# NOTICE

of

# CORPORATE GOVERNANCE COMMITTEE MEETING

*Pursuant to the provisions of Section 88(1) of the Local Government Act 1999*

TO BE HELD IN

## COMMITTEE ROOM
## PLAYFORD CIVIC CENTRE
## 10 PLAYFORD BOULEVARD, ELIZABETH

MEMBERS MAY PARTICIPATE BY ELECTRONIC MEANS

ON

**TUESDAY, 4 AUGUST 2026 AT 5:00 PM**

**SAM GREEN**
**CHIEF EXECUTIVE OFFICER**
Issue Date: Thursday, 30 July 2026

## MEMBERSHIP

**MR MARK LABAZ – PRESIDING MEMBER**

Mr Peter Brass
Mayor Glenn Docherty
Cr Shirley Halls
Mr Martin White

# City of Playford
## Corporate Governance Committee Meeting

# AGENDA
### TUESDAY, 4 AUGUST 2026 AT 5:00 PM

## 1 ATTENDANCE RECORD

1.1 Present

1.2 Apologies

1.3 Not Present

## 2 CONFIRMATION OF MINUTES

**RECOMMENDATION**

The Minutes of the Corporate Governance Committee Meeting held 5 May 2026 be confirmed as a true and accurate record of proceedings.

## 3 DECLARATIONS OF INTEREST

## 4 DEPUTATION / REPRESENTATIONS

Nil

## 5 STAFF REPORTS

**Matters to be considered by the Committee Only**

*Matters for Information*



## 6 INFORMAL DISCUSSION



## 7 INFORMAL ACTIONS

## 8 CONFIDENTIAL MATTERS

Nil

## 9 CLOSURE

# STAFF REPORTS

# MATTERS TO BE CONSIDERED BY THE COMMITTEE ONLY

## *Matters for Information*

## 5.1 COMMITTEE SELF-ASSESSMENT (EXTERNAL ASSESSMENT)

**Responsible Executive Manager :** Luke Culhane

**Report Author :** Skye Nitschke

**Delegated Authority :** Matters for Information

### Purpose

To inform the Corporate Governance Committee on the process for conducting the external assessment in accordance with clauses 10.1 and 10.2 of the Corporate Governance Committee Charter.

**STAFF RECOMMENDATION**

The Corporate Governance Committee receives and notes the proposed process for undertaking an external assessment of the Committee's effectiveness.

### Relevance to Strategic Plan

Decision-making filter: We will ensure we meet our legislative requirements and legal obligations.

An externally facilitated review assists in ensuring that the Corporate Governance Committee (the Committee) possesses the skills and attributes required to fulfil its role as Council's audit and risk committee, in accordance with Section 126 of the *Local Government Act 1999*.

### Relevance to Community Engagement Policy

There is no requirement to consult the community on this matter.

### Background

In May 2018, Council endorsed amendments to the Corporate Governance Committee Charter (the Charter) requiring the Committee to undertake an annual self-assessment to evaluate its ongoing role and effectiveness, with any recommendations reported to Council as required.

The Charter also requires that, in the year preceding a Council election, the Committee undertake an external assessment of its effectiveness, with any relevant recommendations provided to Council to assist in informing the ongoing structure and operation of the Committee.

At the time of drafting this report, the next local government periodic election was scheduled for November 2026. Changes to the *Local Government (Elections) Act 1999* passed through the South Australian Parliament on 26 June 2026 amending the timing of the election to April 2027.

A discussion with the Committee's Executive Officer determined to maintain the proposed schedule for the external assessment of the Committee's effectiveness, as required by the Charter, rather than moving it into 2027 at a time when the Council will be significantly busy with not only the election but the Annual Business Plan and Budget development process.

**Current Situation**

In accordance with Council's Procurement Policy and Procedure, and to ensure a fair, value for money and transparent process for selecting a supplier, Council staff will issue a Request for Quote to engage a suitably qualified and/or experienced person to undertake an external assessment of the effectiveness, performance, and structure of the Committee.

The scope of the Request for Quote will include an assessment of:

- Roles and responsibilities as outlined in the Charter, including clarity and understanding of the Committee's role
- Relationship with management and Council
- Flow of information between management, the Committee and Council
- Committee structure, including required knowledge, experience, and adequacy of skill set to fulfil its role and responsibilities
- Individual member perceptions of Committee performance and opportunities for improvement
- Alignment of the Charter with best practice for audit and risk committees of a similar nature
- Relevance and effectiveness of Committee activities and functions
- Conduct of meetings, including frequency, duration and attendance
- Adequacy of information and support provided to the Committee
- Effectiveness in providing advice and recommendations to Council and/or management
- Access to the external auditor

**Future Action**

The anticipated commencement date of procurement activities is 10 August 2026, to be followed by the selection of a preferred supplier.

It is anticipated that the selected supplier will commence the assessment process from 31 August 2026. A draft report will be presented to the Committee on 1 December 2026 for discussion.

The key milestones associated with the process are outlined in the table below.

| | |
|---|---|
| Advertise Request for Quote | 10 August – 21 August 2026 |
| Review responses and select preferred supplier | 24 August – 28 August 2026 |
| Preferred supplier conduct review | 31 August – 30 September 2026 |
| Draft Assessment Report presented to Committee | 1 December 2026 |

## 5.2 DATA GOVERNANCE INTERNAL AUDIT REPORT

**Responsible Executive Manager :** Sam Green

**Report Author :** Ninad Sinkar

**Delegated Authority :** Matters for Information

**Attachments :** 1⇩. Data Governance Framework Internal Audit Report

### Purpose

The purpose of this report is for the Corporate Governance Committee to receive and note the Data Governance Framework Internal Audit Report (Attachment 1).

**STAFF RECOMMENDATION**

The Corporate Governance Committee notes the Data Governance Framework Internal Audit Report (Attachment 1).

### Relevance to Strategic Plan

The City of Playford is committed to delivering efficient services, this includes the efficient management of its risks and effective internal audit function. The implementation of the recommendations will positively impact service delivery to our community through optimum utilisation of resources, greater accountability, transparency, and continuous improvement of our processes.

### Relevance to Community Engagement Policy

There is no requirement to consult the public on this matter.

### Background

As part of the approved Internal Audit Plan, a data governance internal audit was conducted. The objective of this audit was to evaluate the adequacy and effectiveness of the Council's data governance and security framework. This included assessing supporting data governance policies, procedures, controls, and operational practices across Council and through a selected number of systems. This audit was conducted by external consultants, KPMG.

### Current Situation

The detailed observations and recommendations have been included in the Data Governance Framework Internal Audit Report (Attachment 1).

### Future Action

Going forward, all action items will be tracked by the Internal Auditor. The intention is to ensure all actions are undertaken by their due dates or approved amended timelines.

KPMG

# City of Playford Data Governance

## Internal Audit

—

July 2026

# Acknowledgement of Country

**KPMG acknowledges Aboriginal and Torres Strait Islander peoples as the First Peoples of Australia. We pay our respects to Elders past, present, and future as the Traditional Custodians of the land, water and skies of where we work.**

At KPMG, our future is one where all Australians are united by a shared, honest, and complete understanding of our past, present, and future. We are committed to making this future a reality. Our story celebrates and acknowledges that the cultures, histories, rights, and voices of Aboriginal and Torres Strait Islander People are heard, understood, respected, and celebrated.

Australia's First Peoples continue to hold distinctive cultural, spiritual, physical and economical relationships with their land, water and skies. We take our obligations to the land and environments in which we operate seriously.

Guided by our purpose to 'Inspire Confidence. Empower Change', we are committed to placing truth-telling, self-determination and cultural safety at the centre of our approach. Driven by our commitment to achieving this, KPMG has implemented mandatory cultural awareness training for all staff as well as our Indigenous Peoples Policy. This sincere and sustained commitment has led to our 2021-2025 Reconciliation Action Plan being acknowledged by Reconciliation Australia as 'Elevate' – our third RAP to receive this highest level of recognition. We continually push ourselves to be more courageous in our actions particularly in advocating for the Uluru Statement from the Heart.

We look forward to making our contribution towards a new future for Aboriginal and Torres Strait Islander peoples so that they can chart a strong future for themselves, their families and communities. We believe we can achieve much more together than we can apart.

gilimbaa™

In 2013, we commissioned Gilimbaa, a certified Indigenous creative agency, to design an artwork that reflects the diversity of Aboriginal and Torres Strait Islander cultures and KPMG's commitment to reconciliation.

# Contents

# 01

# Executive Summary

# Executive Summary

## Objective

In accordance with the City of Playford's (CoP) FY2026 Internal Audit Plan, a data governance internal audit was conducted to evaluate the adequacy and effectiveness of the CoP's data governance and security framework. This included assessing supporting data governance policies, procedures, controls, and operational practices across Council and through a selected number of systems.

## Scope

To address the overall objective, the scope of this Internal Audit included consideration of the following areas:

- Data Governance Framework: evaluating policies, standards, roles, responsibilities and alignment to better-practice.
- Monitoring, Assurance & Issue Management: incident management, logging, audit trails and escalation processes.
- Information Classification & Handling: data lifecycle, storage, retention, and disposal practices in alignment to state and federal regulations and framework.
- People Capability & Awareness: staff awareness, training, and compliance with governance requirements.

High-level consideration was given to data access, security & controls which included access provisioning, authentication, privileged access and segregation of duties. Our work included giving reference to the recently completed City of Playford User Access Audit.

Please refer to Appendix 4 for the detailed scope and approach.

## Positive Observations

Several positive observations were noted from the CoP's approach to data governance. Key positive observations are outlined:

- **Defined roles and responsibilities for Nightingale users** - Roles and responsibilities within the Nightingale system are documented within the Nightingale Governance document, including defined system roles and responsibilities that support user access and accountability. These roles provide clarity on how users interact with the system and manage information.
- **Onboarding and offboarding controls –** Onboarding and offboarding processes are in place to manage user access, supporting the timely provisioning, modification, and removal of system access. Systems and datasets within scope are generally provisioned through Azure Active Directory, with access typically aligned to user accounts and associated credentials (e.g. email identity), enabling centralised management of user access across platforms.
- **Established information management governance** - CoP has implemented a structured Information Management framework that provides clear guidance on information system(s), disposal arrangements, practices and processes. This establishes a solid foundation to support consistent information management practices across the CoP. While these provide a solid foundation, the consistent application and operational enforcement of these controls varies across systems and business areas.

## Overarching Comments

The review found that the CoP has established a foundation for information management, with documented frameworks and operational processes in place across key datasets and systems such as Nightingale, SharePoint, Outlook, TechOne and GIS. However, these practices are largely focused on managing information and systems rather than governing data as a Council-wide asset. As a result, data-related activities are generally undertaken at a business unit or system level, limiting Council's ability to consistently define ownership, monitor data quality and leverage data effectively.

Across the CoP, data governance practices are generally procedural, system-specific and reliant on individual knowledge, rather than being supported by a coordinated Council-wide approach. This was most evident in the following areas:

- Lack of a defined data strategy, prioritised critical datasets and clear direction for how data supports service delivery, planning and decision-making;
- Absence of an overarching data governance framework that establishes data ownership, data quality and lifecycle management requirements;
- Gaps between policy intent and operational enforcement, particularly in information protection and classification; and
- Limited training and capability development, with training not consistently completed or aligned to data governance responsibilities.

These gaps suggest the CoP is at an early stage of data governance maturity, with key strategic, governance and operational foundations not yet fully established. As a result, Council may experience fragmented improvement efforts, inconsistent reporting, reduced confidence in data and missed opportunities to use data more effectively to support service delivery, planning and decision-making.

# Executive Summary: Summary of Internal Audit Findings

Internal Audit has identified a number of findings, the details of which are noted in the 'Detailed Findings' section of this report. These findings have been individually rated and are summarised as follows:

| Extreme | High | Medium | Low | PIO* |
|---|---|---|---|---|
| - | 2 | 1 | 1 | - |

Through our discussions with key stakeholders, documentation review, walkthroughs and sample testing performed, Internal Audit identified two (2) high, one (1) medium, and one (1) low risk rated finding. The following table provides a summary of our risk rated findings, the relevant issue owner and target date for implementation. These findings and recommendations were discussed with the CoP Management. Management has accepted the findings and has agreed action plans to address these recommendations. The classification of risk ratings in this report are based on the CoP risk ratings documented in Appendix 5.

| Rating | # | Title |
|---|---|---|
| High | F1 | Data is not managed as a strategic asset. |
| High | F2 | Data ownership, quality and lifecycle management are not consistently defined or applied. |
| Medium | F3 | Gaps in the CoP's IM Framework policy coverage, clarity and enforcement. |
| Low | F4 | Gaps in data management training and capability initiatives. |

Note: Management agrees with the above findings. Details on the Management Response and association actions are contained on the 'Management Response and Action(s)' of this Report (page 8).





*Performance Improvement Opportunity*

# Recommendation Horizons

The table below provides a summary of the recommended actions, based on the findings identified during the internal audit. Recommendations have been grouped across three horizons to reflect a logical sequence of activities, beginning with the establishment of foundational governance arrangements before progressing to broader data management and continuous improvement initiatives. The implementation timing of each horizon will be dependent on the CoP's resource capacity and capability, existing commitments and overall priorities for the CoP.

| HORIZON 1 | HORIZON 2 | HORIZON 3 |
|---|---|---|
| 1. Develop and endorse a Data Governance Framework that establishes governance principles, roles, responsibilities and accountability for managing data across the CoP (Recommendation 2.1). | 1. Embed the data governance operating model by defining priority data domains, critical datasets and operating model principles to help further achieve consistent enterprise approach to data management (Recommendation 1.2). | 1. Implement a centralised data issue management process to capture, prioritise, track and resolve data-related issues to support continuous improvement (Recommendation 2.3). |
| 2. Establish a formal data operating model, to provide oversight mechanisms and accountability arrangements to support coordinated decision-making, issue resolution and management of data across the CoP (Recommendation 1.3). | 2. Standardise data control, quality standards, lifecycle requirements, validation controls and performance measures across priority datasets (Recommendation 2.2). | 2. Expand governance, ownership, stewardship and quality management practices across additional datasets and business areas (Recommendation 1.1). |
| 3. Establish a clear data strategy and roadmap for how data will be managed and leveraged as a strategic asset, ensuring initiatives align with the data governance framework (Recommendation 1.1 and 2.1). | 3. Establish a training framework based on data governance roles to build capability in data ownership, stewardship, quality management and lifecycle responsibilities (Recommendation 4.1). | 3. Implement ongoing maturity, monitoring, KPI reporting and continuous improvement activities. This should be flagged as a key data initiative in the data strategy (Recommendation 1.1). |
| 4. Enhance data visibility and definitions for priority datasets to establish a common language and improve consistency across business areas (Recommendation 2.4). | 4. Update the Information Management Framework to better align information management practices with emerging data governance requirements (Recommendation 3.1). | |
| 5. Drive training completion to increase completion rates and strengthen awareness of governance obligations (Recommendation 4.2). | 5. Embed practical security classification, information handling and protection controls within key business processes and across M365 and Outlook (Recommendation 3.2). | |

# Management Response and Action(s)

| Management Response and Action(s) |
| --- |
| Management acknowledges and accepts the findings and recommendations outlined in the Internal Audit Report.<br><br>The recommendations will be incorporated into a broader, coordinated program of work under the oversight of the General Manager Corporate Services. This approach will ensure that related governance, risk and control initiatives are implemented in an integrated and sustainable manner rather than as standalone activities.<br><br>Implementation will be assessed and prioritised alongside other initiatives to ensure appropriate sequencing, resource allocation, and organisational capacity. Having regard to the findings of the report and interdependencies with actions arising from recent internal audits, an implementation timeframe of approximately 12–18 months is considered practical.<br><br>**Responsible:** General Manager, Corporate Services<br>**Date of Completion:** July 2027 – 31 December 2027 |

# 02

# Background

# Background

## Role of data in Local Government

As local government increasingly rely on digital systems, integrated platforms and data-driven processes, data has become fundamental to how councils operate. It underpins a wide range of core functions, including:

- Service delivery and community programs;
- Infrastructure and asset management;
- Financial reporting and regulatory compliance; and
- Customer engagement and service requests.

As these functions become more complex and data-intensive, councils are relying more heavily on data. This is driving an increasing need for more accurate, consistent and readily available information to support both operational and strategic decision-making.

## Context for the CoP

The CoP operates in a high-growth environment, with increasing demand for services, infrastructure and community programs. Strategic planning and operational activities rely on a growing volume of data, including client and service information, asset and infrastructure records, and financial and operational data. These datasets are critical to supporting day-to-day services as well as long-term planning and community outcomes.

As the CoP continues to grow and implement new systems and processes, data is becoming more distributed across platforms and teams. While this presents opportunities to improve service delivery and decision-making, it also increases the risk of inconsistency, duplication, data quality issues and security exposure if governance practices are not clearly defined and applied consistently.

Effective data governance provides the structure needed to manage these risks and support the CoP's objectives. This includes establishing clear accountability for data, defining consistent standards, and embedding controls to ensure data is accurate, secure, reliable and appropriately used throughout its lifecycle. It also ensures that data can be confidently relied upon to support reporting, planning and performance management.

For the CoP, strengthening data governance will be important to support its ongoing growth and ensure that key datasets can be effectively used to deliver services, manage assets and meet community expectations.

## Potential Risks from Poor Data Governance

**Poor Data Quality**

May result in inaccurate, incomplete or inconsistent data, reducing confidence in reporting, decision-making and service delivery.

**Unclear Ownership**

Data assets may not have defined owners or custodians, reducing accountability for data quality, security, maintenance and lifecycle management.

**Compliance and Regulatory Risk**

The absence of formal data governance may increase the risk of inappropriate handling of sensitive information, unauthorised disclosure, data loss, and non-compliance with regulatory obligations.

**Lack of Strategic Direction**

Without a defined data strategy or prioritised critical datasets, Council may struggle to coordinate data-related investment and improvement activities, limiting its ability to realise value from data.

**Siloed Data Processes**

May result in duplicated effort, inconsistent reporting, varying data definitions and classifications, and inefficient processes across business units.

**Absence of Enterprise Data Governance**

Without a formal data governance framework, there is an increased risk of inconsistent data definitions, duplication and reduced data quality across the CoP.

# Background

## Overview of Data Use and Responsibility

The CoP records, uses, and retains data to support its operations, service delivery, and decision-making. This includes a range of information assets created and managed through the conduct of business activities.

Responsibility for managing information is shared across the CoP. The CoP's Information Management Framework recognises that information management is a collective responsibility and requires appropriate controls, accountability and stewardship across business areas.

Effective management of information supports compliance with legislative requirements, enables reliable access to information, and maintains the integrity and protection of the CoP's records.

## Policies and Procedures

The CoP has established an Information Management Framework that provides guidance on the creation, capture, storage, access, and disposal of information. The Framework has been developed to align with legislative requirements, including the State Records Act and associated standards.

This Framework establishes principles such as:

- Treating information as a council asset;
- Assigning custodianship and accountability;
- Applying appropriate controls based on risk; and
- Ensuring information can be accessed and retrieved when required.

While the framework provides a structured approach to managing records and information, it is primarily focused on information management and regulatory compliance. A formal Data Governance Framework to provide a council-wide direction for managing data as a strategic asset has not been established (refer Findings 1 and 2).

As a result, broader data governance elements, such as enterprise-wide data ownership, data quality management and consistent governance roles, are not formalised within a single council-wide framework.

## Systems and datasets reviewed as part of this audit

Four key systems and datasets were identified through consultation with stakeholders and selected as a focus for the Internal Audit. These areas were selected based on their sensitivity, business criticality and value to service delivery and decision-making, and included:

- **Nightingale:** Utilised by the Positive Ageing team and functions as a specialised system for managing sensitive client information. This includes personal data, service delivery records, medical data and support notes. The system also captures information relating to service resources, such as rooms and vehicles. Given the nature of the data managed within Nightingale, it represents a high-sensitivity dataset requiring strong controls around access, data quality and privacy compliance.
- **TechnologyOne (TechOne) Asset Management Module (Asset Register):** Supports the management of assets by maintaining structured records of asset information. This includes asset attributes, ownership details, location, valuation and lifecycle information such as acquisition, maintenance and disposal. As a core system for asset planning and reporting, the quality, completeness and consistency of data within the Asset Register is critical to supporting operational decision-making, financial reporting and long-term asset management.
- **Outlook**: Serves as the CoP's primary email and calendaring platform, supporting day-to-day communication, meeting coordination, and information exchange both internally and with external stakeholders. As a key communication tool, Outlook contains a significant volume of unstructured data, including correspondence, attachments and calendar records, which may include sensitive or operationally important information. This introduces considerations for information classification, retention and appropriate handling.
- **SharePoint:** Utilised as the CoP's primary document management and collaboration platform. It supports the storage, sharing and co-authoring of documents and working files across teams. SharePoint contains a wide range of operational information, including draft documents, project materials and working datasets. As a collaborative environment, it relies heavily on user-driven structure, making consistency in data capture, naming conventions and access management important for ensuring information can be effectively located, governed and reused.

# Background

## Data Governance Controls

Effective data governance relies on strong access controls to ensure that information is accessible only to authorised users, sensitive data is protected from unauthorised modification or disclosure, and accountability for information assets is maintained throughout their lifecycle.

As part of planning this review, KPMG discussed the scope with Council management and agreed that detailed user access control testing would not be duplicated, given the completion of the recent City of Playford Access Controls Audit (January 2026). Management advised that repeating testing in areas already recently reviewed would create unnecessary duplication of assurance activities and relevant recommendations.

Accordingly, KPMG gave reference to the outcomes of the Access Controls Audit and focused this review on broader data governance arrangements, including governance, ownership, accountability, data quality and strategic management of data. The Access Controls Audit assessed controls across key business systems including TechnologyOne, Pathway, Skytrust, Nightingale, Bookable and CommBiz.

The Access Controls Audit included examining user provisioning and deprovisioning, privileged access management, segregation of duties, password controls, periodic access reviews, logging and monitoring, contractor access, third-party access arrangements and security awareness training.

## Access Controls Audit

The Access Controls Audit identified opportunities to strengthen Council-wide governance arrangements through the development of documented access control policies, formalised access review processes, enhanced monitoring of privileged access and improved governance over user access management.

These controls form important foundations for effective data governance and support the consistent management of data across Council's systems and information assets.

## Results of the report and what it means for CoP's data governance

The January 2026 Access Controls Audit identified a number of strengths, including generally effective onboarding and offboarding processes, role-based access provisioning, multi-factor authentication controls, and strong access management practices within several key systems.

However, opportunities were identified to strengthen governance frameworks, formalise access control requirements, improve periodic user access reviews, enhance monitoring of privileged activities, strengthen segregation of duties within selected systems, and improve oversight of contractor and third-party access.

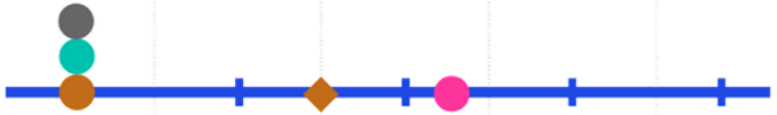
While this Data Governance Review did not re-perform detailed access control testing, the outcomes of the Access Controls Audit are directly relevant to Council's data governance maturity. Access controls are a foundational component of data governance, as they help ensure information is appropriately protected, ownership responsibilities are clear, data quality issues can be identified and addressed, and changes to critical information can be appropriately monitored.

The findings of the Access Controls Audit reinforce several observations identified through this review, particularly the need for clearer governance structures, formalised policies and procedures, defined ownership and accountability, and consistent oversight of Council's information assets. Collectively, implementation of both reviews' recommendations will support improved data integrity, security, stewardship and trust in Council's data.

# Data Governance Maturity Assessment

Current State: The CoP | Council A (2024) | Council B (2024) | Council C (2024) | Target State for the CoP

The graphic below presents the CoP's current data governance maturity as assessed against key elements of the Data Governance Maturity Assessment model. The 'Current State' reflects the CoP's maturity at the time of the Internal Audit and is based on documentation review, stakeholder consultations, process walkthroughs and sample testing performed during the engagement. The assessment provides a point-in-time view of current practices and controls observed across the areas reviewed. Three other South Australian councils of comparable scale and complexity have been included for reference purposes. Refer Appendix A for details of the KPMG Maturity Governance Framework.

| | Low/Initial activity | Initial → Foundational → Established → Developed → Advanced | High/Advanced activity |
|---|---|---|---|
| **Data Ownership and Data Quality**<br>• Assign executive-level owners to key datasets with clear accountability.<br>• Define and monitor data quality standards with regular attestation.<br>• Prioritise enrichment and remediation based on business impact. | There is no formal assignment of data ownership, and data quality issues are unmanaged, undocumented, and reactive. |  | Executive-level data owners are formally assigned, actively engaged, and accountable for maintaining high-quality, trusted data through continuous monitoring and targeted remediation. |
| **Data Attestation and Controls**<br>• Implement controls to trace data lineage and usage context.<br>• Enable management to attest to data origin, quality, and reliability.<br>• Review and embed controls within operational processes. | Data lineage is unclear or non-existent, with no controls in place to support reliable attestation of data origin, usage, or quality. |  | Comprehensive data controls and lineage are embedded across systems, enabling consistent, auditable attestation of data origin, usage, and quality by Management. |
| **Operating Charter**<br>• Formal data governance charter with defined roles and authority.<br>• Run structured meetings with documented decisions and approvals.<br>• Sponsor data programs that support attestation and governance maturity. | No formalised data governance committee, lacking terms of reference, meets irregularly, and has no structured reporting or decision-making processes. |  | The Data Governance Committee operates under terms of reference, with structured meetings, clear decision rights, and active sponsorship of strategic data initiatives. |
| **High-Value Datasets**<br>• Align with business to identify and classify high-value datasets.<br>• Prioritise investment and remediation based on business dependency.<br>• Maintain integrity and availability of critical data assets. | There is no alignment with business teams to identify critical data, resulting in inconsistent prioritisation and underinvestment in key data assets. |  | High-value datasets are systematically identified in partnership with business teams, prioritised for investment, and governed to ensure availability, integrity, and business alignment. |

# 03

# Detailed Findings

# Internal Audit Findings

**High**

## Finding 1 – Data is not managed as a strategic asset

### Observations

The CoP does not have a defined data strategy, which limits its ability to treat data as a strategic asset, prioritise investment and align data initiatives with the CoP's long-term objectives, service delivery requirements and community outcomes.

The CoP has an Information Management (IM) Framework, but it is primarily focused on information and records management, not a data strategy that defines how data supports service delivery, asset planning, regulatory reporting, customer insights or community outcomes. The IM Framework describes itself as a central repository for information management artefacts, governance mechanisms, roles, reporting, systems and procedures, but it does not include a data strategy, data roadmap, prioritised data domains or enterprise data investment pathway.

Data-related activities are occurring across business areas, but without a shared strategic direction guiding how data should be prioritised, integrated or leveraged.

In a local government environment, data plays a central role in service delivery, asset lifecycle planning, financial management and community outcomes. Without a clear direction for how data is managed and used, activities remain operational and fragmented, rather than contributing to coordinated council-wide value.

The review further identified that no formal artefacts or structures exist to support a strategic approach to data. Specifically:

- **Data strategy and roadmap:** No data strategy or documented roadmap was identified to articulate the CoP's strategic intent for data, define priority initiatives or sequence uplift activities to improve data governance and maturity over time.
- **Data domains and prioritised datasets:** No defined data domains or structured approach to identifying critical or high-value datasets was identified. This limits the CoP's ability to understand which data is most important to service delivery and outcomes and to prioritise effort and investment accordingly.
- **Enterprise data investment planning:** No enterprise-wide data investment plan or defined pathway for funding and resourcing data initiatives was identified.
- **Governance and oversight mechanisms:** No formal data governance forum or committee was identified to oversee data-related initiatives, resolve cross-functional data issues or support prioritisation and decision-making across the CoP.

A defined data operating model has not been established to articulate how data responsibilities are structured across the CoP (e.g. centralised/decentralised/federated). In practice, stakeholder consultation and walkthroughs indicated that the CoP has informally adopted a decentralised, business unit driven model, where individual teams manage data independently based on system ownership and operational needs.

However, this model has not been formally defined, governed or supported by enterprise-level structures. This has resulted in inconsistent data management practices across business units, limited coordination of data initiatives, duplication of effort, and challenges in resolving cross-functional data issues or establishing council-wide priorities.

During the review it was identified that Nightingale and Asset Register/GIS are currently being managed through local practices, user guides, operational knowledge and system-specific controls rather than a coordinated council-wide approach. This contributes to limited visibility and coordination of data activities.

### Risk

- Without a defined data strategy, prioritised critical datasets, clear ownership and consistent quality controls, the CoP is more likely to experience fragmented improvement activity, duplicated effort, inconsistent reporting and reduced confidence in the information used to support operational and strategic decisions.
- Strategic and operational decisions may rely on incomplete or low-confidence data, increasing the risk of suboptimal service delivery, planning outcomes and financial decisions.
- Investment in systems and data capability may be misaligned or duplicated, resulting in inefficiencies and increased long-term costs.
- Key data risks, including poor data quality or gaps in reporting, may remain undetected or unmanaged, increasing exposure to operational and compliance issues.
- Opportunities to improve efficiency, service delivery or planning through data are not realised, limiting the CoP's performance.

*(continued on next page)*

# Internal Audit Findings

High

## Finding 1 – Data is not managed as a strategic asset (contd.)

*(continued from previous page)*

**Recommendations**

**1.1 Establish Data Strategy:** The CoP should develop and formally endorse an enterprise data strategy, supported by a multi-year roadmap and aligned investment plan, to define how data will be managed and leveraged as a strategic asset. The strategy should include:

- Articulation of the strategic role of data in supporting the CoP's objectives, service delivery and community outcomes.
- Identification and sequencing of priority data initiatives to uplift data governance and maturity over time.
- Alignment of data initiatives and funding decisions to priorities of the CoP and its community.

**1.2 Define an Enterprise Data Model (Domains, Datasets and Operating Model):** The CoP should establish a structured council-wide approach to managing data by defining key data assets and how responsibilities are organised across the CoP. This should include:

- Definition of data domains aligned to core business functions and services;
- Identification and prioritisation of critical and high-value datasets to focus governance and improvement efforts;
- Development of a formal data operating model (e.g. centralised, decentralised or federated), including clearly defined roles, responsibilities and decision rights (e.g. data owners, stewards and custodians – this should be consistent with Management Actions relating to Finding 2); and.
- Establishment of consistent standards and guidance for managing data across systems and business units.

**1.3 Establish Data Governance Structures and Oversight Mechanisms:** The CoP should implement a formal governance structure to provide oversight, coordination and decision-making for data as a council asset. This should entail establishment (or formal allocation) of a data governance forum or committee with responsibility for overseeing data-related initiatives, prioritisation and issue resolution. This forum/committee should also support the:

- Implementation of processes to manage cross-functional data issues, reduce duplication of effort and improve visibility of data activities;
- Integration of governance activities with the data strategy, roadmap and investment planning processes to ensure alignment and accountability; and
- Introduction of metrics and reporting to monitor data quality, maturity and progress against planned uplift activities.

# Internal Audit Findings

High

## Finding 2 – Data ownership, quality and lifecycle management are not consistently defined or applied

### Observations

While the CoP has established governance arrangements for information and records management, data governance responsibilities are not consistently defined at a dataset level. As a result, ownership, accountability and data quality management practices vary across systems and business areas.

The CoP has established governance through the Information Management (IM) Framework and Information Asset Register, with business stakeholders generally aware of their responsibilities for managing information assets. However, these arrangements primarily support information and records management and do not consistently extend to dataset level accountability.

As a result, key concepts such as dataset ownership, data stewardship, data quality management and lifecycle accountability are not formally defined or consistently applied across systems. This creates a disconnect between ownership of systems and information assets and accountability for the quality, integrity and ongoing management of data.

**Data ownership and accountability**

- The IM Framework has defined information management responsibilities across the CEO, General Managers, Senior Manager Information, Technology and Governance, Information Management Team, Workers and Information Owners. However, these responsibilities are focused on information and records management, and are not consistently translated into dataset level roles including accountability for completeness, accuracy, validation rules, data correction and ongoing data quality monitoring.
- While ownership is established at a system and information asset level, in practice, accountability for data is informal, particularly where datasets span multiple systems or teams. For example:
  - The Asset Register dataset is jointly maintained by the Asset management and Finance teams; however, accountability for data quality, issue resolution, maintenance activities and ongoing stewardship has not been documented.
  - While Nightingale has documented system roles and access controls, accountability for data quality, issue resolution and ongoing dataset stewardship is not formally defined at a dataset level and remains dependent on operational practices and local knowledge.
  - The Nightingale Governance document describes governance roles, system permissions, work instructions and support arrangements, but does not clearly define dataset ownership, data stewardship or accountability for data quality at a dataset level.
- This creates a disconnect between ownership of systems and information assets and accountability for the quality, integrity and ongoing management of data. As a result, data issues are addressed locally and reactively rather than in a coordinated and sustainable way across the CoP.

**Data management guidance**

- Data definitions, standards and business rules are fragmented and inconsistently maintained across systems, limiting Council's ability to apply a consistent approach to data management. While metadata standards are established within the Enterprise Content Management (ECM) environment, these are not consistently applied across other systems and are not subject to regular review.
- While both Nightingale and the TechOne Asset Register module contain references to data definitions within user guides, these vary in terms of content and completeness. For example:
  - Nightingale includes a glossary of terms within its governance documentation, however, guidance on how these definitions are applied in practice is limited.
  - The Asset Register user guide describes asset attributes but functions more as an instructional guide rather than a structured data dictionary.
- Procedural documentation supporting these datasets is inconsistently maintained and lacks standardisation. Testing identified that the Asset Data Maintenance User Guide has not been updated in line with current practices, while supporting documents (e.g. asset creation and training procedures) are informal and maintained as working notes rather than structured, governed documentation. Stakeholder input also confirmed that data entry and maintenance activities are often reliant on individual knowledge and experience.

**Data quality controls and validation**

Data validation and quality controls vary across systems, with no council-wide standard or process for enforcing data quality. Testing identified that system controls do not consistently reflect the criticality of data fields. For example:

- In the Asset Register, data identified as mandatory in upstream processes is not consistently enforced within TechOne. X and Y coordinates are mandatory within the asset handover form but are not mandatory within TechOne, creating a risk of inconsistent asset information. While testing did not identify an error in this field, given the importance of the data, the control is not designed to consistently prevent omission.

*(continued on next page)*

# Internal Audit Findings

High

**Finding 2 – Data ownership, quality and lifecycle management are not consistently defined or applied (contd.)**

*(continued from previous page)*

- In Nightingale, testing identified that a client record created via mail merge captured an address as a PO Box, while the correct residential address was recorded elsewhere in the system and required manual correction. This is inconsistent with the Instructions - New CHSP Client.docx work instruction, which explicitly states that the client address entered in Nightingale should be the address of the client's usual place of residence and not their PO Box.
- Further, in Nightingale, there is limited audit trail functionality, reducing visibility over data changes and the ability to track amendments to client records. This limitation has been raised with the vendor but remains unresolved.

- Data quality issues identified through testing demonstrate that existing controls do not consistently prevent or detect errors. This included inconsistencies in how asset information is recorded across Asset Register modules, including where the project commencement date is not mandatory within Asset Details tab but is required within the Asset Book tab.
- Data processes across both datasets are heavily reliant on manual activities, including data entry, reconciliation, interpretation and validation. These processes are not consistently supported by system-enforced controls, increasing variability and reducing reliability.
- In addition, there is no centralised process to capture and manage data issues across systems, meaning errors identified in datasets such as Nightingale and the Asset Register are not formally tracked, analysed or resolved at a systemic level.

### Risks

- Data inconsistencies within key datasets may impact reporting, operational processes and decision-making, including service delivery and asset management outcomes.
- The absence of clearly defined dataset ownership may reduce accountability for resolving data quality issues and increase the likelihood of recurring errors over time.
- Inconsistent data definitions and lack of standard metadata lead to misinterpretation of data across teams and systems, reducing trust and limiting effective use.
- Reliance on manual processes significantly increases the risk of data entry errors, duplication and inconsistent updates, particularly as data volumes increase.
- Over time, unresolved data quality issues may accumulate across systems, increasing remediation effort and reducing confidence in information used for reporting, planning and operational decision-making.

### Recommendations

**2.1 Develop and Implement a Data Governance Framework:** Develop and implement a Data Governance Framework that establishes key governance pillars (such as data ownership and stewardship, data quality and data controls) to enable better data consistency and accountability. The framework should formally define roles and responsibilities for key datasets, establish governance structures and provide consistent guidance for how data is managed across systems, aligned to the Data Strategy (refer to Finding 1).

**2.2 Standardise Data Controls and Quality:** Introduce a consistent approach to data quality and lifecycle management across priority datasets. This should include strengthening validation rules, implementing mandatory data controls, improving consistency in data capture and leveraging system-based enforcement to reduce reliance on manual processes. In addition, establish defined data standards, lifecycle management practices and data quality KPIs (e.g. percentage of critical fields completed, error rates, timeliness of updates and duplication rates) to support ongoing monitoring and improvement.

*Longer-term initiative dependent on Data Governance Framework implemented:*

**2.3 Introduce Data Issue Management Model:** Establish a centralised data issue management process to capture and track data issues identified within systems. This should support assignment of ownership, root cause analysis and monitoring of recurring issues to drive continuous improvement.

**2.4 Enhance Data Visibility and Definitions:** Develop foundational capabilities such as standardised data definitions and improved visibility of datasets to support consistent interpretation and use of data across the CoP. This will help reduce ambiguity and improve alignment between systems.

# Internal Audit Findings

Medium

## Finding 3 – Gaps in the CoP's IM Framework policy coverage, clarity and enforcement

### Observations

The CoP's IM Framework provides a foundation for records and information management; however, broader data governance requirements have not yet been consistently defined, embedded or monitored across Council systems and datasets. In the absence of a formal data governance framework, there are gaps between the expectations outlined in the IM Framework and how data controls and practices are applied across the CoP.

The CoP has an established IM Framework that provides a strong foundation for managing information. However, stakeholder consultation and sample testing identified instances where policy expectations are not consistently reflected in operational processes, training, monitoring activities or system controls across sampled environments (refer to Finding 4)

In a council environment, policies are most effective when expectations are clearly defined, embedded into training and system controls and actively monitored. Where this alignment does not occur, there is a risk that staff interpret requirements differently and apply controls inconsistently across the council.

Observations noted with respect to the IM Framework are outlined below:

**Security classification and information protection:**

- Security classifications have been assigned to information assets within the Information Asset Register; however, supporting requirements for applying, managing and protecting classified information are not consistently embedded in training, operational processes or system controls.
- Training materials focus on general information types and access controls but provide limited guidance on how to classify information in practice. This is further reflected in the limited implementation of key supporting controls, such as those listed below:
  - Sensitivity labelling has not been enabled within Microsoft Outlook/M365, limiting the CoP's ability to systematically apply and enforce classifications.
  - Secure transmission requirements for sensitive information have not been standardised, such as the use of encryption or password protection for information classified as OFFICIAL: Sensitive.
  - Monitoring and governance of external information sharing are limited, including visibility of files shared externally or uploaded to external cloud platforms.

**Records management and definition of official records**

- While training provides some guidance on identifying what an official record is, this is not defined in the IM Framework itself. Furthermore, delays in training completion (refer to Finding 4) create a period where employees may not fully understand their records management obligations, increasing the risk that official records, such as emails, are not appropriately retained.
- Stakeholder consultations indicate that there is limited monitoring to ensure records are consistently transitioned from collaboration environments (e.g. SharePoint) into the TechOne ECM module, increasing the risk that records are not captured or retained appropriately.

**File structure and information management practices**

- The CoP has developed guidance for standardised file structures and folder hierarchies, however, these standards are not consistently enforced across the CoP.
- For example, testing identified instances where folder structures exceeded prescribed limits (e.g. more than three levels), particularly within operational areas supporting asset-related data.

### Risk

- Sensitive information may be inappropriately classified, handled or shared, increasing the risk of privacy breaches, regulatory non-compliance and reputational damage.
- The absence of enforced classification and secure handling standards increases the likelihood of unauthorised access or disclosure of OFFICIAL: Sensitive information.
- Poor file structure and information management practices reduce the ability to locate, retrieve and manage information efficiently, impacting productivity and increasing operational risk.

*(continued on next page)*

# Internal Audit Findings

Medium

**Finding 3 – Gaps in the CoP's IM Framework policy coverage, clarity and enforcement (contd.)**

*(continued from previous page)*

**Recommendations**

**3.1 Enhance IM Framework:** In consideration of implementation of actions relating to Finding 2, Management may consider updating the IM Framework to provide clearer, more prescriptive guidance across data governance areas, including classification, data handling, lifecycle management and definition of official records. This should ensure expectations are clearly articulated and aligned to operational practices across systems.

**3.2 Embed Security and Handling Controls:** Where feasible, implement system-enforced controls to support policy requirements, including sensitivity labelling within M365, defined standards for secure transmission of sensitive information and clearer guidance on classification and handling practices. This should focus on protecting sensitive data, particularly within high-risk datasets.

# Internal Audit Findings

Low

## Finding 4 – Gaps in data management training and capability initiatives

### Observations

The CoP has established mandatory information management training requirements through its IM Framework, including induction and annual refresher training. However, training completion and capability development are not operating as a consistently controlled process.

The IM Framework establishes that information management training is mandatory for all staff and contractors, including induction training at commencement of employment and annual refresher training. The Framework also specifies that mandatory TechOne ECM training is to be provided to all new starters and that staff should receive training appropriate to their role. While this establishes a baseline understanding of records management and system usage, evidence indicates training is not always completed in a timely manner and is frequently deprioritised due to operational commitments.

Effective data governance requires staff to understand not only how to use systems, but also their responsibilities and accountability for the data they manage. Where this capability is not developed or reinforced, governance practices are inconsistently applied and become dependent on individual experience rather than embedded council-wide behaviour.

Specifically, the following issues were identified:

- The content of the training is largely focused on information management and cyber awareness, with limited emphasis on broader data governance responsibilities such as data ownership, data quality and lifecycle management.
- Analysis of ECM training records identified delays, missed sessions and inconsistent completion. Of the 100 personnel required to complete training, 88 had done so; however, 27 (30.7%) did not complete training at the first available opportunity, and completion timeframes varied significantly, with some staff taking more than 180 days from commencement to completion.
- The training records further show that delays are driven by a combination of delivery issues and operational constraints. Common reasons recorded in the training notes included session cancellations / low attendance, roster or availability constraints, meeting or appointment clashes, operational priorities or work-load pressures.
- The register also identified 6 cases where staff had not completed training prior to leaving the CoP, suggesting that training is not consistently embedded within onboarding, induction or minimum role capability requirements.
- In addition, consultants and casual or contingent workers have not consistently undertaken mandatory training, despite the IM Framework applying to all staff and contractors and requiring ECM training for new starters. Records indicate instances where these groups were marked as "not required" or did not complete training, demonstrating a gap between policy requirements and implementation.
- Although training is mandatory, there are no formal consequences or escalation mechanisms for non-attendance, reducing its overall effectiveness.
- Training is delivered exclusively through in-person sessions, meaning attendance is dependent on staff availability and competing operational priorities. This creates variability in participation and contributes to delays in completion.
- Although data ownership is informally recognised within systems, there is no targeted training provided to individuals responsible for managing data.

### Risk

- Staff responsible for key datasets may lack the knowledge and capability required to maintain data quality and manage issues effectively, leading to errors and inconsistencies.
- Weak understanding of data governance roles and expectations may result in data quality issues remaining unidentified, unresolved or recurring.

### Recommendations

**4.1 Establish Training Framework:** Following implementation of recommendations in connection with Finding 2, develop a structured training and capability approach aligned to data governance responsibilities. This should define expected competencies for staff managing data, including data ownership, quality management and lifecycle responsibilities and provide targeted training for key roles supporting datasets.

**4.2 Enforce Training Completion:** Strengthen the training model by introducing defined completion timeframes, monitoring and escalation mechanisms to ensure mandatory training is completed in a timely manner. Consider expanding delivery methods beyond in-person sessions to improve accessibility and reduce reliance on scheduling availability.

# 04

# Appendices

# Appendix 1: Asset Register

The current Asset Management Register is primarily stored within two systems, being:

- **TechnologyOne Asset Management module:** The CoP's primary asset register used to manage the financial, lifecycle and administrative aspects of assets, including acquisition, valuation, depreciation and disposal.
- **GIS:** The CoP's spatial asset management system used to maintain and visualise the physical location, attributes and mapping information of assets

An Excel-based Asset handover form is used by the Asset Maintenance and GIS team to capture and transfer asset information required for the creation, update or disposal of assets within GIS and TechnologyOne. These systems are impacted by informal data attestation processes and limited system-enforced controls. As a result, there is inconsistent data capture across the datasets, limited standardisation of mandatory fields and an absence of formalised procedures and knowledge management practices to support ongoing maintenance and stewardship of information.

These factors increase reliance on individual knowledge and manual processes, creating a heightened risk of inconsistencies in the way information is recorded, maintained and interpreted across the team. While the CoP is currently developing documentation to formalise key procedures, business rules and knowledge areas, these initiatives remain in progress and have not yet been fully embedded. Consequently, gaps relating to mandatory field requirements, data validation controls and standardised data management practices continue to impact the consistency and reliability of information held within the datasets.

| | *Operations – **Asset register*** |
|---|---|
| **Overview of Dataset** | The GIS & Asset Maintenance team at the CoP currently manages asset data using TechnologyOne asset management module and GIS system before manually transferring the data to TechOne ECM to archive. The dataset held by the team includes handover forms, asset registers, maintenance records and work orders linked to asset servicing. Additionally, the team maintains active project asset documentation, such as Cost Dataset on a SharePoint site. |
| **Positive Finding(s)** | • Assets within the GIS system are assigned a unique numeric code, supporting the consistent identification of assets and reducing the risk of duplicate records.<br>• A validation check of data within the Asset handover form is conducted prior to entering the relevant data to TechnologyOne and GIS system.<br>• A project and process tracker is maintained, with responsibility for activities assigned to designated personnel, supporting accountability and progress monitoring. |
| **Observation(s)** | Data Ownership and Data Quality<br>• Handover forms utilised for the creation and update of asset register entries do not enforce mandatory data fields. While testing did not show any errors, this increases the risk of incomplete or inconsistent information being recorded as it is up to individual knowledge, impacting the quality and reliability of the dataset.<br>• Data quality checks are done informally, and employees currently can enter data themselves if there are missing fields or known knowledge areas. Checks are mainly done in the handover forms, with cross checking done between the tabs within the Excel sheet, not in the asset register system.<br>• The process for registering a new asset or updating a project asset is completed through an Excel-based handover form. This approach relies on manual data entry and lacks formal validation controls to enforce mandatory data requirements prior to submission.<br>• Currently the Asset Management and the Finance team both have ownership of the Asset register, however there is no clear documented delineation of area of responsibility. |
| **Business Implication(s)** | • Mandatory data within the Asset handover form is not enforced as mandatory entry field within TechOne Asset Register.<br>• The same asset is recorded with differing values when compared against other similar entry fields, indicating inconsistencies in asset information and reducing confidence in data accuracy.<br>• The absence of clearly defined ownership may lead to duplicated activities and uncertainty in the allocation of responsibilities across the Asset register. |

# Appendix 1: Nightingale

Nightingale is primarily utilised by the Positive Ageing Team to manage client information and record details relating to assets and activities required by the business unit. The system incorporates user access permissions and data controls to support the security and management of information. However, opportunities exist to strengthen data governance practices, as reporting capabilities within the system are limited and the auditability of changes is constrained. In particular, the system provides limited visibility over modifications to records, reducing the ability to track data changes, monitor data quality, and maintain a comprehensive audit trail. These limitations may impact oversight, reporting, and assurance over the accuracy and completeness of information maintained within the system.

| | *Operations* – **Nightingale** |
|---|---|
| **Overview of Dataset** | The Positive Ageing Team collects, maintains and retains sensitive client and asset information within Nightingale, alongside reports, work instructions, and historical documentation. The volume and sensitivity of this information highlights the importance of robust data governance, information management, and retention practices to ensure information remains accurate, secure, and appropriately managed throughout its lifecycle. |
| **Positive Finding(s)** | • Roles and responsibilities are documented in governance materials and understood in practice, with users aware of their responsibilities.<br>• Access restrictions in place within Nightingale and SharePoint, limiting data access from employees, volunteers, clients and 3rd parties. |
| **Observation(s)** | Data Definitions and Standards<br>• While Nightingale includes a glossary of terms within its governance documentation, there is limited guidance on how these definitions should be consistently applied in practice.<br>• Data definitions and standards are not maintained as authoritative sources and are not formally linked to broader enterprise data governance practices.<br>Data Attestation and Controls<br>• Data quality reviews are primarily undertaken during reporting activities, with limited ongoing validation of client records throughout the year.<br>• Changes to records within Nightingale do not require a formal approval or review process, increasing the risk of unauthorised, inaccurate or unreported updates.<br>• Testing identified limited audit trail functionality within Nightingale, reducing visibility over data amendments and the ability to monitor changes to client information.<br>Data Quality Management<br>• Data quality activities are heavily reliant on manual data entry, user judgement and local knowledge rather than system-enforced controls.<br>• Formal training for key system functions is not consistently established, increasing the risk of inconsistent data entry practices between users.<br>• Testing identified instances where client information required manual correction, demonstrating that existing controls do not consistently prevent or detect data quality issues.<br>Ownership and Accountability<br>• While stakeholders are generally aware of their operational responsibilities within Nightingale, ownership of data quality, integrity and ongoing maintenance activities is not formally defined.<br>• There is no centralised process for recording, monitoring and resolving data quality issues, limiting visibility over recurring errors and opportunities for continuous improvement.<br>• Data management activities remain heavily reliant on individual knowledge and experience, increasing key-person dependency and reducing consistency in processes. |
| **Business Implication(s)** | • Inaccurate data being stored within each data system due to the manual process required to move information across.<br>• Inability to assign work may cause duplications in work-load as the business unit expands.<br>• Without a formal procedure when checking personnel when information is collected for retention or updates, this can cause unauthorised changes to client information and miss information to be entered within Nightingale.<br>• Incomplete ownership of work processes such as the lack of an approval before data is updated, can cause misinformation, duplicated and unreported changes to information within Nightingale. |

# Appendix 1: SharePoint & Outlook

Outlook and SharePoint are Microsoft tools used by the wider council to manage email communications and store/archive documents. Both system are managed by the IT team, who manage back-end architecture and access controls, and by the information management team, who supports the IT team with managing the information within the systems. Similarly with other findings, the two systems are impacted by informal data attestation processes and limited system-enforced controls. These gaps increase the risk of inappropriate data access, data leakage, and non-compliant information handling practices as reliance is placed on user adherence rather than consistently enforced system controls.

The CoP has implemented several security measures to strengthen its control environment, including role-based access controls, geo-blocking, preliminary email screening, multifactor authentication, and automated reporting of suspected malicious link activity. While these measures provide an important foundation for protecting information assets, the continued growth of the Council and the increasing volume of data collected and retained will require further enhancements to governance processes and control mechanisms. Addressing the identified gaps will help support ongoing compliance obligations and strengthen the protection of sensitive information.

| | *Operations* – **Outlook & SharePoint** |
|---|---|
| **Overview of Dataset** | Outlook is used by the CoP to support communication, calendar management, meeting coordination, and contact management across business units. SharePoint serves as the primary repository for active documents and working drafts, storing a broad range of CoP information including asset registers, forms, policies, procedures, and reports. While Outlook is primarily used for communication and scheduling, it also contains critical and non-critical information and document copies that are retained through email correspondence, attachments and within the deleted items folder |
| **Observation(s)** | Data Attestation and Controls<br>• Attachments and files stored in mailboxes, deleted items folders and SharePoint folders are not subject to automated retention controls or regular review, increasing the volume of information retained.<br>• There is no mandated or standardised approach for classifying information across the CoP. Sensitivity labels are not consistently applied within SharePoint, and controls to enforce classification of Outlook attachments have not been implemented.<br>• Requirements for encrypting or password-protecting sensitive information during transmission have not been formally defined.<br>• The CoP has not established a consistent mailbox size standard or monitoring process, limiting the ability to oversee and manage mailbox growth.<br>• Structure guidelines are not consistently followed, resulting in variations in information management practices across business areas. Such as the 3-4 deep folder structure guideline within SharePoint.<br>• The absence of controls to identify, block, and report the transfer of sensitive or large files reduces visibility over data movement and increases the risk of inappropriate or unauthorised handling of information.<br>• There is no automated process or integration between Outlook and SharePoint to TechOne ECM. Additional TechOne add-ons are required to enable automation between the two systems and TechOne ECM. |
| **Business Implication(s)** | • Increased risk of data breach or unauthorised access and edit of sensitive data.<br>• Inability to protect data from being downloaded or transferred to unauthorised personnel.<br>• Data and records are not consistently stored within the TechOne ECM module and may be retained longer than required, reducing oversight of information lifecycle management.<br>• Inability to enforce classifications on documents throughout Outlook and SharePoint. |

# Appendix 2: Data Governance Maturity Assessment Model

The maturity model below is derived from KPMG's Data Governance Maturity Model and has been tailored to the domains in scope for this internal audit.

| | Initial | Foundational | Established | Developed | Advanced |
|---|---|---|---|---|---|
| **Data Ownership and Data Quality** | There is no formal assignment of data ownership, and data quality issues are unmanaged, undocumented, and reactive. | Data owners are informally identified for some datasets. Limited data quality checks exist but are inconsistent and not standardised. | Data ownership is formally assigned for key datasets. Data quality standards are defined, and periodic monitoring is performed. | Data owners are accountable at a functional level. Data quality is actively monitored with defined metrics, and remediation is prioritised based on impact. | Executive-level data owners are formally assigned, actively engaged, and accountable for maintaining high-quality, trusted data through continuous monitoring and targeted remediation. |
| **Data Attestation and Control** | Data lineage is unclear or non-existent, with no controls in place to support reliable attestation of data origin, usage, or quality. | Basic controls exist for some systems, but lineage and traceability are incomplete. Attestation is informal or manual. | Data lineage is documented for key datasets. Controls are implemented to support data accuracy, and attestation processes exist. | Data controls are embedded into operational processes. Management regularly attests to data quality, origin, and usage using defined evidence. | Comprehensive data controls and lineage are embedded across systems, enabling consistent, auditable attestation of data origin, usage, and quality by Management. |
| **Operating Charter (Governance Structure)** | No formalised data governance committee, lacking terms of reference, meets irregularly, and has no structured reporting or decision-making processes. | Informal governance forums exist but lack clear roles, accountability, or regular cadence. | A formal data governance structure is defined, including roles and responsibilities. Meetings occur regularly with documented outcomes. | Governance forums are active and effective. Decisions are structured, and governance supports business priorities and initiatives. | The Data Governance Committee operates under terms of reference, with structured meetings, clear decision rights, and active sponsorship of strategic data initiatives. |
| **High-Value Datasets** | There is no alignment with business teams to identify critical data, resulting in inconsistent prioritisation and underinvestment in key data assets. | Some high-value datasets are recognised, but there is no formal classification or prioritisation framework. | High-value datasets are identified and documented. There is alignment with business priorities for investment and management. | High-value datasets are prioritised based on business impact. Controls ensure availability, integrity, and appropriate use. | High-value datasets are systematically identified in partnership with business teams, prioritised for investment, and governed to ensure availability, integrity, and business alignment. |

# Appendix 3: KPMG Data Governance Framework


**KPMG's Data Governance Framework was used to assess the current pains and blockers for the CoP around data governance and build a roadmap aligned to the CoP' data ambition.**

Data Governance refers to the suite of technology and processes that ensure data is of the right context, accuracy, timeliness and completeness to expose the right insight which directs the stakeholder towards the right action.

Adopting and building a roadmap to implement a data governance framework is key to improving the management of data and analysis within an organisation. Each organisation will have varying degrees of maturity as a starting point with unique priorities, so there is no one-size-fits-all for implementation of a Data Governance Framework.

As an organisation's maturity increases, the key benefit achieved is the improved realisation of value from data. This benefit will manifest in several ways, including:

- Reduced cost to maintain;
- Improved quality and trust;
- Better yield on investment; and
- More efficient operations.

Data governance is as much about operational culture as it is about technology.

# Appendix 4: Scope

| | |
|---|---|
| **Objective** | The objective of this Internal Audit was to assess the adequacy and effectiveness of the CoP's (the Council) data governance and data security framework, including the supporting policies, procedures, controls, and practices established to manage, protect, and govern data across the CoP. The audit assessed the implementation and operation of data governance and security controls across a sample of Council systems selected to provide a representative view of practices across different service areas, with a limited number of systems subject to detailed testing to evaluate the practical application of Council-wide data governance arrangements. |
| **Scope** | This review considered the Council's processes, practices, and systems relating to data governance and data security, with a focus on the following areas:<br>**Data governance framework:**<br>• Existence, adequacy, and currency of data governance policies, standards, procedures, and guidance.<br>• Defined roles and responsibilities for data ownership and accountability.<br>• Alignment of the framework to support informed decision-making, data quality, and risk management.<br>**Monitoring, assurance, and issue management:**<br>• Processes for monitoring data integrity, security incidents, and anomalous activity.<br>• Logging, audit trails, and reporting mechanisms for data access, changes, and usage.<br>• Escalation, investigation, and resolution of data-related issues and breaches.<br>**Information classification and handling:**<br>• Existence and application of an information classification framework.<br>• Data handling, storage, retention, and disposal practices.<br>• Alignment with legislative, regulatory, and better-practice requirements.<br>**People capability and awareness**<br>• Staff awareness of data governance and data security obligations.<br>• Training programs supporting compliance with relevant policies and procedures.<br>**Data access, security, and controls:**<br>• Consistency of authorisation, authentication, and access controls applied to data within the selected systems.<br>• Appropriateness of user access provisioning, modification, and removal processes.<br>• Segregation of duties and management of privileged access.<br>Our work over the above areas included giving reference to the recently completed City of Playford User Access Audit, so as to not duplicate other recent Internal Audit work.<br><br>**Out of Scope – Unless specifically identified during fieldwork, the following areas were excluded from the scope of the review:**<br>• Detailed penetration testing or technical vulnerability assessments.<br>• Review of all Council systems (testing was limited to selected systems).<br>• Assessment of third party service providers beyond Council-controlled governance and oversight arrangements. |

# Appendix 4: Scope

| | |
|---|---|
| **Approach** | The scope of this engagement included the following:<br>• A desktop review of relevant documentation, including policies, procedures, and guidelines relating to data governance methodologies and processes.<br>• Five (5) consultations with key stakeholders to obtain an understanding of the relevant data governance processes.<br>• Sample testing of key priority systems to assess the effectiveness of data governance processes, adherence to policies, access and usage practices, and lessons learned.<br>• Walkthroughs of relevant processes, systems, and controls to assess the extent to which current practices aligned with better-practice.<br>• A high-level gap analysis of the City of Playford's (CoP) current framework and processes against KPMG's Data Governance Framework.<br>• Reporting, including the identification of performance improvement opportunities and better-practice insights relating to the data governance framework.<br>• Discussion of findings with Management and the subsequent issuance of a draft Internal Audit Report for feedback and finalisation. |

# Appendix 5: Ratings Classifications

The following framework for internal audit ratings has been developed and agreed with CoP Management for prioritising internal audit findings according to their relative significance depending on their impact. The individual internal audit findings contained in reports will be discussed and rated with CoP Management.

### Risk Matrix

| | | Consequence | | | | | |
|---|---|---|---|---|---|---|---|
| **Level** | **Descriptor** | **Financial Sustainability** | **Regulatory Compliance** | **Reputation** | **Work Health & Safety** | **Service Delivery** | **Environmental Impact** |
| **1** | Insignificant | Negligible financial loss/impact; no material disruption to business | Isolated non-compliance breach: Dispute that can be resolved without legal remedy | No media/political attention; local complaints; no social media commentary | Negligible injury; first aid treatment. No impact on staff morale. No lost work time | Interruption to a function with no noticeable impact to customers | Negligible environmental damage that could be reversed immediately |
| **2** | Minor | Minor financial loss/impact; no material disruption to business; variation to budget can be managed within current financial year | Contained non-compliance or breach; statutory authority makes enquiries; may require involvement of legal firms | Localised community concern; some local media/political attention, unlikely adverse; minimal social media commentary, with no substance | Injury requiring short term medical intervention. Minimal impact on staff morale. Minimal or no lost work time | Interruption to a critical function with minimal impact to customers or short term loss of a non-critical function | Minor instances of environmental damage that could be reversed |
| **3** | Moderate | Moderate financial loss/impact; material impact on program or business operations; impact on budget beyond current financial year | Material breach; forma investigation by statutory authority; fines or penalties; require involvement of legal firms | Public interest; potential for adverse local media or political attention; some social media commentary with substance | Injury requiring hospitalisation. Short term impact on staff morale. Some lost work time. | Interruption to a critical function with some impact to customers or loss of multiple non-critical functions. May require activation of Continuity Management Team | Major loss of environmental amenity and a danger of continuing environmental damage |

# Appendix 5: Ratings Classifications

| Consequence | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Level** | **Descriptor** | **Financial Sustainability** | **Regulatory Compliance** | **Reputation** | **Work Health & Safety** | **Service Delivery** | **Environmental Impact** |
| **4** | Major | Major financial loss/impact; major impact on program or business operations; budget recovery over multiple financial years | Major breach formal investigation by statutory authority; prosecution or litigation; require involvement of legal firms | High levels of public interest; state-wide media attention; potential for long term effect on reputation of Council; major social media commentary | Injury requiring major medical treatment. Long term major impact on staff morale. Lost work time for an extended period | Complete loss of a critical function with extended impact to customers. Requires activation of Continuity Management Team | Major loss of environmental amenity and a danger of continuing environmental damage |
| **5** | Catastrophic | Significant financial loss/impact loss of program; external intervention required to recover | Significant breach, gross negligence; formal investigation by statutory authority prosecution, significant fines and penalties; imprisonment of workers, class actions; require involvement of legal firms | Extensive public outcry; potential national media attention; prolonged media/political attention; potential for irreparable damage to reputation with community and other agencies; widespread negative social media commentary | Injury resulting in permanent disablement or death. Long-term significant impact on staff moral | Complete loss of multiple critical functions for an extended period. Requires activation of Continuity Management Team | Significant widespread loss of environmental amenity and progressive irrecoverable environmental damage |

# Appendix 5: Ratings Classifications

**Risk Matrix**

| Consequence | Insignificant | Minor | Moderate | Major | Catastrophic |
|---|---|---|---|---|---|
| Likelihood | 1 | 2 | 3 | 4 | 5 |
| Almost Certain 5 | Low 5 | Medium 10 | High 15 | Extreme 20 | Extreme 25 |
| Likely 4 | Low 4 | Medium 8 | High 12 | High 16 | Extreme 20 |
| Possible 3 | Low 3 | Medium 6 | Medium 9 | High 12 | High 15 |
| Unlikely 2 | Low 2 | Low 4 | Medium 6 | Medium 8 | Medium 10 |
| Rare 1 | Low 1 | Low 2 | Low 3 | Low 4 | Low 5 |

**Likelihood Table**

| Likelihood | | |
|---|---|---|
| Level | Descriptor | Description |
| 1 | Rare | Only ever occurs under exceptional circumstances |
| 2 | Unlikely | Conceivable but not likely to occur under normal operations |
| 3 | Possible | Not generally expected to occur but may under specific circumstances |
| 4 | Likely | Expected to occur at some stage under normal operations |
| 5 | Almost Certain | Expected to occur most times during normal operations |

# Appendix 6: Stakeholders Consulted

Listed below is the list of stakeholders consulted as part of this internal audit.

| # | Name | Position |
|---|---|---|
| 1 | Luke Culhane | General Manager – Corporate Services |
| 2 | Bao Tram | Senior Manager – Information Technology |
| 3 | Mathew Pilcher | Manager – Asset Management |
| 4 | Georgia Proctor | Manager – Positive Ageing |
| 5 | Skye O'Flaherty | Manager – Information Management |
| 6 | Dimity Burgess | Manager – ICT Service Solutions |
| 7 | Nicole Mahoney | Senior GIS and Asset Data Analyst |
| 8 | Dennis Okiror | Information Management Partner |
| 9 | Nathaniel Walter | ICT Service Delivery Coordinator |
| 10 | Abdoulaye Barry | ICT Technical Specialist |
| 11 | Ninad Sinkar | Internal Auditor |

# Disclaimers

**Inherent Limitations**
This report has been prepared as outlined with The City of Playford in the Scope Section of the engagement letter/contract dated 15 April 2026. The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and, consequently no opinions or conclusions intended to convey assurance have been expressed.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, The City of Playford stakeholders consulted as part of the process.

Unless specifically prohibited by you under our Engagement terms, AI may have been used to support the drafting of this document. Where AI has been used, this document, including any outputs generated by AI, has undergone human review by the engagement team in accordance with KPMG's AI Policy and Trusted AI Framework. For any questions regarding our use of AI, please contact Heather Martens.

No reliance should be placed by The City of Playford on additional oral remarks provided during the presentation, unless these are confirmed in writing by KPMG.

KPMG have indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report.

KPMG is under no obligation in any circumstance to update this report in either oral or written form, for events occurring after the report has been issued in final form.

**Reference to 'Review' and 'Audit'**
Reference to 'Review' and 'Audit' throughout this report has not been used in the context of a review in accordance with assurance and other standards issued by the Australian Auditing and Assurance Standards Board.

**Third Party Reliance**
This report is solely for the purpose set out in the Scope Section and for the City of Playford information, and is not to be used for any purpose not contemplated in the engagement letter/contract or to be distributed to any third party without KPMG's prior written consent.

This report has been prepared at the request of the City of Playford in accordance with the terms of KPMG's engagement letter/contract dated 15 April 2026. Other than our responsibility to the City of Playford, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

**Electronic Distribution of Report**
This KPMG report was produced solely for the use and benefit of City of Playford and cannot be relied on or distributed, in whole or in part, in any format by any other party. The report is dated July 2026 and KPMG accepts no liability for and has not undertaken work in respect of any event subsequent to that date which may affect the report.

Any redistribution of this report requires the prior written approval of KPMG and in any event is to be complete and unaltered version of the report and accompanied only by such other materials as KPMG may agree.

Responsibility for the security of any electronic distribution of this report remains the responsibility of City of Playford and KPMG accepts no liability if the report is or has been altered in any way by any person.

KPMG

# Contact us

**Heather Martens**
**Director**
T: +61 431 586 324
E: hmartens@kpmg.com.au

**Viraj Pawar**
**Director**
T: +61 3 9288 6435
E: vpawar3@kpmg.com.au

**KPMG.com.au**

## 5.3 CORPORATE GOVERNANCE COMMITTEE WORK PLAN

**Responsible Executive Manager :** Luke Culhane

**Report Author :** Skye Nitschke

**Delegated Authority :** Matters for Information

**Attachments :** 1⇩. Corporate Governance Committee Work Plan 2026

### Purpose

The purpose of this report is for the Corporate Governance Committee (the Committee) to review and monitor the Corporate Governance Committee's Work Plan (the Work Plan) and ensure it is meeting the obligations set out in the *Local Government Act 1999*.

**STAFF RECOMMENDATION**

The Committee notes the Corporate Governance Committee Work Plan 2026 (Attachment 1).

### Relevance to Strategic Plan

Decision-making filter: We will ensure we meet out legislative requirements and legal obligations.

The Committee is established in accordance with Section 126 of the *Local Government Act 1999* (the Act). The Charter sets out how the Committee fulfils its legislative obligations, while the Work Plan (Attachment 1) is the planning tool to ensure that these responsibilities are met.

### Relevance to Community Engagement Policy

There is no requirement to consult the community on this matter.

### Background

The Committee was established at the commencement of the 2022 Council term to fulfil Council's obligation under Section 126 of the Act, to maintain an audit and risk committee. The Committee's purpose is to provide independent assurance and advice to Council on matters relating to accounting, financial management, internal controls, risk management and governance.

### Current Situation

The Work Plan (Attachment 1) has been developed to ensure the Committee's business is appropriately planned on an annual basis and that its obligations under the Act and Charter are met. The Work Plan is reviewed at each meeting and updated as required.

**Future Action**

The Committee will receive a report on the Work Plan (Attachment 1) at each Committee meeting.

| Corporate Governance Committee Work Plan 2026 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| AGENDA | CGC Charter Reference | Report Type | Non-recurrent/ Recurrent | Meeting Dates | | | | | |
| | | | | 3 Feb 2026 | 7 Apr 2026 | 5 May 2026 | 4 Aug 2026 | 6 Oct 2026 | 1 Dec 2026 |
| **POLICY REVIEW** | | | | | | | | | |
| Consider relevant Policies for CGC input (as needs basis) | 2.6 Accounting, Internal Control, Reporting and other Financial Management Systems | Decision Report | N | | | | | | |
| **FINANCIAL MANAGEMENT** | | | | | | | | | |
| External Audit: | | | | | | | | | |
| Annual External Audit Plan | 2.5 Council's External Auditor | Information Report | R | External Auditor attend | | | | | |
| Management Update on Internal Control Findings (External Audit Interim Report) | 2.3 Monitor Auditor Recommendations | Information Report | R | | | | | | |
| Adoption of Annual Financial Statements & External Audit Report | 2.1 Financial Reporting and 2.5 Council's External Auditor | Decision Report | R | | | | | External Auditor attend | |
| Meeting with External Auditor | 2.5 Council's External Auditor | Informal Discussion (Committee Only) | R | | | | | External Auditor attend | |
| Review of External Auditor performance | 2.5 Council's External Auditor | Information Report | R | | | | | | |
| Budget Reviews | 2.1 Financial Reporting | Information Report | R | Mid-year review | | | | Budget Review One | |
| Rates Review (as needs basis) | 2.1 Financial Reporting | Decision Report / Information Session | N | | | | | | |
| Rolling Asset Revaluation Update | 2.1 Financial Reporting | Information Report | R | | | | | | |
| **RISK MANAGEMENT** | | | | | | | | | |
| Strategic Risk Report | 2.8 Risk Management | Information Report | R | | | | | | |
| Risk and WHS Audit Action Plans - Progress Update | 2.8 Risk Management | Information Report | R | | | | | | |
| Insurance Portfolio | 2.8 Risk Management | Information Report | R | | | | | | |
| Major Project Update (as needs basis) | 2.8 Risk Management | Information Report | N | | | | | | |
| Disaster Recovery Plan (as needs basis) | 2.8 Risk Management | Information Report | N | | | | | | |
| Business Continuity Plan (as needs basis) | 2.8 Risk Management | Information Report | N | | | | | | |
| **INTERNAL AUDIT** | | | | | | | | | |
| Internal Audit Work Plan | 2.7 Internal Audit Function | Information Report | R | | | | | | |
| Internal Audit Finding Reports (as needs basis) | 2.3 Monitor Auditor Recommendations | Information Report | N | | | | | | |
| Internal Audit Status Update (as needs basis) | 2.3 Monitor Auditor Recommendations | Information Report | N | | | | | | |
| **STRATEGIC MANAGEMENT PLANS** | | | | | | | | | |
| LTFP Update and Assumptions | 2.2 Strategic Management Plans and Annual Business Plans | Informal Discussion | R | | | | | | |
| Update on ABP, LTFP, SAMP | 2.2 Strategic Management Plans and Annual Business Plans | Informal Discussion | R | | | | | | |
| **PRUDENTIAL REPORTS** | | | | | | | | | |
| Prudential Reports (as needs basis) | 2.9 Prudential Reports | Decision Report / Informal Discussion | N | | | | | | |
| **PUBLIC INTEREST DISCLOSURES** | | | | | | | | | |
| Public Interest Disclosures (as needs basis) | 2.10 Public Interest Disclosures | Information Report | N | | | | | | |
| **OTHER INVESTIGATIONS OR EVALUATIONS** | | | | | | | | | |
| Other Investigations (Section 130A) (as needs basis) | 2.4 Other Investigations or Evaluations | Decision Report | N | | | | | | |
| **COMMITTEE GOVERNANCE** | | | | | | | | | |
| Workplan & Schedule of Meetings | 4. Delegations | Decision Report | R | | | | | | |
| CGC Communique | 11. Reporting and Review | Informal Discussion | R | | | | | | |
| Appointment of Presiding Member | 4. Delegations | Decision Report | R | | | | | | |
| Committee Self Assessment (external assessment - year of election) and Annual Report | 11. Reporting and Review | Decision Report | R | | | | External assessment | Findings | |
| CEO update | | Information Report | R | | | | | | |
| Training and Development (Finance, Risk and Standards update) (as needs basis) | 9. Independent Member Support | | N | | | | | | |

# INFORMAL DISCUSSION

## 6.1 Content for the Corporate Governance Committee Communique

**Presenter:** Luke Culhane, General Manager Corporate Services

**Purpose:** For the Committee to provide input into the Corporate Governance Committee Communique for the August 2026 meeting.

**Duration:** 5 Minutes

Section 126(8)(a) of the *Local Government Act 1999* states the audit and risk committee of a Council must provide a report to the Council after each meeting summarising the work of the Committee during the period preceding the meeting and the outcomes of this meeting.