



Information Classification and Management Review – Future State Report

Sunshine Coast Council

DECEMBER 2022

Document control

Report details:	
Title:	Information Classification and Management Review – Future State Report
Author(s):	Senior Consultant, GWI
Reviewer:	Associate Director, GWI
Status:	Final
Release by:	Chief Executive Officer, GWI Managing Partner, GWI
Client:	Sunshine Coast Council
Client contact:	Acting Coordinator CEO Governance & Operations, Sunshine Coast Council
Synopsis:	Future state information classification processes and recommendations to uplift Council's related capabilities.
Disclaimer:	In preparing this report we have relied on information and material supplied by you, the client, and do not take responsibility for the accuracy of the information and material provided to us. This document was originally delivered to Council under a commercial in confidence agreement.

Revision details	Date of issue	Version number
Draft version	07 OCT 2022	1.0
Draft version – Initial feedback incorporated	28 OCT 2022	2.0
Final version	1 NOV 2022	3.0
Steering Committee feedback incorporated	14 DEC 2022	4.0
Final public release version	20 DEC 2022	5.0

Executive summary

Sunshine Coast Council (Council) must manage the use, disclosure, and release of its information in accordance with its legislative and regulatory obligations, as well as best practice. However, to provide transparency about its operations and to meet community expectations, Council seeks to balance these obligations with the proactive publication of Council information. To understand Council's current environment, GWI conducted an independent review of the classification and management of Council's information. The current state report findings indicate that, while Council understands its challenges relating to information security classification and the management of confidential Council meeting information, a lack of foundational information management practices is preventing capability uplift. Council is addressing these challenges through its Inform Program; however, specific requirements exist for the development of documented processes for information security classification, as well as information governance roles and responsibilities, to enable and support classification. Improved classification practices will also underpin Council's ability to uplift transparency and accountability through the appropriate management and release of information to the public.

To address these requirements, this document sets out a practical approach that is aligned to best practice information classification and protection and is based on requirements in the Queensland Government Enterprise Architecture (QGEA) frameworks, policies, and guidelines, specifically the Queensland Government Information Security Classification Framework (QGISCF). Adopting and implementing this approach will enable Council to make improved decisions about the management and release of its information and to comply with its legislative and regulatory obligations.

To inform the development of an information security classification approach and recommendations, GWI has:

- Adopted Council's Information Security Policy principles to ensure alignment between the policy and the approach for classifying information
- Reviewed the QGISCF
- Reviewed current state report findings
- Reviewed the Inform Program's scope and progress.

The table below outlines the high-level steps of the classification process.

Phase	Classification process steps
Plan	Define process for Business Impact Level (BIL) assessments.
Plan	Review and approve BIL assessment process via governance group.
Do	Identify information asset and add it to Council's Information Asset Register (IAR).
Do	Conduct BIL assessment for the information asset and capture results in IAR.
Do	Assess security classification of information asset and add details to the IAR.
Do	Apply information security classification labels to records.
Check / Act	Conduct quality assurance across IAR and source systems.

The information classification process is reliant on the implementation of the recommendations provided in this report. Below is a summary of the recommendations. Recommendations marked with an asterisk (*) are recommendations that have a direct relationship with the initiatives covered by Council's Inform Program. Refer to Appendix B for more information.

#	Recommendation
1	Improve how Council communicates its processes and efforts to make Council meeting information available to the public.
2	Update and operationalise Council's Information Access and Management Policy.*
3	Update and operationalise Council's Custodianship Policy.*
4	Review scope and logical order of training modules and formalise a plan for modules' completion.*
5	Operationalise the recently developed Administrative Access & Right to Information Policy and Guideline.
6	Ensure information systems that are source of truth for Council's records and information have up-to-date information security classification labels.

Table of Contents

1	Introduction	1
1.1	Purpose and audience	1
1.2	Background.....	1
1.3	Objective	2
1.4	Scope	2
1.5	Approach	2
1.6	Related documents.....	2
2	Information classification approach.....	3
2.1	Information security classification principles	3
2.2	Information security classification process.....	3
2.2.1	High-level business process	4
2.2.2	Detailed description of process.....	4
3	Recommendations	6
	Appendix A Client documents reviewed	9
	Appendix B Recommendations and the Inform Program	10
	Appendix C Recommendations and pain points addressed	11
	Appendix D Glossary	13

List of figures

Figure 1: Approach to development of future state process and recommendations.....	2
Figure 2: Information security classification principles.....	3
Figure 3: High-level information security classification process	4

List of tables

Table 1: Related documents	2
Table 2: Detailed description of information security classification process	5
Table 3: Future state recommendations.....	8
Table 4: Client documents reviewed.....	9
Table 5: Recommendations and the Inform Program.....	10
Table 6: Information Security Classification recommendations and pain points addressed.....	12
Table 7: Council meetings information practices recommendations and pain points addressed.....	12
Table 8: Glossary of terms	13

1 Introduction

Sunshine Coast Council is actively working to uplift its information management practices and capabilities and has established the Inform Program to address recommendations arising from the following external reports:

- Recordkeeping and Information Management Maturity Assessment (GWI)
- Best practice alignment for Information Sharing (GWI)
- Compliance audit report – Sunshine Coast Regional Council (Office of the Information Commissioner).

As part of the Inform Program's Information & Records Management (I&RM) Standard initiative, an independent review of Council's information classification and management was conducted to inform the development and implementation of a best practice information management and access approach for the sensitivity of information held by Council.

GWI's current state assessment of Council's information classification practices identified key pain points relating to the:

- Definition and embedding of information governance roles and responsibilities, particularly in relation to information release processes.
- Currency of the Information Access and Management Policy and the lack of underlying processes that support its operationalisation.
- Capability of key systems, such as Content Manager (EDDIE) and Microsoft 365, for information security classification.
- Lack of community awareness of Council's current efforts to make information available to the public, particularly in relation to Council meeting information.

1.1 Purpose and audience

The purpose of this report is to support the improvement of Council's understanding and application of information classification and to define a practical approach that is aligned to best practice classification and protection. This will enable Council to make improved decisions about the management and release of its information and to comply with its legislative and regulatory obligations.

This report is intended to be used by the Information Classification and Management Review Steering Committee and should be read in conjunction with the SCC Information Classification and Management Review Current State Report.

1.2 Background

Council's existing Information Access and Management Policy sets out information classifications that are outdated and inconsistent with the current Queensland Government Information Security Classification Framework (QGISCF). In addition, there are no supporting processes or training available for staff to enable the appropriate classification of Council information.

As a result, Council is unable to fully operationalise its Information Security Policy, leading to non-compliance with legislative and regulatory requirements. Without the ability to appropriately classify information, Council is unable to make informed and timely decisions about which information assets are appropriate for release to the public via administrative access or RTI processes. In addition, while Council manages its meetings' information in accordance with section 254J of the *Local Government Regulation 2012* (Qld), it seeks to improve its practices around informing the community of its mechanisms for making information available to the public.

1.3 Objective

This report's objective is to provide Council with a future state information classification approach including:

- A best practice and fit-for-purpose process for the application of security classification to Council's information.
- A set of recommendations to enable the implementation of the process across Council and to uplift community perception of Council's commitment to transparency and the proactive publication of information.

1.4 Scope

This future state report focuses on the process for the classification and management of Council information in line with the QGISCF. The report includes recommendations that relate to:

- Updating and operationalising key policies and guidelines which directly support Council's information classification processes.
- Ensuring systems are updated accordingly to enable alignment with policies.
- Improving the community's perception of Council's efforts to operate in a spirit of openness and accountability in alignment with the RTI Act.

1.5 Approach

Figure 1 outlines the approach undertaken to conduct the future state assessment.

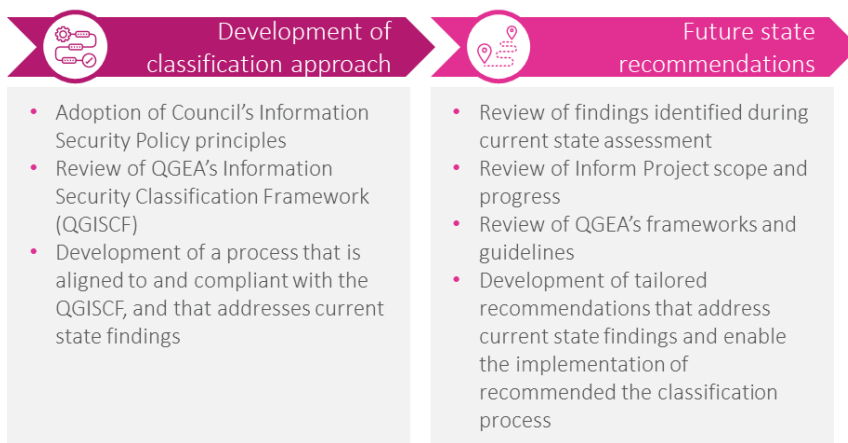


Figure 1: Approach to development of future state process and recommendations

1.6 Related documents

The following documents were used to inform the development of this report:

Document	Produced by	Year
Identification and Classification of Information Assets	QGEA	2016
Information Security Assurance and Classification Guideline	QGEA	2018
Queensland Government Information Security Classification Framework	QGEA	2018
SCC Inform Program Exec Presentation_D2022 773006 ELTS Draft Presentation	Sunshine Coast Council	2022
SCC IT Governance Structure [D2022 281073]	Sunshine Coast Council	2022

Table 1: Related documents

2 Information classification approach

According to the QGEA, applying consistent security classifications to information assets supports government agencies in making informed and timely decisions about how they should capture, store, maintain, transmit, process, use, and share information to best deliver services to the community.

The fit-for-purpose process developed for Council is based on and compliant with the QGISCF. It incorporates steps that reflect Council's ongoing and planned initiatives as outlined in the Inform Program roadmap.

2.1 Information security classification principles

The principles from Council's Information Security Policy apply to information and information security classification:




 <p>Principle 1 Confidentiality</p>	Protection against unauthorised access, disclosure or modification of information assets.
 <p>Principle 2 Integrity</p>	Protection against the unauthorised or accidental modification or manipulation of information assets.
 <p>Principle 3 Availability</p>	Information assets are reliably accessible and available to authorised users and protected against unauthorised or accidental disablement or destruction.

Figure 2: Information security classification principles

2.2 Information security classification process

The current state assessment identified two key pain points that are negatively impacting Council's ability to apply security classifications to its information:

- The lack of a formalised and operationalised Business Impact Level (BIL) assessment process¹.
- The lack of appropriate information management training currently provided to Council staff, including in relation to information security classification.

The BIL assessment process identifies the business impact from a loss of confidentiality, availability, and integrity of Council's information. The assessment ranks the impact levels as either low, medium, or high. The rankings are then used to determine the appropriate security controls that should be implemented to safeguard Council's information. Appropriate information management training will empower staff to use and manage information across its entire lifecycle in compliance with legislative and regulatory obligations, as well as Council's policies and procedures, and mitigates the risk of Council information being inadvertently released or inappropriately used.

The information security classification process outlined below is reliant on the implementation of the recommendations provided in this report (refer to section 3. Recommendations) which include the development of a process for BIL assessments and the review of planned information management training modules.

¹ [Queensland Government Information Security Classification Framework](#)

2.2.1 High-level business process

Figure 3 provides a high-level overview of the information security classification steps and the actors involved in the process. Section 2.2.2 provides a detailed description of the process.

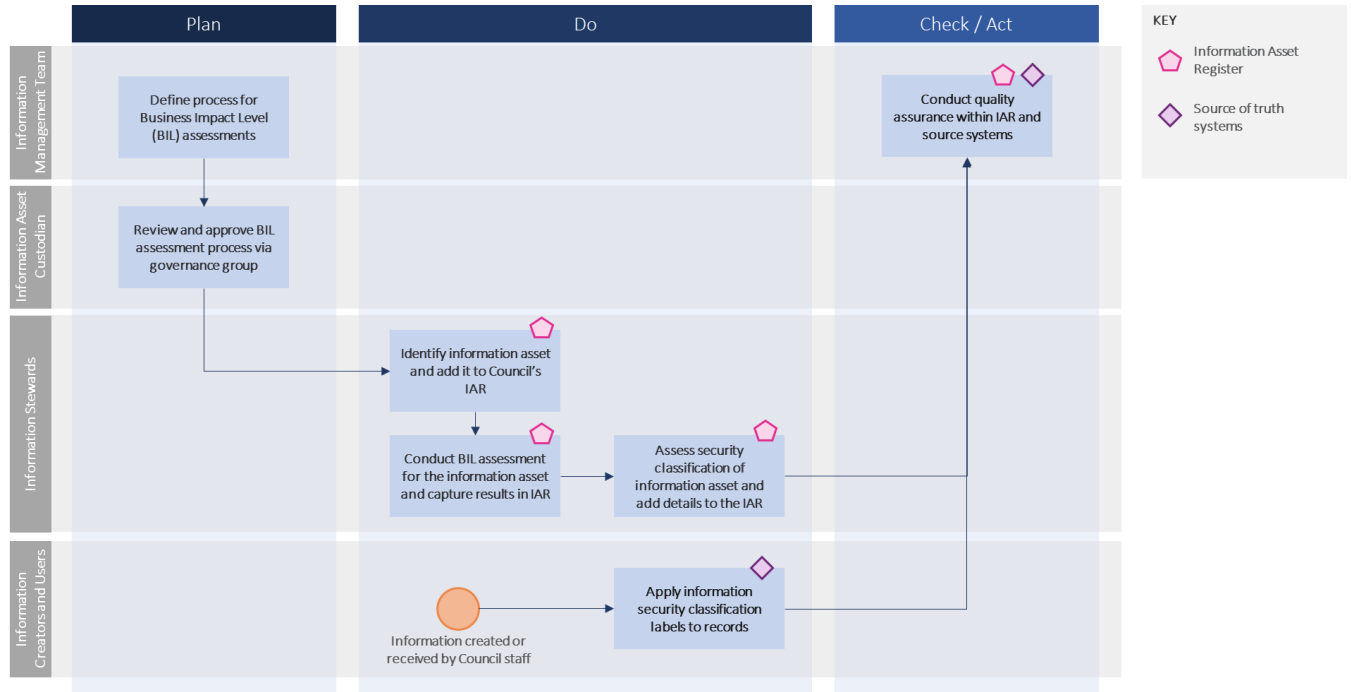


Figure 3: High-level information security classification process

2.2.2 Detailed description of process

Table 2 provides a detailed description of the steps in the information security classification process.

Classification process steps	Description
Define process for Business Impact Level (BIL) assessments	<p>Responsible: Information Management Team</p> <ul style="list-style-type: none"> Define and capture Council’s BIL assessment process (within a guideline or procedure document), including the security controls to be applied based on the outcome of a BIL assessment. Send the assessment process to Information Asset Custodians via governance group for review and approval. Conduct periodical reviews of the security controls to ensure they are appropriate and in line with legislative and regulatory requirements.
Review and approve BIL assessment process via governance group	<p>Responsible: Information Asset Custodians via governance group</p> <ul style="list-style-type: none"> Review the BIL assessment process to ensure the identified business impacts from the loss of confidentiality, availability, and integrity are accurate and in line with Council’s risk tolerance levels. Make the guideline/procedure available to Information Stewards to guide them in assessing business impact levels and applying security classifications to information assets within Council’s Information Asset Register (IAR).
Identify information assets and add to Council’s Information Asset Register (IAR)	<p>Responsible: Information Stewards</p>

Classification process steps	Description
	<ul style="list-style-type: none"> Identify information assets that pertain to a specific function. This can be accomplished by filling out a form such as QGEA's Information Asset Identification and Classification Form². Add the identified information asset to Council's IAR and capture metadata appropriately.
Conduct BIL assessment for the information asset and capture results in IAR	<p>Responsible: Information Stewards</p> <ul style="list-style-type: none"> Conduct BIL assessments for information assets identified using the approved process. Capture the assessment results for levels of confidentiality, integrity, and availability within Council's IAR.
Assess security classification of information asset and add details to the IAR	<p>Responsible: Information Stewards</p> <ul style="list-style-type: none"> Capture information assets security classification within Council's IAR.
Apply information security classification to records	<p>Responsible: Information Creators and Users</p> <ul style="list-style-type: none"> Within source of truth systems apply the appropriate security classification to records being created and used. <p>Responsible: Information Asset Stewards or delegated officers</p> <ul style="list-style-type: none"> Monitor and ensure that information assets under their responsibility are labelled and secured appropriately.
Conduct quality assurance across IAR and source systems	<p>Responsible: Information Management Team</p> <ul style="list-style-type: none"> Conduct periodical quality assurance across IAR to identify completeness and accuracy of metadata captured. Conduct periodical quality assurance across source systems to identify if records and information are being assigned the appropriate security classification. Ensure inconsistencies are raised with the relevant Information Asset Custodian for remediation.

Table 2: Detailed description of information security classification process

² Information Asset Identification and Classification Form

3 Recommendations

In response to GWI's current state assessment of Council's information classification practices, the below recommendations have been developed, taking into consideration:

- Council's current information management maturity levels
- Ongoing and planned initiatives within the Inform Program
- Requirements under QGEA frameworks and guidelines.

The implementation of these recommendations is necessary to enable the operationalisation of the information classification process outlined in the previous section of this report.

Recommendations marked with an asterisk (*) are recommendations that have a direct relationship with the initiatives covered by Council's Inform Program. Refer to Appendix B for information about which streams of work the recommendation relates to.

#	Recommendation	Description	Why it is important
1	Improve how Council communicates its processes and efforts to make Council meeting information available to the public	<ul style="list-style-type: none"> • Create a page on Council's website that is dedicated to outlining: <ul style="list-style-type: none"> – Council decision-making processes – Reasons for a Council meeting to be closed – The types of Council meeting information that will be considered confidential in accordance with <i>Local Government Regulation 2012</i> (Qld) – Which information from Council meetings will be immediately available to the public – How and when Council meeting information will be available to the public if that information is classified as confidential under <i>Local Government Regulation 2012 s 254J</i>. • Create a register on Council's website to: <ul style="list-style-type: none"> – Inform the community of information that has been classified as confidential, including the reason for the required confidentiality (aligned to s 254J of the <i>Local Government Regulation 2012</i>) and predicted review/release date. – Provide the community with links to Council meeting reports that are no longer classified as confidential. • Develop a communications plan to ensure the community is aware of how Council is ensuring transparency by improving publication of 	<ul style="list-style-type: none"> • Improves community perception of Council's commitment to operate in a spirit of openness and accountability in alignment with the RTI Act. • Improves information findability on the Council website.

#	Recommendation	Description	Why it is important
		<p>its practices around the management of confidential meeting information.</p> <ul style="list-style-type: none"> Reassess community perceptions (within 6 months after the implementation of changes to the website) by sending the same survey form <i>“Information Classification and Management at Sunshine Council”</i> to the same recipients to identify the impacts of the changes made. 	
2	Update and operationalise Council’s Information Access and Management Policy*	<ul style="list-style-type: none"> Update the Information Access and Management Policy to ensure it is aligned with the latest version of the QGISCF. Develop a supporting process for the application of security classification to Council’s information assets. Create a process for conducting and capturing Business Impact Level (BIL) assessments across Council’s information assets. Define security controls for the different possible BIL assessment outcomes which are commensurate with the assessed security levels (e.g., more robust controls should be applied to information assessed as having a higher business impact level). Ensure records are labelled appropriately (where functionality exists) within source of truth systems by implementing the approach outlined in this report. Ensure security controls are consistently applied to information assets as per the developed BIL assessment process. 	<ul style="list-style-type: none"> Ensures compliance with the QGISCF. Improves compliance with legislative and regulatory requirements. Ensures information assets are appropriately secured. Reduces risks and impacts for Council from the loss, compromise, or misuse of information.
3	Update and operationalise Council’s Custodianship Policy*	<ul style="list-style-type: none"> Update the Information Custodianship Policy to ensure it is aligned with the latest version of QGEA’s Information Asset Custodianship Policy (IS44). Develop information governance framework, including the establishment of an Information Governance Committee or Group. Define information governance roles and responsibilities, including for the approval of publication of Council’s information and data (e.g., administrative access). Identify appropriate stakeholders to fill the necessary roles and onboard them to ensure they are aware of their responsibilities. Identify, register, and classify Council’s outstanding information assets in Council’s Information Asset Register (IAR)*. 	<ul style="list-style-type: none"> Formalises information asset processes and highlights information assets’ relevance to departmental services. Enables Council to establish accountability for information and data release decisions and approvals. Ensures Council’s information assets are managed appropriately throughout their lifecycle. Reduces the risk of inadvertent release of information that is incorrect or out-of-date.

#	Recommendation	Description	Why it is important
4	Review scope and logical order of training modules, and formalise a plan for modules' completion*	<ul style="list-style-type: none"> Review the scope of planned training modules to ensure they cover topics necessary for the implementation of this report's recommendations, including: <ul style="list-style-type: none"> Information security classification Information custodianship roles and responsibilities Administrative access and RTI requests. Review the logical order for the development and completion of information management-related training modules. Formalise a plan for the completion of modules by staff and ensure completion is monitored. 	<ul style="list-style-type: none"> Ensures training modules cover the information necessary for staff to confidently comply with and implement Council's policies and procedures. Ensures the development and suggested completion by staff follows a logical order (e.g., Information Security Classification module should be completed before Information Sharing module). Fosters an information management and recordkeeping culture across Council.
5	Operationalise the recently developed Administrative Access & Right to Information Policy and Guideline	<ul style="list-style-type: none"> Develop a process for the identification of what type of information can be classified as "Public". Develop a process for the release of information classified as "Public". 	<ul style="list-style-type: none"> Improves compliance with the RTI Act and IP Act which require government agencies to proactively disclose information unless there is a good reason not to. Reduces the number of RTI requests and subsequently reduce costs associated with the administration of requests. Establishes clear mechanisms and processes for the release of information to the public.
6	Ensure information systems that are the source of truth for Council's records and information have up-to-date information security classification labels	<ul style="list-style-type: none"> Update information security classification labels within EDDIE to ensure they are aligned with QGISCF's current labels. Review the current use of and need for existing caveats within the EDDIE system to allow for the classification process to be streamlined. Enable sensitivity labelling functionality within Microsoft 365 apps to allow for information to be appropriately classified in the source system. Assess possibility of re-establishing InfoCouncil and EDDIE integration to reduce manual effort requirement. 	<ul style="list-style-type: none"> Enables the consistent application of appropriate security controls to information stored in Council's source systems. Ensures compliance with legislative and regulatory requirements. Ensures compliance with the QGISCF. Reduces the risk of inadvertent release of sensitive or protected information. Reduces risks and impacts for Council from the loss, compromise, or misuse of information. Reduces costs from the manual transfer of information between InfoCouncil and EDDIE.

Table 3: Future state recommendations

Appendix A Client documents reviewed

Document	Owner	Last review
Administrative Access & Right to Information Organisational Policy	Sunshine Coast Council	2021
Administrative Access & Right to Information Organisational Guidelines	Sunshine Coast Council	Not available
Compliance Audit Report – Sunshine Council Regional Council	Office of the Information Commissioner	2021
Information Access and Management Policy	Sunshine Coast Council	2018
Information Classification and Management at Sunshine Coast Council Survey Results	Sunshine Coast Council	2022
Information Security Guidelines	Sunshine Coast Council	2022
Information Security Policy	Sunshine Coast Council	2020
SCC Inform Program Exec Presentation_D2022 773006 ELTS Draft Presentation	Sunshine Coast Council	2022
SCC IT Governance Structure [D2022 281073]	Sunshine Coast Council	2022

Table 4: Client documents reviewed

Appendix B Recommendations and the Inform Program

Recommendation	Inform Program initiative	Intent and scope
2. Update and operationalise Council's Information Access and Management Policy*	Implement I&RM Standards	<ul style="list-style-type: none"> Promote and provide advice and guidance on how records management relates to our business activities, decisions, legal obligations, and corporate responsibilities.
3. Update and operationalise Council's Custodianship Policy*	OIC Response Privacy Assessments and Information Asset Register	<ul style="list-style-type: none"> Design, develop, and implement an Information Asset Register containing all information assets held by SCC. Produce a public facing version of the Information Asset Register demonstrating information assets held by council, their purpose, and how these are used (Office of the Information Commissioner requirement).
4. Review scope and logical order of training modules, and formalise a plan for modules' completion*	Skills & Training	<ul style="list-style-type: none"> Design high quality learning materials that support the Inform Program and specifically information and records management changes. Reduce dependence on face-to-face learning and cost of delivery by using PeopleHub delivery using Articulate courseware. Provide proof of learning delivery and competency through the learning management system.

Table 5: Recommendations and the Inform Program

Appendix C Recommendations and pain points addressed

Table 6 outlines pain points and recommendations relating to information security classification processes (refer to section 2.3 of the Current State Report). Table 7 outlines pain points and recommendations relating to Council meetings information practices (refer to section 2.5 of the Current State Report).

Category	Pain points (from current state assessment)	Recommendations
People	Application of Council's Information Access and Management Policy and Information Security Policy is limited.	<p>2 Update and operationalise Council's Information Access and Management Policy</p> <p>4 Review scope and logical order of training modules, and formalise a plan for modules' completion</p>
	Staff do not know who to go to for support in relation to information related queries.	3 Update and operationalise Council's Custodianship Policy
	Limited training is provided to staff in relation to information management.	4 Review scope and logical order of training modules, and formalise a plan for modules' completion
	Not all users understand the process for classifying information within Council's Content Manager system (EDDIE).	4 Review scope and logical order of training modules, and formalise a plan for modules' completion
	Roles and responsibilities for approving the publication and/or release of information are not formalised or embedded.	3 Update and operationalise Council's Custodianship Policy
	Responsibility for Council's policy management is not formalised.	(Being addressed by the adoption of an e-Policy Suite (Policy-Management-as-a-Service))
Process	Most council information is not being classified due to the lack of formalised processes.	<p>2 Update and operationalise Council's Information Access and Management Policy</p> <p>4 Review scope and logical order of training modules, and formalise a plan for modules' completion</p>
	Council's Information Access and Management Policy is out of date.	2 Update and operationalise Council's Information Access and Management Policy
	Council's Information Custodianship Policy is out of date.	3 Update and operationalise Council's Custodianship Policy
	No formalised process for conducting Business Impact Level (BIL) assessments.	2 Update and operationalise Council's Information Access and Management Policy

	There is no formalised process to operationalise the recently developed Administrative Access & Right to Information Policy and Guideline.	4 Review scope and logical order of training modules, and formalise a plan for modules' completion
Technology	Sensitivity labelling functionality within Microsoft 365 is not yet enabled.	2 Update and operationalise Council's Information Access and Management Policy 6 Ensure information systems that are source of truth for Council's records and information have up-to-date information security classification labels
	Labels for information classification within Council's Content Manager (EDDIE) are out of date.	2 Update and operationalise Council's Information Access and Management Policy 6 Ensure information systems that are source of truth for Council's records and information have up-to-date information security classification labels

Table 6: Information Security Classification recommendations and pain points addressed

Category	Pain points (from current state assessment)	Recommendations
Process	Information security classification is not consistently applied to meeting information.	2 Update and operationalise Council's Information Access and Management Policy 4 Review scope and logical order of training modules, and formalise a plan for modules' completion
	Community does not have visibility of Council's current efforts relating to making information available, which impacts their perception of transparency and openness.	1 Improve how Council communicates its processes and efforts relating to making meetings information available
Technology	InfoCouncil is not integrated with EDDIE.	6 Ensure information systems that are source of truth for Council's records and information have up-to-date information security classification labels

Table 7: Council meetings information practices recommendations and pain points addressed

Appendix D Glossary

Acronym, word or phrase	Description*
Business Impact Level (BIL)	Business impact measures the consequence and significance of an impact to Council if a disruption was to occur to a system, process, project and/or other business operation. The Business Impact Level (BIL) is determined by the impact to confidentiality, integrity and availability if Council information is lost, compromised or misused.
Information asset	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling Council to perform its business functions, thereby satisfying a recognised Council requirement.
Information Asset Custodian	The role responsible for implementing and maintaining information assets to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility. A custodian will be responsible for specific classifications or categorisations of information.
Information Asset Register (IAR)	A register of information about the significant information assets held by Council. For each information asset, the register holds details of its content type, source type, custodianship, information exchange capability, the role played by the agency in its collection, its scope of use and level of support within Council as well as the ongoing management costs.
Information Asset Steward	The role responsible for the day-to-day management of information assets within their functional area. Stewards are responsible for activities associated with the integrity, quality and protection of information assets.
Information classification	The process by which Council assesses the information it holds and the appropriate level of protection it should be given.
Information Creator	Council staff who capture or create information in alignment with policies, procedures, processes and business rules to contribute to Council's functions and activities.
Information custodianship	The assignment of roles and responsibilities to information assets to ensure assets are appropriately identified and managed throughout their lifecycle.
Information management (IM)	The means by which Council plans, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains and disposes of its information; as well as any means through which Council ensures that the value of that information is identified and exploited to its fullest extent.
QGEA	The Queensland Government Enterprise Architecture (QGEA) is a decision making and policy framework for enabling government and agencies (including Council) to collaboratively provide better services for Queenslanders, more efficient and effective use of ICT in Government, leverage existing investments and maximise future investments.
QGISCF	The Queensland Government Information Security Classification Framework (QGISCF) supports the government's Information security policy (IS18:2018). The framework sets the minimum requirements for information security classification.

Table 8: Glossary of terms

Descriptions are based on terms defined in the QGEA glossary and ISO 27001.