiring multiple stakeholders, all levels of the community and government to remediate.	≥ $5 million or ≥ 50% of OP. Complete loss of asset.	Irretrievable losses of significant assets or resources through dishonesty, deception or corrupt use of powers causing significant damage to the financial position of the organisation.	Death or permanent disablement.	Most objectives cannot be achieved. Business cannot operate. ≥ 50% variation against KPI.	Catastrophic impact on milestones resulting in the failure to achieve one or more objectives of the project.	≥ 50% of Project Budget or ≥ $5 million, whichever is lower.	≥ 50% of Project Timeline or ≥ 120 days, whichever is lower.	Self-harm. Death. Employee resignation leading to loss of experience and expertise to the organisation.	Moderate 5	Substantial 10	High 15	Extreme 20	Extreme 25

Risk Acceptance Criteria

Risk Level	Criteria	Treatment	Responsibility
Low	Risk acceptable with adequate controls, managed by routine procedures. Subject to annual monitoring or continuous review throughout project lifecycle.	Management through routine operations/project, Risk Registers to be updated.	Head of Business Unit / Manager of Service Unit / Project Manager
Moderate	Risk acceptable with adequate controls, managed by specific procedures. Subject to semi-annual monitoring or continuous review throughout project lifecycle.	Communication and awareness of increasing risk provided to Head of Business Unit / Manager of Service Unit, Risk Registers to be updated.	Head of Business Unit / Manager of Service Unit / Project Manager
Substantial	Accepted with detailed review and assessment. Action Plan prepared and continuous review.	Assess impact of competing Business Unit / Service Unit Projects. Potential redirect of Business Unit / Service Unit resources. Risk registers to be updated.	Director / Steering Committee
High	Risk acceptable with effective controls, managed by Senior Leadership Team Member. Subject to quarterly monitoring or continuous review throughout project lifecycle.	Escalate to CEO, report prepared for Audit, Risk and Compliance Committee (ARC). Quarterly monitoring and review required. Risk Registers to be updated.	Director / Steering Committee / Project Sponsor
Extreme	Risk only acceptable with effective controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring.	Escalate to CEO, report prepared for ARC. Monthly monitoring and review required. Risk Registers to be updated.	CEO / Council / Project Sponsor

Existing Control Ratings

Rating	Foreseeable	Description
Effective	Doing more than what is reasonable under the circumstances.	1. Existing controls exceed current legislated, regulatory and compliance requirements, and surpass relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation; 2. Subject to continuous monitoring and regular testing; and 3. Any control improvements that can be implemented have minimal impact on operations.
Adequate	Doing what is reasonable under the circumstances.	1. Existing controls are in accordance with current legislated, regulatory and compliance requirements, and are aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation; 2. Subject to continuous monitoring and regular testing; and 3. Control improvements may be implemented.
Inadequate	Not doing some or all things reasonable under the circumstances.	1. Existing controls do not provide confidence that they meet current legislated, regulatory and compliance requirements, and may not be aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation; 2. Controls not operating as intended and have not been reviewed and tested; and 3. Existing controls need to be improved.

WHS / Injury / Wellbeing Hierarchy of Control

Effectiveness	Control methodology	Impact on unwanted event (hazard), and examples
100% Effective	Elimination	Remove the hazard, or unwanted event, completely or discontinue the process or practice. *For example, if the electric cable from a stage microphone is a trip hazard, use a wireless microphone instead.*
	Substitution	Replace a hazardous or vulnerable system, material, practice or process with one that presents a lower risk. *For example, if an outdoors event is conducted during a summer day, use of market umbrellas could be substituted by providing marquees or shade sails.*
	Isolation	Use lockable barriers to restrict unauthorised access and separate people from hazard, practice or process. *For example, install guards on machines where there is a risk of a person being trapped in a machine.*
	Engineering	Change the physical characteristics of the practice or process through engineering redesign. *For example, provide ramps if patrons in wheelchairs will be attending an event.*
	Administrative	Establish appropriate policies, practices, procedures, guidelines and operating instructions to control exposures to unwanted events. *For example, if an event requires serving of alcohol, ensure that bar employees have been trained in "Responsible Service of Alcohol".*
≤ 20% Effective	Personal Protective Equipment	Provide appropriate safety equipment. *For example, traffic controllers need to be provided with long sleeves, long trousers, wide brimmed sunhats and high visibility safety vests.*

Increasing Effectiveness

Table 2: Status of Strategic risks

RMSS Risk ID	Risk name	Risk description	Consequence	Likelihood	Residual risk	Risk owner
1	Business continuity and crisis management	Failure to provide business continuity of the City's core services in the event of a major crisis / emergency.	Major 3	Possible 3	Moderate 9	Chief Executive Officer
Progress and Notes 1. The draft document *City of Cockburn Business Continuity Response Plan* has been updated, and has been reviewed by the Legal and Compliance Service Unit. 2. The document will be presented to ELT by August 2024, then presented to the Audit, Risk and Compliance Committee. It is proposed to test this document with a cyber related issue during the second half of the 2023-2024.						
4	Stakeholder relationships	Failure to develop and maintain strategic partnerships and relationships with government agencies and other key stakeholders.	Major 3	Possible 3	Moderate 9	A/Director Corporate and System Services
Progress and Notes 1. Locally relevant Advocacy (through WALGA). 2. External communications and key contacts with Ministers & Local Members. 3. Lobbying communications strategies. 4. Joint Initiatives Zone meeting and National Growth Areas Alliance activities. 5. Direct engagement with a range of State agencies. 6. Limited engagement with targeted Commonwealth agencies.						
5	Built and natural environment	Failure to maintain the City's built and natural environment and resources in a sustainable manner.	Major 3	Possible 3	Moderate 9	Director Planning and Sustainability

RMSS Risk ID	Risk name	Risk description	Consequence	Likelihood	Residual risk	Risk owner
Progress and Notes 1. The City has a number of document and asset management plans that are updated regularly to insure both our buiilt and natural environment are managed in a sustainable manner. These include asset management plans for Buildings, Drainage, Footpaths, Parks and Natural Areas and Road Infrastructure. 2. Other relevant documents include actions which are identified to improve or maintain these assets. These include: Waterwise Council Action Plan, Climate Change Strategy 2020-30 & Natural Area Management Strategy. 3. Service Units such as Facilities Management and Environmental Management are also tasked with ensuring these assets are maintained. 4. Funding is allocated to meet maintenance requirements.						
2	Strategic direction	Lack of clear and aligned strategic vision, direction and implementation.	Critical 4	Unlikely 2	Moderate 8	A/Director Corporate and System Services
Progress and Notes 1. Informing Strategies - A detailed audit of informing strategies is complete, draft strategic framework has been circulated to the administration. 2. Corporate Business Plan - CBP review and development of CBP 2024/25 - 2027/28 is on track for adoption in June. 3. Strategic Community Plan - SCP review scheduled for FY25. 4. Strategy consolidation - Strategy consolidation work is underway and will progress when the final strategic framework is developed during FY26 corporate planning. 5. Business Unit Plans - Rename to Service Plans; 3 yr Service review program is underway. FY25 service plans are on track for adoption in June 2024.						
3	Project management planning	Failure to consistently plan for capital works projects	Critical 4	Unlikely 2	Moderate 8	A/Director Infrastructure Services
Progress and Notes						

RMSS Risk ID	Risk name	Risk description	Consequence	Likelihood	Residual risk	Risk owner
1. Project Management framework and tools are continuing to be implemented. The Investment Prioritization and Optimisation (IPO) process was undertaken for a second FY and is reducing the number of parachute projects, silo approach to project delivery (through centralised delivery) and incomplete project scoping (by assessment of idea scope and proposed budget during the IPO process). 2. Project portfolio management systems, including reporting tools such as EMR and EAM, are being used to monitor project risk, budget and timeframes during delivery. 3. External project management resources continue to be engaged for high value and high risk projects, such as the Cockburn ARC expansion and Malabar BMX Track.						
6	Technology use and change	Failure to identify, manage and capitalise on the effective and efficient use of changing technology.	**Critical 4**	**Unlikely 2**	**Moderate 8**	A/Director Corporate and System Services
Progress and Notes 1. IT Strategy scheduled for development July 2024. 2. Information Classification System is in the process of being developed as part of Privacy and Responsible Information Sharing project. 3. Cyber Security Framework now includes Australian Signals Directorate (ASB) Essential Eight controls, maturity level one is currently being developed and scheduled for December 2024 completion.						
7	Financial sustainability	Erosion of Council's financial sustainability.	**Critical 4**	**Unlikely 2**	**Moderate 8**	A/Director Corporate and System Services
Progress and Notes 1. Annual capital expenditure & operational expenditure budget processes and sign off (at multiple levels, including controllable operational expenditure measures): The City has Enterprise Budgeting process with cascading authorisation. The ELT does final reviews on all projects to determine the final budget. 2. City of Cockburn Long Term Financial Plan 2019-2020 to 2032-2033: LTFP FY25 - FY34 has now been updated and will be adopted at SCM 25 June 2024.						

RMSS Risk ID	Risk name	Risk description	Consequence	Likelihood	Residual risk	Risk owner
15	Landfill capping [Financial risk]	Failure to fund the capping of existing exposed landfill cells.	Catastrophic 5	Unlikely 2	Substantial 10	Head of Operations and Maintenance [ELT Member Director Infrastructure Services]
Progress and Notes 1. Cell 7 capping and leachate pond construction can't safely occur at the same time, whilst keeping the site operational. A decision was made to defer Cell 7 Capping, on the basis that the new leachate pond construction will mitigate any risk of additional leachate being deposited. This information formed part of DWER's decision to allow the City to commence landfilling on Cell 4 & 5 and DWER are comfortable that the construction of the leachate pond will be sufficient to mitigate any risks of excessive leachate generation.						
16	Reduced water availability from decreased rainfall [Compliance risk]	Decreased liveability, reduced water availability, loss of urban vegetation and biodiversity caused by climate change impacts (decreased rainfall).	Minor 2	Almost certain 5	Substantial 10	Head of Sustainability and Environment [ELT Member Director Planning and Sustainability]
Progress and Notes 1. The City's Climate Change Strategy, Public Health Plan, Waterwise Council Action Plan, Natural Area Management Strategy, Bushfire Management Plan and Urban Forest Plan identify a range of actions to address decreased liveability, reduced water availability, loss of urban vegetation and biodiversity caused by climate change impacts (decreased rainfall). 2. A number of business units are tasked with funding and implementing these actions.						
17	Urban forest decline from climate change [Compliance risk]	Urban forest decline caused by climate change impacts (increased temperatures and decreased rainfall).	Minor 2	Almost certain 5	Substantial 10	Head of Sustainability and Environment [ELT Member Director Planning and Sustainability]

11.2.2 (2024/MINUTE NO 0022) Completion of Inquiry Recommendations

Executive Chief Executive Officer
Author Manager Legal and Compliance
Attachments 1. DG Correspondence to COC CEO Completion of Inquiry Recommendations ⇩

Officer Recommendation/Committee Recommendation
MOVED Cr M Separovich SECONDED Deputy Mayor C Stone
That Council:

(1) RECEIVES the acknowledgement of the Completion of Inquiry Recommendations from the Department of Local Government, Sport and Cultural Industries.

CARRIED 5/0

Background

On 14 April 2020, the Director General of the Department of Local Government, Sport and Cultural Industries (the Department) authorised an inquiry into the City of Cockburn (the Inquiry) in accordance with section 8.3(2) of the *Local Government Act 1995*.

Council authorised publication on the City's website of the City of Cockburn Authorised Inquiry Action report for the community to review the City's actions following the inquiry in September 2022.

Since the last update to Council, the City has been working collaboratively with the Department to address matters related to the Inquiry which the Department considered outstanding.

The Departments focus was on the recommendations from the "Cole" Report, and how those recommendations have been addressed by the City.

The completion and endorsement of the Inquiry Recommendations was endorsed by Council on 14 December 2024, noting that some actions are in progress, however considered complete by the City and the Department as the City has committed to delivery.

Submission

N/A

Report

The purpose of this report is for Council, via the Audit, Risk and Compliance Committee, the recent correspondence from the Department acknowledging the completion of the Inquiry Recommendations.

The Inquiry Recommendations

1. The City undergo an independent governance review (with scope approved by the Director General) within three months of this report becoming final and provide the Director General with a copy of the review's findings and report upon its completion.
2. All Elected Members and members of the City's Executive Team undertake training and mediation as determined appropriate by the Director General, within six months of receipt of the final report, to enable them to work as a cohesive and well-governed group in the best interests of the local government.
3. Within six months of receipt of this report, the City's CEO is to deliver a report to the Director General of the Department outlining:
    i. Steps taken in response to the above recommendations
    ii. Identifying the persons who have attended training as set out in recommendation 2 and any reasons given for non- attendance
    iii Any other information considered to be relevant in respect to any further changes the City has made in response to the recommendations and/or information contained within this report.

The City has continued to engage with the Department since the commencement of the Inquiry, informing the Department of the status of delivery and implementation of the recommendations.

On 14 December 2023, Council endorsed the completion and implementation of the Inquiry and Independent Governance Review Recommendations.

The Department have reinforced, through the correspondence that it is important that the City maintains strong governance practices.

The City has recently completed a Governance Review, which will see the adoption of a Governance Improvement Plan, which will support the City on the continued delivery and implementation of improvement of its governance practices.

Strategic Plans/Policy Implications

Listening and Leading
A community focused, sustainable, accountable, and progressive organisation.
• Best practice Governance, partnerships and value for money.
• Employer of choice focusing on equity, innovation and technology.

Budget/Financial Implications

There are no budget implications from the recommendations in this report.

Legal Implications

Section 8.3(1) of the *Local Government Act 1995* (the Act) gives the Director General of the Department of Local Government, Sport, and Cultural Industries (the Department) the authority to inquire into all local governments and their operations and affairs.

The Director General may, by written authorisation, authorise a person to inquire into and report on any aspect of a local government or its operations or affairs.

The Director General of the Department authorised an inquiry into the City (the Inquiry) in accordance with section 8.3(2) of the Act.

Community Consultation

N/A

Risk Management Implications

There is a low risk associated with the recommendation in this report.

The Department have requested that this correspondence by received by Council at the next Ordinary Council Meeting. Council will receive the correspondence via the Audit, Risk and Compliance Committee.

The Completion of the Inquiry Recommendations is a part of the City's governance journey, with the Department acknowledging the City's duty to maintain strong governance practices.

The City is in the process of developing a Governance Improvement Plan, which will continue to support the strengthening of the City's Governance Practices.

Advice to Proponent(s)/Submitters

The Department has been advised this matter will be referred to Council via the Audit, Risk and Compliance Committee.

Implications of Section 3.18(3) *Local Government Act 1995*

Nil.

Department of
Local Government, Sport and Cultural Industries
GOVERNMENT OF WESTERN AUSTRALIA

Our Ref E24005269
Enquiries Suleila Felton, A/Executive Director
Phone (08) 6552 1410
Email Suleila.Felton@dlgsc.wa.gov.au

Mr Daniel Simms
Chief Executive Officer
City of Cockburn
9 Coleville Crescent
SPEARWOOD WA 6163

Dear Mr Simms

via email dsimms@cockburn.wa.gov.au

CITY OF COCKBURN – COMPLETION OF INQUIRY RECOMMENDATIONS

I refer to the City of Cockburn's (the City) recent correspondence in relation to the implementation of the Authorised Inquiry recommendations and completion of the Independent Governance Review (Governance Review) recommendations.

The Department of Local Government, Sport and Cultural Industries (DLGSC) acknowledges:

1. the City's cooperation with DLGSC and the actions it has undertaken to implement the Authorised Inquiry recommendations and complete the Governance Review recommendations;

2. the Audit and Risk Committee's endorsement of the completion and implementation of the Authorised Inquiry and completion of the Governance Review recommendations on 7 December 2023; and

3. that Council considered the Audit and Risk Committee's endorsement and unanimously resolved to endorse the completion and implementation of the Authorised Inquiry and complete the Independent Governance Review recommendations at its Ordinary Council Meeting on 14 December 2023.

It is important the City maintains strong governance practices, and I encourage you, your team and Council to continue focusing on building a strong culture and positive working environment at the City.

If you have any questions regarding this process, please do not hesitate to contact Suleila Felton, A/Executive Director Local Government on the details provided above.

246 Vincent Street Leederville WA 6007
Telephone (08) 9492 9800
Gordon Stephenson House, 140 William Street Perth WA 6000
PO Box 8349 Perth Business Centre WA 6849
Telephone (08) 6552 7300
Email info@dlgsc.wa.gov.au
Web www.dlgsc.wa.gov.au

Additionally, I encourage you to contact DLGSC's Local Government team via email at lghotline@dlgsc.wa.gov.au should the City require any legislative or governance support.

Yours sincerely

Lanie Chopping
DIRECTOR GENERAL

Date 8 June 2024

12. Motions of Which Previous Notice Has Been Given

Nil

13. Notices Of Motion Given At The Meeting For Consideration At Next Meeting

Nil

14. New Business of an Urgent Nature Introduced by Members or Officers

Nil

15. Matters to be Noted for Investigation, Without Debate

Nil

16. Confidential Business

Nil

17. Closure of Meeting

There being no further business, the Presiding Member closed the meeting at 6:31pm.