Office of the Information Commissioner
Queensland

Publishing OFFICIAL information assets

Supporting the push model through proactive disclosure

Right to Information Act 2009 (Qld)

Report No. 3 to the Queensland Legislative Assembly for 2022-23

Copies of this report are available on our website at www.oic.qld.gov.au and further copies are available on request to:

Office of the Information Commissioner
Level 7, 133 Mary Street, Brisbane, Qld 4000
PO Box 10143, Adelaide Street, Brisbane, Qld 4000

Phone +61 7 3234 7373 or Freecall 1800 OIC QLD (1800 642 753)
Email administration@oic.qld.gov.au
Web www.oic.qld.gov.au

ISBN: 978-0-6456316-1-6

March 2023

Mr Peter Russo MP
Chair
Legal Affairs and Safety Committee
Parliament House
George Street
Brisbane QLD 4000

Dear Mr Russo

I am pleased to present 'Publishing OFFICIAL information assets: Supporting the push model through proactive disclosure'. This report is prepared under section 131 of the *Right to Information Act 2009* (Qld).

The report outlines how three Queensland government departments identify and classify their OFFICIAL information assets and how they support the push model through maximum disclosure of these information assets. The report identifies examples of good practice and makes one recommendation to all government agencies.

In accordance with subsection 184(5) of the *Right to Information Act 2009* (Qld), I request that you arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

Table of contents

Summary

Government agencies collect, hold and use a significant amount of information. Under the *Right to Information Act 2009* (the Act), they should release information as a matter of course unless there is a good reason not to. This is referred to as the 'push model'. This proactive disclosure approach increases accountability and transparency. It also helps build trust in government.

A range of policies and guidelines govern how Queensland Government departments manage the information they hold. The Queensland Government Enterprise Architecture Information access and use policy (IS33)[1] supports the push model. It states that

> *Departments must provide government information to the public to the maximum extent possible.*

In addition to identifying and classifying their information assets, departments must establish and maintain an information asset register.

The Queensland Government Enterprise Architecture (QGEA) defines an information asset as 'an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business function, thereby satisfying a recognised agency requirement'.[2]

The register should capture all information assets across the department and their key characteristics, including their security classification. One element of information security is **confidentiality** – the risk of unauthorised or inappropriate disclosure or release. Departments can apply one of three confidentiality labels to their information assets – OFFICIAL, SENSITIVE and PROTECTED.[3]

Overall, **OFFICIAL** information represents most Queensland Government's information by volume, but lowest business impact per document if compromised or lost.[4] OFFICIAL information is routine information without special sensitivity or handling requirements.

1 Available on QGEA website
2 QGEA Identification and classification of information assets guideline, available on QGEA website
3 The Queensland Government Information Security Classification Framework (QGISCF) does not provide specific guidance for handling national security information, classified material or systems that are assessed to have confidentiality requirements above PROTECTED.
4 QGISCF, available on QGEA website

OFFICIAL information is highly relevant in the context of the Act and the push model. Assessing the confidentiality element of their information assets gives agencies a guide as to whether these assets may be suitable for publication or release.

Publishing data on public platforms is an effective way to proactively share information with the community. Open data portals or websites, publication schemes and administrative access arrangements are important strategies that support the proactive and maximum disclosure of government information.

When considering whether to publish information, government agencies need to balance the information security risks against the disclosure benefits. De-identification, aggregation and redaction techniques can be used to support proactive information release through publication, including datasets that may be in a SENSITIVE or PROTECTED information asset.

Agencies also need to consider other obligations they may have about the information, for example confidentiality agreements or licensing considerations.

The objective of the audit was to determine whether departments have systems in place that support the push model through maximum disclosure of OFFICIAL information assets.

We audited three departments – the Department of Employment, Small Business and Training (**DESBT**), the Department of State Development, Infrastructure, Local Government and Planning (**DSDILGP**) and the Queensland Corrective Services (**QCS**) and assessed how they:

- identify and classify information assets
- make OFFICIAL information assets available to the maximum extent possible.

Conclusions

Information assets vary greatly between government agencies. Identifying the assets and their characteristics in a centralised register helps an agency manage the assets consistent with the rules governing access and use of the information. Clear, documented procedures outlining roles and responsibilities support good information management.

The three audited departments have established information asset registers and a documented approach with defined roles and responsibilities to approve the publication of information. However, they also have deficiencies in how they maintain their information asset registers.

These registers have gaps. Not recording all information assets and their access or use constraints and rights increases the risk of unauthorised disclosure, misuse or unavailability of the information. It also means that the departments may not maximise the disclosure of low-risk OFFICIAL information to the public.

DSDILGP and QCS's publication approval procedures involve their Right to Information team or manager in the process. This is good practice. It shows that the departments are mindful of their legislative obligations under the Act and the *Information Privacy Act 2009* and take deliberate steps to assess and mitigate privacy risks before publishing the information.

While the approval procedures of these two departments clearly refer to the security classification of the information assets considered for publication, this is not the case for DESBT's procedure. It does not mention the information security classification labels, OFFICIAL or otherwise, when considering information assets suitable for public release. This means DESBT is not using the information security classification label of an asset as a trigger for potential publication and may not provide information to the public to the maximum extent possible.

The three audited departments do not publish their information asset register, or a redacted version of it. DESBT and QCS advised they are working towards this. When the community does not know what information assets a government agency holds, this can result in inefficient processes to access information. For example, members of the public may seek access under a legislative process to information that the agency has already determined suitable for disclosure or administrative release.

Key findings

Governance

As the Information governance policy[5] requires, the three audited departments have established an information governance framework. Information steering committees act as the oversight and/or advisory body on information management, including information security.

Under the Information asset custodianship policy (IS44)[6] departments, through their information asset custodians, must identify and register their information assets. A complete, current and accurate information asset register, with clear classifications,

5 Available on QGEA website
6 Available on QGEA website

access/use constraints and rights, can help agencies assess whether they provide information to the public to the maximum extent possible.

The departments have outlined the responsibilities of the information asset custodians. At DSDILGP and QCS, the custodians must record the details of the information assets under their care in the department's information asset register.

However, DESBT's policy and guideline do not assign responsibility for recording the information assets in the register. This increases the risk of the information asset register being incomplete or inconsistent.

The three audited departments have established information asset registers, but these have gaps. For example, the departments have published datasets on the Queensland Government Open Data Portal.[7] DSDILGP and QCS record these datasets in their respective registers, but DESBT does not. DSDILGP advised its register is incomplete.

Identifying and classifying information assets

The Information asset register guideline[8] outlines recommended practices. It suggests a structure and outlines the content requirements for an information asset register.

DESBT and QCS do not capture all the 11 recommended minimum requirements and DSDILGP's register showed limited or no information in some rows. Not recording all the information assets and the specific rules governing access and use of the information increases the risk of unauthorised disclosure, misuse or unavailability of the information.

QCS advised it previously captured the 11 recommended minimum requirements but since removed some columns because they were not suitable or duplicated within the register.

DESBT and QCS make their information asset registers available to all staff. DSDILGP makes the register available to relevant staff only. Granting access to a wider internal audience will increase awareness of the information assets the department holds.

The three audited departments review their registers for high business impact information assets as part of their annual reporting obligations about information security risk management.

DESBT and QCS do not regularly review the OFFICIAL information assets on their registers. This means they cannot be sure that they are maximising public disclosure of

7 https://www.data.qld.gov.au/
8 Available on QGEA website

the information they hold or that their risk mitigation strategies, including against re-identification risks, are effective.

Publishing information assets

"Departments must provide government information to the public to the maximum extent possible"

Source: Queensland Government Enterprise Architecture Information access and use policy (IS33)[9]

All three audited departments have a documented approach with defined roles and responsibilities to approve information for public disclosure.

The DESBT Open data procedure does not reference OFFICIAL information or make connection with information security classification labels suitable for public release. This could increase the risk of disjointed processes for identifying and classifying OFFICIAL information assets considered for public disclosure. This could also increase the risk of unauthorised disclosure or misuse of information assets.

None of the three audited departments publish their information asset register, or a redacted version of it. This means that the community does not know what OFFICIAL information is held by these agencies. As a result, members of the public may seek access under a legislative process to information that the agency has already determined suitable for disclosure or administrative release.

DESBT and DSDILGP mention administrative access on their RTI webpages but do not specify what information they release administratively.

In 2018 we surveyed all departments to find out what level of information management they aimed to achieve, and how they self-assessed their maturity at the time.

QCS has achieved its 2018 targets maturity for the elements about information asset registers, custodianship and classification. DESBT and DSDILGP remain at the 2018 maturity level and are still working towards their targets.

9 Available on QGEA website

Recommendations

We made specific recommendations to each audited department. The departments accepted all recommendations.

The audit raised issues relevant to all government agencies. We make one recommendation to all agencies.

Recommendation 1

We recommend that within 6 months the Department of Employment, Small Business and Training assigns responsibility for recording the information assets in its register.

Recommendation 2

We recommend that within 18 months the Department of Employment, Small Business and Training and the Department of State Development, Infrastructure, Local Government and Planning record all their information assets in their respective registers.

Recommendation 3

We recommend that within 18 months the Department of Employment, Small Business and Training, the Department of State Development, Infrastructure, Local Government and Planning and Queensland Corrective Services record in their respective registers the asset constraints for all their information assets.

Recommendation 4

We recommend that within 18 months the Department of State Development, Infrastructure, Local Government and Planning makes its information asset register available to all staff.

Recommendation 5

We recommend that within 18 months the Department of Employment, Small Business and Training and Queensland Corrective Services establish a process to regularly review the security classification of the OFFICIAL information assets recorded in their respective registers, and whether the associated security controls remain appropriate.

Recommendation 6

We recommend that within 12 months the Department of Employment, Small Business and Training incorporates considering the information security classification labels of

information assets into its procedure for assessing whether the assets are suitable for publication or release.

Recommendation 7

We recommend that within 18 months the Department of Employment, Small Business and Training and the Department of State Development, Infrastructure, Local Government and Planning list their administrative access arrangements on their RTI webpage.

Recommendation 8

We recommend that within 18 months the Department of Employment, Small Business and Training, the Department of State Development, Infrastructure, Local Government and Planning and Queensland Corrective Services publish their information asset register, or a version of it, on their websites.

Recommendation to all government agencies

We recommend that all government agencies publish their information asset register, or a version of it, on their websites.

Agency responses

We provided a copy of this report to the audited departments for their comments. We have considered their views in reaching our conclusions. The departments' responses are in Appendix 1.

1 Context

To manage information effectively, departments should have a systematic approach, including clear authorising and governance arrangements, to support public access to information while safeguarding the information that requires protection.

A range of policies and guidelines govern how Queensland Government departments manage the information they hold:

- The Information security policy (IS18)[10] recognises that to build trust and deliver business value, it is critical departments appropriately protect the information they hold.
- The Information access and use policy (IS33)[11] states that departments must provide government information to the public to the maximum extent possible.
- The Information asset custodianship policy (IS44)[12] requires departments to identify and register their information assets, and assign appropriate custodianship roles and responsibilities.
- Departments must meet minimum security requirements and comply with the Queensland Government Information security classification framework (QGISCF)[13] and associated policies.

An information asset is:

> *An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business function, thereby satisfying a recognised agency requirement.*[14]
>
> *Information assets can be documents, electronic messages, a row in a database (or the database table itself), collections of metadata, or a table or figure within a document. An information asset may hold information in multiple formats or media types.*[15]

This means there is not necessarily a 1:1 relationship between an information asset and a dataset.

10 Available on QGEA website
11 Available on QGEA website
12 Available on QGEA website
13 Available on QGEA website
14 QGEA Identification and classification of information assets guideline, available on QGEA website
15 QGISCF, available on QGEA website

The QGISCF provides a process and direction for determining the classification of information assets under three elements of information security: confidentiality, integrity and availability.

Confidentiality is about the risk of unauthorised or inappropriate disclosure or release. Three labels can be used to classify an information asset depending on its confidentiality: OFFICIAL, SENSITIVE and PROTECTED.

Overall, OFFICIAL information represents most government-held information by volume and lowest business impact. It should be proactively disclosed to support the push model, where appropriate.

In addition to identifying and classifying their information assets, departments must establish and maintain an information asset register:

> *A register of information about the significant assets in the agency's information portfolio. 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 the agency as well as the ongoing management costs.*[16]

The register should capture all information assets across the department, assess their level of confidentiality and suitability for public release, and assign custodians to each information asset. Publishing information asset registers, or a version of them, can also provide assurance that departments are maximising disclosure.

It is important to note that overclassifying information assets (ie selecting SENSITIVE for information that should be OFFICIAL) can add additional risks to the ongoing management, including increased costs, additional storage and protection requirements, and reduced accessibility.

Publishing data on public platforms is an effective way to proactively share information with the community. Government agencies can use de-identification, aggregation and redaction techniques to support proactive information release under *Right to Information Act 2009* and achieve open data goals. They need to ensure the security of personal information when releasing data derived from information about individuals.

The objective of the audit was to determine whether departments have systems in place that support the push model through maximum disclosure of OFFICIAL information assets.

16 Queensland Government glossary https://www.forgov.qld.gov.au/news-events-and-consultation/glossary

We assessed whether the audited departments:

- identify and classify information assets
- make OFFICIAL information assets available to the maximum extent possible.

Department of Employment, Small Business and Training

The Department of Employment, Small Business and Training (DESBT) was established in December 2017 with responsibilities drawn from other departments.

DESBT's purpose is to support Queensland's future workforce by connecting all Queenslanders to learning opportunities through quality training, employment opportunities and by helping small businesses to start, grow and thrive.[17]

DESBT is structured into three service delivery areas:

- Employment – To increase employment opportunities for Queenslanders, in particular disadvantaged cohorts
- Small Business – To ensure small business can seamlessly interact with government and are supported to start, grow and employ
- Training and Skills – To regulate Queensland apprenticeships and traineeships, and facilitate access and participation in vocational education and training pathways, enabling Queenslanders to gain employment in current and future industries.[18]

As at June 2022, DESBT employed 568 full time equivalent employees.[19]

Department of State Development, Infrastructure, Local Government and Planning

Following changes[20] effective from 12 November 2020, the former Department of Local Government, Racing and Multicultural Affairs became the Department of State Development, Infrastructure, Local Government and Planning (DSDILGP).

DSDILGP's purpose is to connect industry, businesses, community and government at all levels to create place-based solutions that leverage regional strengths and unlock sustainable growth. The department promotes global competitiveness, facilitates modern infrastructure design and environmentally sustainable development, promotes innovation and enterprise, and fosters initiatives that sustain Queenslanders and their communities.[21]

17 DESBT Annual Report 2021-22
18 DESBT 2022-23 Service Delivery Statements
19 DESBT Annual Report 2021-22
20 Administrative Arrangements Order (No. 2) 2020, dated 12 November 2020.
21 DSDILGP Annual Report 2021-22

DSDILGP is shaping Queensland's future by driving economic growth and enabling well-planned, inclusive and resilient local communities.[22]

As at June 2022, DSDILGP employed 944 full time equivalent employees.[23]

Queensland Corrective Services

Queensland Corrective Services' (QCS) purpose is to provide safe, modern and responsive correctional services which rehabilitate prisoners and offenders and prevent crime, making Queensland safer.[24]

QCS, in partnership with other key criminal justice agencies, is committed to the critical role of community safety and crime prevention.

QCS operates 11 high security and six low security correctional centres. QCS also operates 35 community corrections district offices and over 140 reporting locations across the State. Prisoners and offenders are provided with appropriate classification, supervision and access to programs, education and vocational training to maximise their chance of successful reintegration into society.[25]

As at June 2022, QCS employed 6,492 full time equivalent employees.[26]

Report structure

We structured our report as follows:

Section	Table column heading Contents
Chapter 2	presents the findings about information management governance
Chapter 3	discusses how the audited departments identify and classify their information assets, and record them in the information asset register
Chapter 4	examines the approval processes for publishing information assets
Appendix 1	contains agency responses and action plans
Appendix 2	outlines the maturity of information management legend
Appendix 3	outlines our audit methodology

22 DSDILGP website: https://www.statedevelopment.qld.gov.au/about-us
23 DSDILGP Annual Report 2021-22
24 QCS Annual Report 2021-22
25 QCS website: https://corrections.qld.gov.au/about-queensland-corrective-services/
26 QCS Annual Report 2021-22

2 Information management governance and maturity

2.1 Introduction

Information is a core strategic asset. Good information governance helps to drive practices that ensure the right information is available, to the right person, at the right time.

Under the Information governance policy,[27] departments must implement formal information governance. They can establish a body responsible for information governance or assign responsibility to an existing body.

The role of the body includes reviewing and monitoring conformance to obligations, for example legislation, principles, policy and architecture requirements.[28] This includes managing information asset custodianship and assigning responsibility for and overseeing maintenance of the department's information asset register.

Under the Information asset custodianship policy (IS44)[29] departments, through their information asset custodians, must identify and register their information assets. This ensures that custodians have a clear understanding of the information assets under their care and promotes a consistent approach.

The Information management roles and responsibilities guideline[30] provides more details on the various roles.

2.2 Conclusion

The three audited departments have established an information governance framework within their corporate governance structure. Information steering committees act as the oversight and/or advisory body on information management, including information security.

The departments also have outlined the responsibilities of the information asset custodians. At DSDILGP and QCS, the custodians must record the details of the information assets under their care in the department's information asset register.

However, DESBT's policy and guideline do not assign responsibility for recording the

27 Available on QGEA website
28 QGEA Implementing information governance guideline Available on QGEA website
29 Available on QGEA website
30 Available on QGEA website

information assets in the register. This increases the risk of the information asset register being incomplete or inconsistent.

In 2018 we asked all departments to self-assess the maturity of their information management practices and indicate what maturity level they aimed to achieve. This audit gave us the opportunity to assess the three audited departments' progress in three specific areas.

QCS has achieved its 2018 targets maturity for the elements about information asset registers, custodianship and classification. DESBT and DSDILGP remain at the 2018 maturity level and are still working towards their targets.

2.3 Results

The three audited departments have documented how they identify and classify information assets. Their approach aligns with Queensland Government Information security classification framework (QGISCF).[31]

DESBT uses a template to assess the security classification of an information asset. The template includes consideration of business impact, risk analysis and controls. The default classification level for all information assets within the department is OFFICIAL. This means that any information without a classification label is OFFICIAL.

Similarly, DSDILGP assesses the level of business impact or risk across the information security elements of confidentiality, integrity and availability. In its procedure, the department notes that

> *a security classification label is not to be applied to information in order to either restrain competition, hide violations of law, inefficiency, or administrative error to prevent embarrassment to an individual or to the department or prevent delays in the release of information that does not need protection.*

QCS uses a form to record the information asset security classification and assessment. The form is set out in five sections:

1. Information asset details: The description, name, custodian, date of assessment, details, location the information asset will be stored and security control notes.
2. Approved conditions for modifying the security classification. This includes any specific conditions such as embargos and sequence activities.

31 Available on QGEA website

3. Approved modification table: Description, confidentiality score, integrity score, and availability score.
4. Delegate approval: Information asset custodian approval statement for the information security classification impact assessment.
5. Instructions: QCS business impact levels (BILs) and examples. It also includes risk considerations and impact table for each CIA element.

Information asset custodians

While DESBT and DSDILGP do not have a standalone custodianship policy, other policy and procedure documents outline the custodian roles and responsibilities which includes the management of information assets.

DESBT outlines the roles and responsibilities in its Information security classification and handling policy, and Information security classification and handling guideline. The information asset owner (custodian) is responsible for applying the correct classification levels and that the controls to protect the information assets are effective.

The policy and guideline do not prompt the custodian to record the information assets in the department's register.

DSDILGP outlines the roles and responsibilities in its Information security policy, Information security classification and control procedure, and Information management and technology delegations. The information asset custodian is responsible for identifying information assets, completing business impact assessments, applying the confidentiality security levels, recording the details in the register, and maintaining the information asset throughout its lifecycle.

QCS outlines roles and responsibilities in its Information security classification and handling policy, Information security classification and handling procedure, and Information asset custodianship policy. Information asset custodians are responsible for approving the information security classification, ensuring the security and confidentiality of the information, establishing and maintaining a register, and overall accountability for the lifecycle of the information asset.

Recommendation 1
We recommend that within 6 months the Department of Employment, Small Business and Training assigns responsibility for recording the information assets in its register.

Information management maturity

Our Audit of information management maturity report[32] was tabled in Parliament on 14 February 2019. We also provided individual feedback to each department.

We developed a self-assessment tool[33] to be completed by the departments. The tool includes questions about information asset registers, custodianship and classification. It sets five levels of maturity: unmanaged, ad hoc, defined, managed and proactive. Appendix 2 outlines what the various maturity levels look like for each element of information asset management.

The tool is available on the OIC website.[34] We encourage all departments to regularly monitor the maturity of their information management and determine whether they achieve their targets.

This aligns with the Implementing information governance guideline[35] which states:

> *The information governance body may assess the agency's information management maturity from time to time. The information governance body should oversee and analyse the outcomes of these assessments.*

Figure 1

2018 self-assessment results for specific criteria

Department	Information asset register		Custodianship		Classification	
	Maturity	Target	Maturity	Target	Maturity	Target
DESBT	Ad-hoc	Managed	Ad-hoc	Managed	Ad-hoc	Managed
DSDILGP	Ad-hoc	Defined	Ad-hoc	Defined	Managed	Proactive
QCS	Defined	Managed	Unmanaged	Defined	Unmanaged	Defined

Source: Office of the Information Commissioner

We reviewed the 2018 self-assessment results to determine the departments' progress towards their target maturity level. In assessing current maturity, we considered audit evidence and observations and consulted the respective department.

32 Available on OIC website
33 Available on OIC website
34 Available on OIC website
35 Available on QGEA website

Figure 2

Current information management maturity for specific criteria

Department	Information asset register	Custodianship	Classification
	Current maturity	Current maturity	Current maturity
DESBT	Ad-hoc	Ad-hoc	Ad-hoc
DSDILGP	Ad-hoc	Ad-hoc	Managed
QCS	Managed	Defined	Defined

Source: Office of the Information Commissioner

QCS has achieved its 2018 targets maturity for the elements about information asset registers, custodianship and classification. DESBT and DSDILGP remain at the 2018 maturity level and are still working towards their targets.

3 Identifying and classifying information assets

3.1 Introduction

OFFICIAL information is highly relevant in the context of the *Right to Information Act 2009* (the Act) which recognises that information in a government agency's possession or control is a public resource.

Under the Act, government agencies should release information as a matter of course, unless there is a good reason not to. This approach increases accountability and transparency. It also helps build trust in government.

Government agencies collect, hold and use a significant amount of information. To ensure trust and deliver business value, agencies must protect this information appropriately. The Queensland Government's Information security policy (IS18)[36] seeks to ensure all departments apply a consistent, risk-based approach when implementing information security to maintain confidentiality, integrity and availability.

Under the Information asset custodianship policy (IS44),[37] departments must identify their information assets, ensure they establish and maintain an information asset register, and assign appropriate custodianship roles and responsibilities to ensure these assets are managed throughout their lifecycle.

The Queensland Government Information Security Classification Framework (QGISCF)[38] released in February 2020 states that:

> *Content classification of information helps Queensland Government agencies make more informed and timely decisions about how they should capture, store, maintain, transmit, process, use and share information to best deliver services to Queenslanders*.

The QGISCF supports IS18. It provides a process and direction for determining the security classification of information under three elements of information security: confidentiality, integrity and availability. Confidentiality is about the risk of unauthorised or inappropriate disclosure or release.

When agencies assess the confidentiality element of their information assets, it gives them a guide as to whether these assets may be suitable for publication or release.

36 Available on QGEA website
37 Available on QGEA website
38 Available on QGEA website

3.2 Conclusion

Information assets vary greatly between departments. Identifying information assets, and the rules about access to and use of the information, in a centralised register helps a department understand and manage its assets and facilitates access to and reuse of information.

The three audited departments have an established register that assigns a custodian and security classification to OFFICIAL information assets. However, the registers have gaps.

They do not capture some information assets or the constraints, use and rights for certain assets. Not recording all information assets and their constraints or rights increases the risk of unauthorised disclosure, misuse or unavailability of the information.

As environments and circumstances change, information owners should review confidentiality levels to ensure security classification and controls remain appropriate. DESBT and QCS do not regularly review the security classification of OFFICIAL information assets on their registers. This means they may not maximising public disclosure of the information they hold or check that their security risk mitigation strategies are effective.

While all DESBT and QCS staff have access to their department's information asset register, DSDILGP makes the register available to relevant staff only. Granting access to a wider internal audience will increase awareness of the information assets the department holds.

3.3 Results

Information asset register

An information asset register lists the existing information assets across all business units within an organisation. It enables users of information to identify the available information resources from a single source and gives information custodians an overview of the information assets under their care.

The Information asset register guideline[39] outlines recommended practices. It suggests a structure and outlines the content requirements for an information asset register. The guideline supports IS44.

39 Available on QGEA website

When an agency has an established and maintained information asset register, it identifies, classifies and organises the assets in a way that facilitates access to and reuse of the information.

All three audited departments have an established register that assigns a custodian and security classification to OFFICIAL information assets. Figure 1 gives an overview of the registers' features.

Figure 3

Information asset register features – OFFICIAL classification

Criteria	DESBT	DSDILGP	QCS
Established information asset register	✓	✓	✓
Records OFFICIAL information assets	✓	✓	✓
Assigns a custodian to information asset	✓	✓	✓
Records open data and information assets published on the agency website	X	✓	✓
Assigns assets constraints and rights	X	✓	✓
Captures recommended minimum requirements outlined in the Information asset register guideline	X	✓	X
All staff can access the register	✓	X	✓
Regularly reviews of the security classification of OFFICIAL information assets	X	✓	X

Source: Office of the Information Commissioner

Register and published information

Government agencies publish a range of information, for example on their websites or on the government's open data portal. By nature, agencies should classify this information as OFFICIAL in their register.

PUBLIC is not a security classification level under the QGISCF. The framework explains that

> *Public information is OFFICIAL information that has undergone an agency authorised publication process to identify that it was suitable to be published.*

At the time of the audit, DESBT recorded 42 information assets in its register, of which 6 were classified OFFICIAL. The 6 OFFICIAL information assets related to ICT assets under 3 categories: business processes, software and network.

DESBT's information asset register has gaps and does not capture open data or information assets published on the department's website, for example information available through the publication scheme. In July 2022, the department had 48 datasets published on the Queensland Government Open Data portal but these datasets are not listed in its information asset register.

This indicates that the department's approach to registering its information assets is not effective. DESBT advised it is updating its register to record all OFFICIAL information assets, including those the department has already published.

DSDILGP and QCS's registers record open data and information assets published on the respective department's website. For example, they list the gifts and benefits register, annual report data, overseas travel, on-time payment reports, awarded contracts and grants, department priorities, decisions and policies.

QCS recorded 156 information assets in its register, of which 39 were classified OFFICIAL at the time of the audit. The 39 OFFICIAL information assets relate to resources and training, media and communication data, financial data, escort/security data and registers, reportable deaths in custody, workforce data, strategic risks, governance, policies, procedures, research, contract and procurement, performance, asset management, fleet register, inventory and budgets.

At the time of the audit, DSDILGP recorded 191 information assets in its register, of which 145 were classified OFFICIAL. The 145 OFFICIAL information assets relate to planning and development, maps, funding, projects, consultation, complaints, policies, grants, gifts and benefits, training, appeals, performance, probity and right to information data.

However, the department advised the register is incomplete. DSDILGP is planning a focused resourcing effort to cover all its information assets and uplift the register by end of 2023.

Recommendation 2

We recommend that within 18 months the Department of Employment, Small Business and Training and the Department of State Development, Infrastructure, Local Government and Planning record all their information assets in their respective registers.

Minimum requirements

The QGEA Information asset register guideline helps departments developing their information asset register. It highlights the 11 recommended minimum requirements for an information asset register:

- asset identifier
- information asset title (business name for the information asset)
- information asset description
- original acquisition/creation date
- keywords (theme or keywords that may enable faster searching for the information asset)
- security classification
- information asset owner
- information asset custodian
- access constraints
- use constraints
- access rights.

DSDILGP's register captures all the recommended minimum requirements however some rows and columns had limited or no information. The department advised in these instances the confidentiality, integrity and availability elements had not yet been assessed.

DESBT's register does not capture all the recommended minimum requirements, for example asset identifier, original acquisition date/creation date and keywords. The department advised it is updating its register to capture all recommended minimum requirements.

QCS's register does not capture all the recommended minimum requirements, for example original acquisition date/creation date and keywords. QCS previously incorporated the minimum requirements into its register but has since removed some columns because they were not suitable or duplicated within the register.

Access constraints and access rights helps departments understand and manage the specific rules relating to the access to and use of the information asset, including publishing or sharing the information asset content.

Figure 4

Asset constraints definitions

Asset constraints	
Access constraints	Specific constraints relating to access to the information asset.
Use constraints	Specific constraints relating to the use of the information asset.
Risk profile*	Specific risks to the organisation relating to the misuse or unavailability of the information asset and details of mitigation strategies.
Access rights	Rules related to the publication or sharing of the information asset content.

** Not a recommended minimum requirement*

Source: Queensland Government Enterprise Architecture, Information asset register guideline

DSDILGP and QCS record minimal asset constraints in their registers.

DESBT does not record asset constraints in its register. This could increase the risk of unauthorised disclosure, misuse or unavailability of the information asset. DESBT advised it is updating its register to include asset constraints and rights.

Recommendation 3

We recommend that within 18 months the Department of Employment, Small Business and Training, the Department of State Development, Infrastructure, Local Government and Planning and Queensland Corrective Services record in their respective register the asset constraints for all their information assets.

Access to the register

Making an information asset register available to all staff enables users of information to:

- identify the available information resources from a single source
- note the classification of information assets and their access or use constraints
- identify the custodian of information assets
- avoid duplication of information, systems and processes.

DESBT and QCS make the register available to all staff.

DSDILGP makes the register available to relevant staff only. The department advised it is working towards broadening access to the register following a discovery information profiling project. Granting access to a wider internal audience will increase awareness of the information assets the department holds.

Recommendation 4
We recommend that within 18 months the Department of State Development, Infrastructure, Local Government and Planning makes its information asset register available to all staff.

Classifying information assets

Departments should classify their information and information assets according to business impact and implement appropriate controls according to the classification. The QGISCF[40] outlines the classification process and sets minimum requirements.

One element of information security is **Confidentiality** – the risk of unauthorised or inappropriate disclosure or release. The three confidentiality classification labels covered by the QGISCF are:

- OFFICIAL – for example an agency's published annual report
- SENSITIVE – for example certain personal information which agencies must safeguard under the *Information Privacy Act 2009*
- PROTECTED – for example information which, if compromised, could cause serious damage to the State, the Government, commercial entities or members of the public.

40 Available on QGEA website

At the agency level, decision-makers require sufficient guidance about classifying information to support consistent outcomes and meet legislative and regulatory obligations tailored to each level of confidentiality and risk.

The three audited departments have sufficient guidance for decision-makers to facilitate risk assessments. This guidance supports a risk-based approach by performing business impact assessments to determine the appropriate information security classification.

DESBT uses an Information Security Classification Assessment template which embeds business impact, risk analysis and controls into the process. The template includes confidentiality risk considerations.

DSDILGP provides guidance in its Information security classification and control procedure for the identifying information assets, completing business impact level assessments and assigning confidentiality security levels. It includes the confidentiality risk considerations and their potential impacts.

QCS uses an Information security classification impact assessment form which embeds business impact, risks analysis, conditions, security classification, and approval into the process. It includes the confidentiality risk considerations.

Regular reviews

As environments and circumstances change, information owners should review confidentiality levels to ensure controls remain appropriate.[41] The impact from loss, compromise, or damage to information may reduce or increase over time.

The QGISCF states that

"An agency must apply security controls which are commensurate with the assessed business impact."

While the framework does not mandate specific controls, agencies should select the controls best suited to their business and technology needs. The controls must adequately protect the information based on the confidentiality level of the information.

The three departments review their register annually as part of their reporting obligations under IS18. They focus on information assets that would have high business impact if lost, compromised or misused. These assets are likely to be classified SENSITIVE or PROTECTED, for example because they

"may include personal information or legal professional privilege."[42]

41 QGISCF available on QGEA website
42 QGISCF available on QGEA website

OFFICIAL information assets have the lowest business impact per document if compromised or lost. This is because OFFICIAL information is routine information without special sensitivity or handling requirements.

DSDILGP's Information security classification and control procedure states that the department will undertake continuous review and assurance of information security classification. It advised the continuous review includes OFFICIAL information assets.

DESBT and QCS do not regularly review the security classification and controls of their OFFICIAL information assets. This means there is a risk that they are not maximising public disclosure of the information they hold or reviewing the effectiveness of their security controls.

Recommendation 5

We recommend that within 18 months the Department of Employment, Small Business and Training and Queensland Corrective Services establish a process to regularly review the security classification of the OFFICIAL information assets recorded in their respective registers, and whether the associated security controls remain appropriate.

4 Publishing information assets

4.1 Introduction

Government agencies hold a lot of information. Under the *Right to Information Act 2009* (the Act) they should release information as a matter of course, unless there is a good reason not to. This proactive disclosure approach increases transparency and accountability of, and community confidence in, government.

The Queensland Government Enterprise Architecture Information access and use policy (IS33)[43] outlines the approach to access, exchange and license government information. The policy supports the Act which established a 'push' model as a default position for the proactive release of government information.

It also supports the Queensland Government Open Data Policy Statement (the open data policy) and commitment to releasing data and allowing it to be freely used.[44] Under IS33,

> *Departments must provide government information to the public to the maximum extent possible*

Publishing data on public platforms is an effective way to proactively share information with the community. Open data portals, publication schemes and administrative access arrangements are important strategies that support the proactive and maximum disclosure of government information, unless contrary to the public interest.

Government agencies are increasingly looking at publishing information in interactive and interrogative forms such as dashboards and visualisations.

A complete, current and accurate information asset register, with clear classifications, access/use constraints and rights, can help agencies assess whether they provide information to the public to the maximum extent possible.

When deciding to publish information, government agencies need to balance the information security risks against the disclosure benefits. De-identification, aggregation and redaction techniques can be used to support proactive information release through publication. For example, SENSITIVE or PROTECTED information assets may consist of many datasets, some of which agencies could publish once they have applied de-identification techniques.

43 Available on QGEA website
44 https://www.data.qld.gov.au/_resources/documents/qld-data-policy-statement.pdf

Depending on the nature of the information, agencies should also consider a range of other factors including, but not limited to, confidentiality agreements, data quality and re-identification risks not considered in the security classification.

4.2 Conclusion

The three audited departments have a documented approach with defined roles and responsibilities to approve publishing information.

DSDILGP and QCS's publication approval procedures involve their Right to Information (RTI) team or manager in the process. This is good practice. It means that the departments are mindful of their legislative obligations under the *Right to Information Act 2009* and the *Information Privacy Act 2009* and take deliberate steps to assess and mitigate privacy and other risks before publishing the information. Their approval procedures also clearly refer to the security classification (OFFICIAL) of the information assets considered for publication.

However, DESBT's procedure does not mention the information security classification labels, OFFICIAL or otherwise, when considering information assets suitable for public release. This increases the risk of unauthorised or inappropriate disclosure or release of information.

The three audited departments do not publish their information asset register, or a redacted version of it. DESBT and QCS advised they are working towards this. When the community does not know what information assets a government agency holds, this can result in inefficient processes to access information. For example, members of the public may seek access under a legislative process to information that the agency has already determined suitable for disclosure or administrative release. Or the scope of their information access application is broad and unclear.

DESBT and DSDILGP mention administrative access on their RTI webpages but do not specify what information they release administratively.

4.3 Results

The departments document their publication approval process approach in various policies, procedures or guidelines often related to publishing on the Queensland Government Open Data Portal (the open data portal).[45]

Open data is an important part of proactive disclosure of government-held information and is consistent with Queensland public sector agencies' obligations under the Act.

45 Queensland Government Open Data portal: https://www.data.qld.gov.au/

Agencies can also disclose information through other mechanisms such as publication on their websites (including the publication scheme) or administrative release.

Open data

Open data is non-sensitive data that is freely available, easily discovered and accessed, published in ways and with licences that allow easy re-use.[46]

The three audited departments have published datasets on the open data portal. Figure 3 shows the number of datasets published on the portal as at July 2022 and gives some examples of the type of information contained in these datasets.

Figure 5

Datasets on the open data portal

DESBT	DSDILGP	QCS
48 datasets	64 datasets	21 datasets
• Apprenticeship statistics • Training qualifications • Remuneration information • Small business grants	• Regional planning interests • Local laws • Community action program • Funding and loans	• Custodial incidents report • Community offender trends • Prison locations • Community service work performed

Source: Office of the Information Commissioner

In addition, the departments also publish mandatory information such as their gifts and benefits registers, overseas travel and consultancy spending.

The open data policy sets specific expectations on departments, including:

- develop action plans and identify existing mechanisms and policies to support the implementation of the open data policy
- develop a public listing (schedule) of high value data sets, non-sensitive datasets that are not yet openly available, and sensitive datasets that will not be made publicly available.

This means departments should implement a clear open data strategy and schedule to facilitate the cost-effective release of government information whilst upholding the highest standards of security and privacy for individuals.

46 Queensland Government Open Data Policy Statement available on the Queensland Government Open Data portal

The three audited departments have an open data strategy aligned to the open data policy, but these were outdated. DSDILGP and QCS also have a release schedule – outdated – but we could not find a release schedule for DESBT.

We note that, at the time of the audit, the overarching Queensland Government Open Data Policy Statement is under review. The Open Data Portal states that:

> *Agencies are currently working to update their open data strategies. The new strategies will incorporate the direction provided in the Open Data Policy Statement.*

QCS release schedule is embedded in its strategy. It lists published data sets which includes the dataset name, description, first published date, and the frequency of update. It also includes proposed data sets list for publication.

DSDILGP's schedule includes the dataset title, description, licence, update frequency, target publication month, custodian and contact for active, inactive and closed datasets. It advised that a resource has been allocated for 3rd quarter 2022-23 to refresh the strategy, release schedule and action plan.

Outdated strategies increase the risk that departments are not maximising the disclosure of OFFICIAL information assets and government-held information to support a transparent, accountable, efficient and responsive government.

Publication approval process

DESBT has a framework, procedures and guidelines which outline the roles and responsibilities for publishing information assets. Its Open data procedure provides a step-by-step process for data preparation, approval, adding, editing data sets to open data portal, including data formats and licencing. It clearly states that no data is to be published on the open data portal without prior approval.

Datasets or publications are submitted to the DESBT Data and Information Steering Committee for consideration and endorsement. The Director-General, or the appropriate Deputy Director-General, and the information asset custodian must approve the publication before an information asset is made publicly available.

The DESBT Open data procedure states that it:

> *should be read in conjunction with the Queensland Government's Open Data Policy Statement and the DESBT Open Data Strategy 2019-2022,*[47]

and that the custodians must ensure that the data to be published fully complies with the

47 The DESBT Open Data Strategy published on the Open Data portal covers the 2019-20 period.

Information Privacy Act 2009. However, it makes no mention of the information security classification labels, OFFICIAL or otherwise.

This lack of linkage between classifying an information asset and approving its publication increases the risk of unauthorised or inappropriate disclosure or release of information.

Recommendation 6

We recommend that within 12 months the Department of Employment, Small Business and Training incorporates considering the information security classification labels of information assets into its procedure for assessing whether the assets are suitable for publication or release.

The publication approval process for DSDILGP and QCS explicitly refer to the information security classification labels.

DSDILGP outlines roles and responsibilities for publishing information in its Information security classification policy and control procedure, Information management and technology delegations and Open data release guideline.

The guideline steers employees through the end-to-end process for identifying, assessing, formatting and obtaining approval for new data or modification to already released data to the open data portal. It stipulates that only data that has been security classified as OFFICIAL or UNCLASSIFIED is considered for release to the open data portal. There is a link to the Information security classification and control policy for determining the security classification levels.

DSDILGP's Open data release guideline contains good practice elements when considering and mitigating possible risks of publishing information.

Case study - extract from DSDILGP guideline

Privacy and confidentiality

All datasets must have all personal or confidential information removed in accordance with requirements under the *Information Privacy Act 2009 (Qld)*. Refer to the following guidelines relating to the management of personal information:

- Dataset publication and de-identification techniques guideline introduces the tools and techniques for removing personal information from data so that its publication can comply with the privacy principles in the *Information Privacy Act 2009 (Qld)*
- Key privacy concepts guideline provides guidance on personal information that must be protected as set out in the *Information Privacy Act 2009 (Qld)* when publishing data.

Financial information assessment

For any datasets containing financial information, the Chief Financial Officer (CFO) must assess the financial details contained in the datasets and endorse the release as part of the electronic approval process.

Right to Information (RTI) assessment

All datasets, prior to approval, requires the RTI team to perform an independent risk assessment relating to privacy and confidentiality using the dataset publication and risk assessment guideline, to ensure all personal information has been removed and there is no other information in the dataset that could identify individuals.

The RTI team will perform this assessment as part of the electronic approval process.

Source: Department of State Development, Infrastructure, Local Government and Planning

The department's Information Management and Technology Delegation (No. 1) 2020[48] shows that the Director-General and the Deputy Director-General, Business, Commercial and Performance have the authority to release new open datasets, or make significant content and format changes to existing datasets, on the open data portal.

QCS outlines roles and responsibilities in its Information security classification and handling policy and procedure, Information asset custodianship policy, Information management framework, Registering and managing open data procedure, and Open data management and release procedure flowchart.

QCS's Registering and managing open data procedure states that datasets classified

48 Published under the former Department of State Development, Manufacturing, Infrastructure and Planning

OFFICIAL will be considered for release, or where a custodian determines a dataset can achieve a classification of OFFICIAL-PUBLIC through reasonable use of aggregation or de-identification techniques.

The Manager, Right to Information and Privacy, plays a critical role in deciding whether the information is suitable for public release based on the provisions of the *Information Privacy Act 2009* and the *Right to Information Act 2009*.

Publication scheme

Departments must maintain a publication scheme in accordance with the *Right to Information Act 2009* and the Ministerial Guidelines.[49]

The Ministerial Guidelines state that a publication scheme:

> *should be regularly reviewed to ensure information on the publication scheme is current and up to date. Each agency should implement procedures to ensure that new information covered by the publication scheme is available and that any out dated information is replaced or archived.* [50]

Each audited department has a publication scheme which is easy to find. The schemes' structure follows the categories outlined in the Ministerial Guideline. They detail the terms of access, and all content is available free of charge.

Administrative release

Another way government agencies can disclose information is through administrative release. This is not a publication procedure. However, it is a way of responding to requests for information that promotes a pro-disclosure approach. A key benefit of administrative access arrangements is that they give access to information easier and faster than a formal application under the *Right to Information Act 2009* or the *Information Privacy Act 2009.* The legislative process should be a last resort.

DESBT and DSDILGP mention administrative access on their Right to Information (RTI) webpages but do not specify what information they release administratively.

DESBT recommends that the public contact the relevant business unit directly for any information which may be released administratively. While the webpage shows the contact details for the RTI Services team, it does not provide the contact details of the business units.

49 Section 24 of the *Right to Information Act 2009*
50 https://www.rti.qld.gov.au/right-to-information-act/publication-schemes

DSDILGP's RTI webpage states:

> *If you cannot find what you are looking for, please contact our Right to Information team on (07) 3452 6961 or by email at RTI@dsdilgp.qld.gov.au who can help determine if the information is accessible (including through an administrative release process), or if you need to make a formal RTI or IP application to access it.*

QCS does not operate an administrative access arrangement. It explained that the majority of formal access applications for information are about prisoner documentation. QCS considers that this information is not suitable for administrative access because it often contains information about either other prisoners or victims. Disclosing it could impact the safety of the correctional centre, other prisoners and QCS staff.

QCS does however promote administrative release ahead of formal applications. On its RTI webpage it encourages the public to contact the department if they cannot find the information on the website.

Recommendation 7
We recommend that within 18 months the Department of Employment, Small Business and Training and the Department of State Development, Infrastructure, Local Government and Planning list their administrative access arrangements on their RTI webpage.

Published information asset register

In previous audits we have recommended agencies publish a version of their information asset register on their website. By publishing its information asset register, or a version of it, an agency informs the community about the information it holds. This can also assist community members focus their requests for information, leading to increased efficiency, openness and transparency.

The three audited departments do not publish their information asset register, or a redacted version of it. DESBT and QCS advised they are working towards publishing a version of their register for OFFICIAL information assets.

In July 2022 we scanned the websites of the 20 Queensland government departments. We found that only 2 departments publish a version of their current information asset register:

- Department of Education[51]
- Queensland Police Service.[52]

Agencies other than departments also publish their information asset register, for example the Inspector-General Emergency Management, Queensland University of Technology, Gold Coast Hospital and Health Service and Townsville City Council.

Recommendation 8

We recommend that within 18 months the Department of Employment, Small Business and Training, the Department of State Development, Infrastructure, Local Government and Planning and Queensland Corrective Services publish their information asset register, or a version of it, on their websites.

Recommendation 9

We recommend that all government agencies publish their information asset register, or a version of it, on their websites.

51 Department of Education website: https://ged.qld.gov.au/about-us/rti/publication-scheme/our-lists
52 Queensland Police Service website: https://www.police.qld.gov.au/rights-information/information-asset-register

5 Appendices

Appendix 1 – Agency responses

Appendix 2 – Maturity of information management legend

Appendix 3 – Audit methodology

5.1 Appendix 1 – Agencies responses and action plans

Department of Employment, Small Business and Training

Queensland Government

Department of Employment, Small Business and Training

Our ref: 00710/23

Ms Rachael Rangihaeata
Information Commissioner
Email: audit@oic.qld.gov.au

Dear Ms Rangihaeata Rachael

Thank you for your letter dated 8 March 2023 regarding the Publishing OFFICIAL Information Assets audit.

I acknowledge the receipt of the proposed report and accept its recommendations in full. The Department of Employment, Small Business and Training is committed to the proactive disclosure of information assets and will monitor implementation of the report's recommendations.

I wish to inform you that the Department has commenced work on the recommendations contained in the report and has assigned responsibility for recording information assets in its register to the Director of Information and Digital Services under Recommendation 1.

As requested, I have enclosed an action plan detailing remediation work and accompanying timeframes.

Should you require any further information, please contact Mr Chris McCormack, Acting Chief Information Officer, Corporate ICT, Department of Employment, Small Business and Training by email at chris.mccormack@desbt.qld.gov.au or on telephone [redacted].

Yours sincerely

Warwick Agnew
Director-General

14/3/'23

Enc: Action Plan - DESBT

1 William Street Brisbane
Queensland 4000 Australia
PO Box 15483 City East
Queensland 4002 Australia

ABN 84 375 484 963

Action plan – Department of Employment, Small Business and Training

We recommend the agency:		Department of Employment, Small Business and Training
No.	**Recommendation**	
1	within 6 months assigns responsibility for recording the information assets in its register.	**Response**: Accepted
		Proposed management action: Director, Information and Digital Services has been assigned responsibility to record information assets in the register
		Nominated owner: Director, Information and Digital Services
		Nominated completion date: 31 August 2023
2	within 18 months records all its information assets in its register.	**Response**: Accepted
		Proposed management action: Identify and list all known assets
		Nominated owner: Director, Information and Digital Services
		Nominated completion date: 31 August 2024
3	within 18 months records in its register the asset constraints for all its information assets.	**Response**: Accepted
		Proposed management action: Record asset constraints in the register
		Nominated owner: Director, Information and Digital Services
		Nominated completion date: 31 August 2024
5	within 18 months establishes a process to regularly review the security classification of the OFFICIAL information assets recorded in its register, and whether the associated security controls remain appropriate.	**Response**: Accepted
		Proposed management action: Establish process and implement review
		Nominated owner: Director, Information and Digital Services, DESBT
		Nominated completion date: 31 August 2024
6	within 12 months incorporates considering the information	**Response**: Accepted

We recommend the agency:		Department of Employment, Small Business and Training
No.	**Recommendation**	
	security classification labels of information assets into its procedure for assessing whether the assets are suitable for publication or release.	**Proposed management action**: Review information classification labels and suitability for publication and release
		Nominated owner: Director, Information and Digital Services, DESBT
		Nominated completion date: 28 February 2024
7	within 18 months lists its administrative access arrangements on its RTI webpage.	**Response**: Accepted
		Proposed management action: List administrative access arrangements on its RTI webpage
		Nominated owner: Chief Legal Counsel, DESBT
		Nominated completion date: 31 August 2024
8	within 18 months publishes its information asset register, or a version of it, on its website.	**Response**: Accepted
		Proposed management action: Publish Information Asset Register on the DESBT internet site
		Nominated owner: Director, Information and Digital Services, DESBT
		Nominated completion date: 31 August 2024

Queensland Corrective Services

Queensland Government

Ref: QCS-01082-2023

Office of the
Commissioner

Queensland
Corrective Services

14 MAR 2023

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner
audit@oic.qld.gov.au

Dear Ms Rangihaeata

I refer to your email of 8 March 2023 about publishing OFFICIAL information assets and the attached *Supporting the push model through proactive disclosure* audit report.

I can advise that Queensland Corrective Services accepts each of the three recommendations that are relevant to our agency, and attached is a completed action plan with responses outlining how the agency will be acting on the recommendations.

If you require further information regarding this matter, please contact Ms Janne Ward, Manager, Information Management Unit, Digital Services and Information Technology Branch on [redacted] or at janne.ward@corrections.qld.gov.au.

Yours sincerely

Paul Stewart APM
Commissioner

Enc.

QCS Headquarters
L21Northbank Plaza
69 Ann Street Brisbane
GPO Box 1054 Brisbane
Queensland 4001 Australia
Telephone +61 7 3565 7675
ABN 61 993 700 400

OFFICIAL

Action plan – Queensland Corrective Services

We recommend the agency:		Queensland Corrective Services
No.	**Recommendation**	
3	within 18 months records in its register the asset constraints for all its information assets.	**Response**: QCS has commenced recording the constraints for information assets in the agencies Information Asset Register (IAR).
		Proposed management action: The QCS Information Management Unit is currently implementing this recommendation. QCS has added the following fields for asset constraints in the IAR: 1. Access constraints 2. Use constraints 3. Restricted access rights Information Assets classified as SENSITIVE and PROTECTED have been updated, and the assets classified 'OFFICIAL' will be updated to the relevant access constraint according to the OIC recommendations.
		Nominated owner: Debbie Gallagher, Director, Strategy and Business Services, Digital Services and Information Technology Command
		Nominated completion date: Completed December 2023
5	within 18 months establishes a process to regularly review the security classification of the OFFICIAL information assets recorded in its register, and whether the associated security controls remain appropriate.	**Response:** QCS Information Assets and their security classification are reviewed annually as part of the ICT Profile Standard requirements and will include an assessment to ensure the associated controls are appropriate.
		Proposed management action: QCS reviews its IAR for the high business impact information assets as part of its annual reporting obligations under IS18 and the ICT Profiling Standard. Information management staff coordinate this process with data managers and custodians. QCS will implement a process to regularly review system controls for information assets that are recorded in the IAR. This will ensure the associated controls provide sufficient safeguards to adequately protect the information based on the confidentiality level of the information, and that they comply with

We recommend the agency:		Queensland Corrective Services
No.	**Recommendation**	
		the Queensland Government Information Security Classification Framework (QGISF). "An agency must apply security controls which are commensurate with the assessed business impact. The framework does not mandate specific controls - agencies should select the controls best suited to their business and technology needs. The chosen controls must provide sufficient safeguards to adequately protect the information based on the confidentiality level of the information."
		Nominated owner: Debbie Gallagher, Director, Strategy and Business Services, Digital Services and Information Technology Command
		Nominated completion date: June 2024
8	within 18 months publishes its information asset register, or a version of it, on its website.	**Response:** A redacted version of the QCS IAR is being prepared for publishing on the department's website. The publishing of this register will ensure the agency meets the Office of the Information Commission requirements to the below findings: • Publishing established information asset registers, or a version of them, can also provide assurance that agencies are maximising disclosure. • Proactive disclosure of maximum OFFICIAL information assets demonstrates a commitment to openness, accountability and transparency and builds trust.
		Proposed management action: QCS will publish a register of 'official' information assets on the department's website. The register will be published this financial year, however this is currently delayed due to security issues on the web platform.
		Nominated owner: Debbie Gallagher, Director, Strategy and Business Services, Digital Services and Information Technology Command
		Nominated completion date: June 2023

Department of State Development, Infrastructure, Local Government and Planning

Departmentof
State Development, Infrastructure, Local Government and Planning

Our ref: DGC23/181

17 March 2023

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner
audit@oic.qld.gov.au

Dear Ms Rangihaeata

Thank you for your email of 8 March 2023 about the Office of the Information Commissioner Audit into publishing official information assets which supports the push model through proactive disclosure.

The department accepts the recommendations in the final report, and notes it is to be tabled in Parliament this month.

Attached is the department's action plan to address each of these recommendations.

If you require any further information, please contact Kate Felsman, Director, Information, ICT Governance and Risk, Information and Technology Services, Corporate in the Department of State Development, Infrastructure , Local Government and Planning, by telephone on [redacted], or by email at Kate.Felsman@dsdilgpqld.gov.au, who will be pleased to assist.

Yours sincerely

Michael McKee
Deputy Director-General
Corporate

Enc: (1)

1 Willi am Street
Brisbane Queensland 4000
PO Box 15009
City East Queensland 4002
Telephone 13 QGOV (13 74 68)
Website www.statedevelopment. ql d.gov.au
ABN 29 230 178 530

Action plan – Department of State Development, Infrastructure, Local Government and Planning

We recommend the agency:		Department of State Development, Infrastructure, Local Government and Planning
No.	**Recommendation**	
2	within 18 months records all its information assets in its register.	**Response**: Agree
		Proposed management action: Uplift the current Information Asset Register (IAR) and identify any gaps in assets and missing asset information.
		Nominated owner: Craig Vandermeer, Chief Information Officer (CIO), Information and Technology Services (ITS), Corporate
		Nominated completion date: September 2024
3	within 18 months records in its register the asset constraints for all its information assets.	**Response**: Agree
		Proposed management action: The asset constraints for all information assets will be updated in the IAR.
		Nominated owner: Craig Vandermeer, CIO, ITS, Corporate
		Nominated completion date: September 2024
4	within 18 months makes its information asset register available to all staff.	**Response**: Agree
		Proposed management action: The IAR will be published to all staff on the department's intranet.
		Nominated owner: Craig Vandermeer, CIO, ITS, Corporate
		Nominated completion date: September 2024
7	within 18 months lists its administrative access arrangements on its RTI webpage.	**Response**: Agree
		Proposed management action: The RTI section of the DSDILGP website will be updated to include administrative access arrangements.
		Nominated owner: Craig Vandermeer, CIO, ITS, Corporate

We recommend the agency:		Department of State Development, Infrastructure, Local Government and Planning
No.	**Recommendation**	
		Nominated completion date: September 2024
8	within 18 months publishes its information asset register, or a version of it, on its website.	**Response**: Agree
		Proposed management action: A redacted version of the IAR will be published to the department's website.
		Nominated owner: Craig Vandermeer, CIO, ITS, Corporate
		Nominated completion date: September 2024

5.2 Appendix 2 – Maturity of information management legend

	Information asset register	Custodianship	Classification
Unmanaged	We have few processes to identify and register information assets. We have informal arrangements to manage some business-critical information assets. We leave strategic, high value or high-risk information assets unmanaged (unclassified, unregistered in the information asset register and unassigned to an information custodian etc.).	We have informal arrangements for custodians for some information assets. We have no formal custodianship policy or defined roles and responsibilities for custodians.	We have few processes to classify information assets.
Ad hoc	Our information asset register may be missing strategic information assets. We need to review and update our information asset register. We make our information asset register(s) available to relevant staff in some business units.	We have a custodianship policy but we have not implemented it across the department. We inconsistently define and communicate information ownership and custodianship responsibilities.	We have some processes for classifying our information assets but staff do not apply them consistently to all relevant information assets.
Defined	We have an approved information asset register(s), which we have mandated across the department. The information asset register includes all our strategic information assets but is missing most other assets. It provides key context for some information assets.	We assign staff to information assets. They fulfil their roles and responsibilities across the department. We have an approved custodianship policy and have mandated it. Custodians use our defined processes to track and manage information assets over their lifecycle.	Staff follow our mandated processes for classifying information assets.

	Information asset register	Custodianship	Classification
Managed	The information asset register includes most information assets under our control. We update our approved information asset register on at least an annual basis. We follow our defined processes to identify and manage additional information assets. Our register(s) is single source of truth.	Our custodianship model meets departmental needs and is in line with QGEA guidelines. Custodians understand their responsibilities and register and maintain information assets through their lifecycle. We assign custodians for both existing and new information assets.	We monitor the quality of information asset classification and have a process to address quality issues. We are using ongoing revision and improved classification of information assets to benefit our information planning.
Proactive	The information asset register includes all information assets under our control including key context for each information asset. We use the register(s) as the primary internal source for information provision and services. We publish a public version of our information asset register. We use our register(s) to shape information management planning initiatives.	Custodians understand their responsibilities and register and maintain information assets through their lifecycle. We assign custodians for both existing and new information assets. Custodians have appropriate business experience and understanding. Custodians work actively with information users to improve usability, sharing and the identification and management of information assets.	We have evidence of improved information service provision, information planning and risk reduction. We consider information asset classification when developing new information systems and products.

Source: Maturity of information management self-assessment[53]

53 Available on OIC website

5.3 Appendix 3 – Audit methodology

We thank the staff of the audited departments for their support and cooperation.

Mandate

We conducted this audit under section 131 of the *Right to Information Act 2009*. We applied our Assurance Engagement Methodology,[54] based on the standards set by the Australian Auditing and Assurance Standards Board.

Audit objective

The objective of the audit was to determine whether departments have systems in place that support the push model through maximum disclosure of OFFICIAL information assets.

We used the following criteria:

Lines of inquiry	Criteria
1. The department identifies and classifies its information assets.	1.1 The department identifies and registers its information assets. 1.2 The department publishes a version of its information asset register.
2. The department makes its OFFICIAL information assets available to the maximum extent possible.	2.1 The department has systems in place to approve OFFICIAL information for public disclosure. 2.2 The department maximises the disclosure of OFFICIAL information assets. 2.3 The department makes it easy to access available OFFICIAL information assets.

Audit scope

The audit examined three government departments:

- the Department of Employment, Small Business and Training
- the Department of State Development, Infrastructure and Local Government and Planning
- Queensland Corrective Services.

The audit examined the confidentiality element of the information security classification framework. The audit did not examine whether

- the confidentiality classification or the related controls were appropriate for each information asset

54 Available on our website www.oic.qld.gov.au

- the integrity and availability elements of the information security classification framework
- the register was complete and accurate
- the department was disposing information in accordance with its security value.

Audit process

The audit team worked with agency officers dealing with identification, classification, management and release of OFFICIAL information, and with information asset registers. It gathered sufficient, appropriate evidence through:

- document review, including internal policies and procedures, risk assessments, registers and other relevant documentation
- system walk through
- interviews with relevant staff and management.