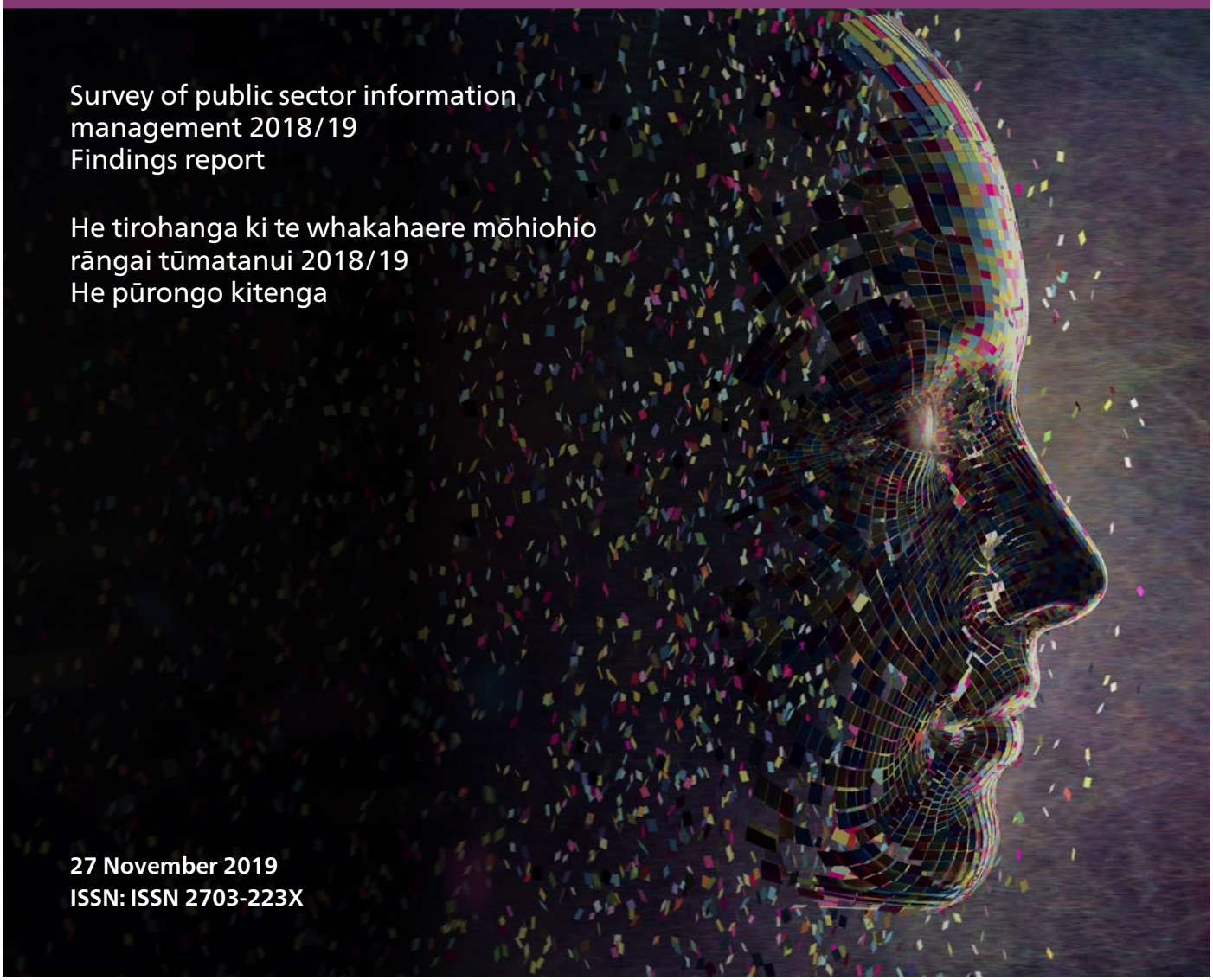
Kia pono ai te Rua Mahara o te Kāwanatanga

Enabling trusted government information

Ko te ahuatanga o Te Rua Mahara o te Kāwanatanga



Survey of public sector information management 2018/19
Findings report

He tirohanga ki te whakahaere mōhiohio rāngai tūmatanui 2018/19
He pūrongo kitenga

27 November 2019
ISSN: ISSN 2703-223X

Te Rua Mahara o te Kāwanatanga
ARCHIVES NEW ZEALAND

New Zealand Government

Contents

1.0 Overview

Purpose

Information is fundamental to open, transparent and accountable government. The Public Records Act 2005 (PRA) exists to enable government accountability.

With this report and its recommendations, Archives New Zealand Te Rua Mahara o te Kāwanatanga wants to improve leadership teams' and decision makers' understanding of the value of information management (IM), and why it matters. We want to support them to make informed decisions on IM programmes so they can measure the value of this investment in the short and long term.

We also aim to support IM practitioners to create a better connection between IM operations and their organisation's strategic framework and communicate benefits effectively.

This findings report has three objectives:

- to illustrate organisations' IM programmes and approaches;
- to provide recommendations that Executive Sponsors and IM practitioners can use to continually improve their IM programmes; and
- to promote best practice IM across the public sector.

The report starts with a section focusing on what we wanted to highlight this year, because of its relevance in the current context or because of its importance. The 'Focus' section provides recommendations, while the other sections offer observations. The second section highlights the results that reflect the current environment in which IM evolves. The next three sections present the findings in high-level groupings (Governance, Systems and Disposal), establishing connections between the questions and the sections, and following the information lifecycle.

Survey objectives

The overarching goal of the survey was to collect quantitative and qualitative data about IM practices in the New Zealand public sector, i.e public offices and local authorities. This will provide a baseline of data for comparison in the coming years. By repeating this survey regularly, we will develop longitudinal data and knowledge about how practices evolve.

The survey and its results will:

- provide a whole-of-system view of IM in the public sector;
- be able to be used by organisations as a self-assessment to benchmark their IM performance;
- feed back into our ongoing monitoring and reporting activities; and
- enable us to identify potential improvements in advice, guidance and education, and plan service delivery.

Survey methodology

The survey was designed and delivered by our Government Recordkeeping Directorate, with the assistance of an internal reference group made up of our principal and senior advisors and specialist analytics and reporting staff from the wider Department of Internal Affairs. A group of Executive Sponsors and IM staff from public offices and local authorities tested the draft survey. The survey was delivered through the online survey tool, SurveyMonkey.

We sent the survey to public offices and local authorities. Executive Sponsors at those organisations received the email link to access the survey and were expected to collaborate with their relevant staff to form the response. The response was mandatory for all public offices as a direction to report to the Chief Archivist under section 31 of the PRA, but was not mandatory for local authorities.

The survey questions were based on the requirements of the *PRA* and the *Information and records management standard* (the IRM standard). The questionnaire can be found on our website *(Link to PDF)*.

Organisations surveyed

254 organisations were surveyed:

- 176 public offices (POs)
- 78 local authorities (LAs).

The 2019 survey did not include all of the entities covered by the PRA; notably school boards of trustees, Ministers, council-controlled organisations, council-controlled trading organisations and local government organisations. Options for expanding the survey coverage will be considered in the coming years.

Response rates

We recorded 228 responses, making the overall response rate of nearly 90%. Of public offices, 168 responded (95% response rate), as did 60 local authorities (77% response rate). Each chart indicates the number of responses (as in N=226). A list of respondents/non-respondents is available at *Appendix 1.* The Government Communications Security Bureau and New Zealand Security Intelligence Service responses are not included in the analysis and results publication.

Open Government Partnership New Zealand – Third National Action Plan 2018-2020

Archives New Zealand is leading Commitment 10 of New Zealand's Third National Action Plan under the Open Government Partnership. This commitment supports trust in government by developing a new approach to monitoring and publicising how well government is managing information. The survey aligns with the objective of Commitment 10 by providing us with better insight into public offices' IM practices. This will enable us to make the management of government information more visible and transparent to the New Zealand public, supporting the Open Government Partnership values of transparency and accountability.

Dataset

The survey results are published as a dataset and available on *data.govt.nz* as a companion to this report.

Report on the State of Government Recordkeeping

As part of the survey design, we selected five key indicators to measure the overall state of government IM and provide a high-level perspective on whether IM within the public sector was improving, deteriorating or remaining stable. This high-level summary is included in the *Report on the State of Government Recordkeeping 2018/19.* The five key indicators cover: governance; resourcing; high value and/or high risk information; building IM requirements into business systems; and active, authorised destruction of information.

Note on the treatment of "other" responses

The survey question picklists were designed from our knowledge of the sector. We tried to limit the number of options to the six we thought relevant to most organisations.

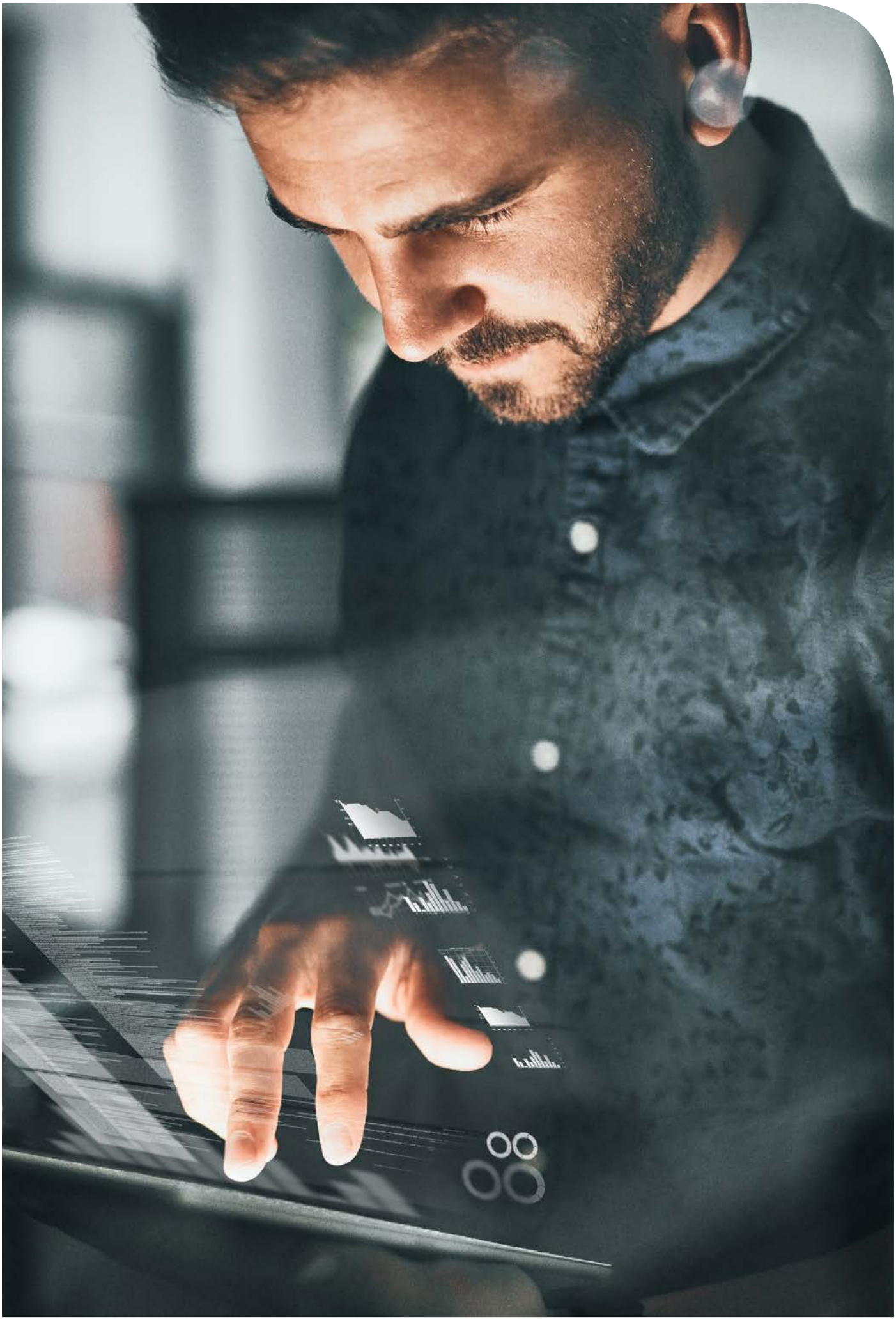
For many questions, we also offered an 'others' option, and provided a free text field. We identified through the analysis that some of the free text responses were not relevant to the questions. For this reason, the charts throughout this report exclude the 'others' option and because these comments are available in full on *data.govt.nz.*

Abbreviations, initialisations and definitions

For ease of reading, we have used the following:

- **IAR –** information asset register
- **IM –** information management
- **IRM standard –** Information and records management standard
- **LAs –** local authorities
- **PRA –** Public Records Act 2005
- **POs –** public offices

Key definitions can be found on the *Archives New Zealand website.*



2.0

Focus

This Focus section summarises key findings for three survey areas we wish to highlight. It provides recommendations for IM professionals and Executive Sponsors and their organisations. The recommendations will help organisations develop action plans to improve their IM practices.

Self-monitoring

What we asked and why it is important

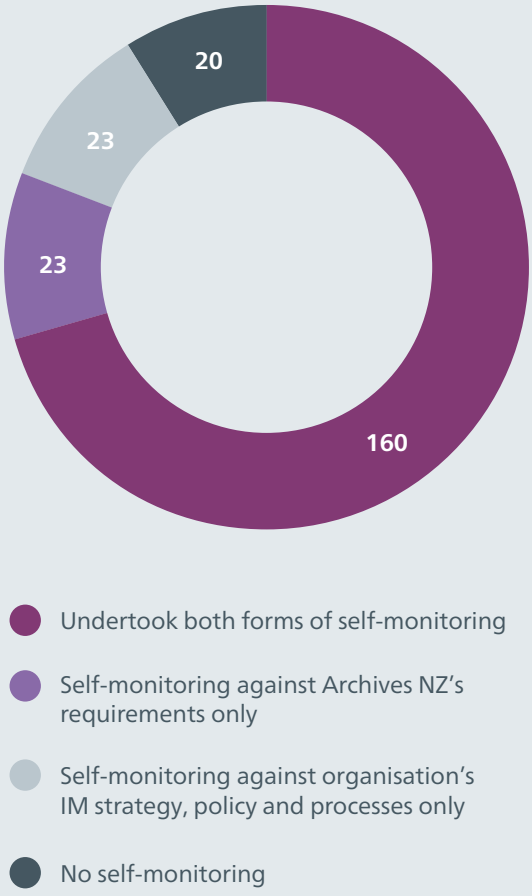
We asked about two types of self-monitoring – assessment against our requirements and standards, and assessment against the organisation's IM strategies, policies and procedures (Q.12 and Q.13). For organisations doing self-monitoring, we also asked what they do with the findings and recommendations (Q.14).

Self-monitoring is a crucial part of establishing a governance framework for IM and part of organisations' responsibilities as a public sector organisation.

Findings

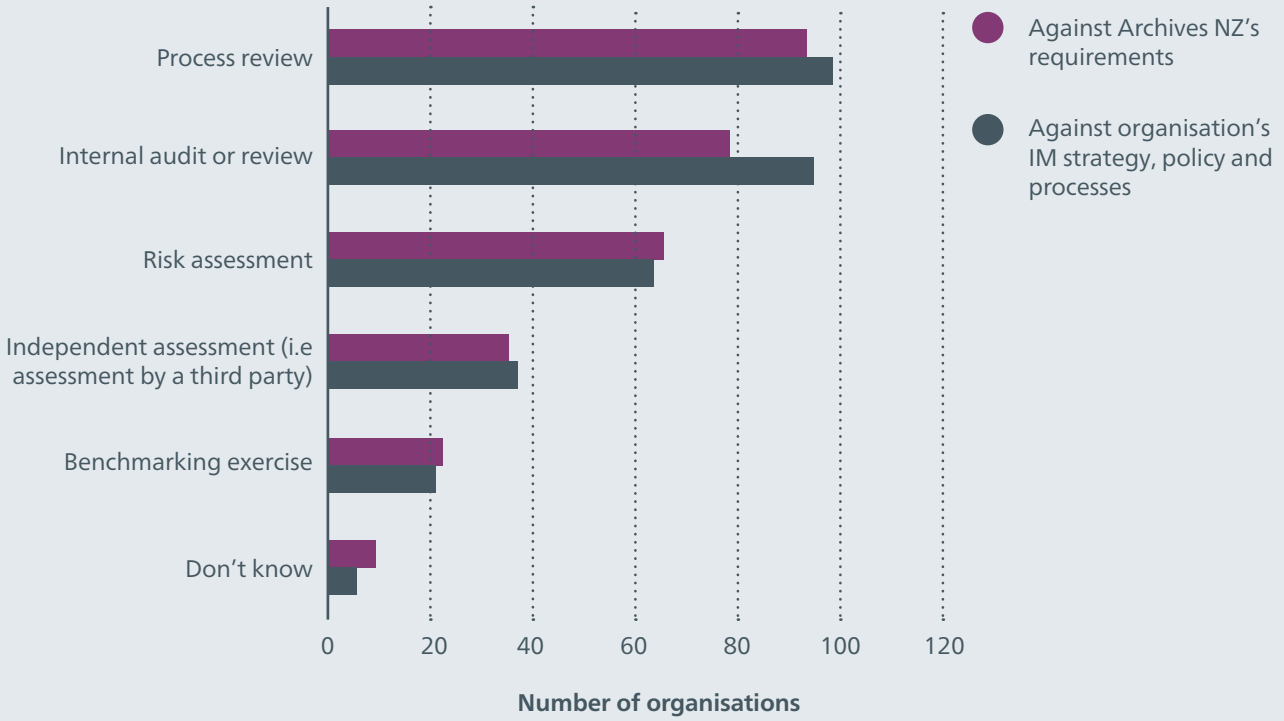
Figure 1 shows the extent to which the organisations did some monitoring. We see that almost three-quarters of the organisations do both types of monitoring. In total, 206 organisations (91%) did some form of self-monitoring. Only 20 (9%) organisations said they did no self-monitoring of either type.

Figure 1: Self-monitoring undertaken by organisations (N=226)



As Figure 2 shows, of those organisations that have done self-monitoring, the two activities undertaken most often were *process review* and *internal audit or review.* There are similar patterns of activity for the two types of self-monitoring.

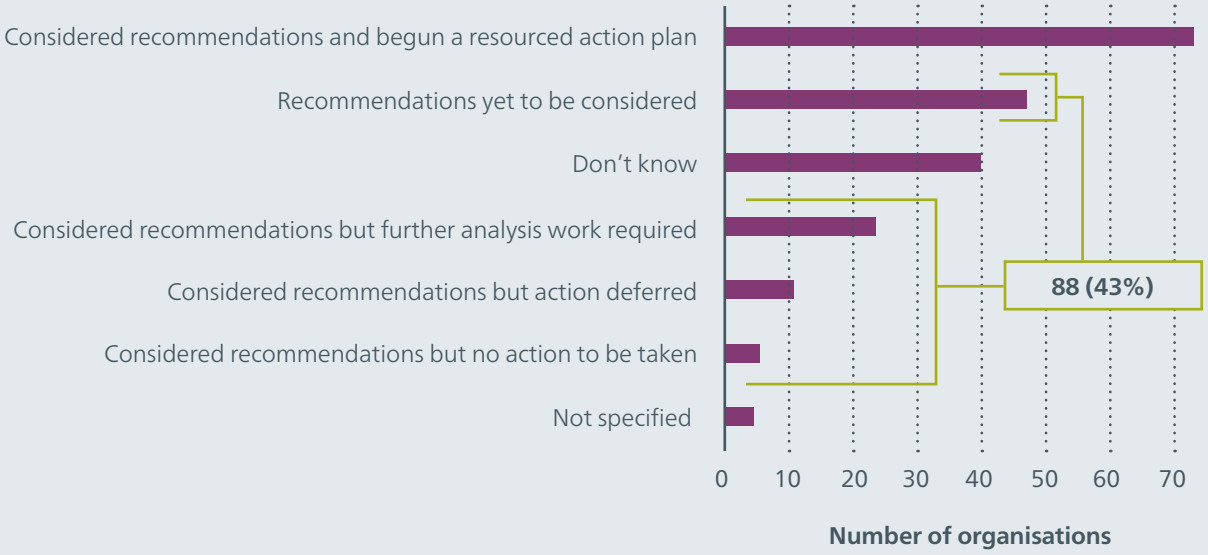
Figure 2: Type of activities undertaken in self-monitoring (N=206)



A few organisations mentioned they undertake a regular compliance assessment, including compliance with the PRA utilising ComplyWith (a legal compliance management tool), as well as a 'Data Management Maturity Assessment'. Additional comments show that some organisations have not grasped the meaning and importance of self-monitoring.

When asked what the Executive Leadership Team and/or the IM Governance Group did with the findings from self-monitoring activities, only 73 (35%) of the 206 organisations undertaking self-monitoring said they had considered the recommendations and had begun a resourced action plan. As Figure 3 shows, a greater number (88, or 43%) were either yet to consider the recommendations, yet to start taking action, had deferred action, or had more action to take. It is concerning that the third most frequent response (40 organisations, or 19%) was they did not know what had been done with their self-monitoring findings. It is possible some of those organisations answering 'don't know' were actually indicating they did not know whether any self-monitoring had been done.

Figure 3: What organisations have done with the findings from self-monitoring (N=206)



Note: "Not specified" in the chart above represents categories of responses where we received ambiguous responses inconsistent with responses to the two previous questions.

Recommendations

Self-monitoring and assurance processes support effective IM and help to raise awareness across an organisation about the importance of information and its appropriate management.

Every organisation should:

- monitor their IM activities and undertake system and process audits on a regular basis;
- document the findings to clearly identify recommendations and actions;
- act on those recommendations, taking corrective actions and addressing non-compliance issues to guarantee their IM is in line with the organisation's needs and strategic direction; and
- monitor the outcomes of those recommendations and the benefits realised.

High value and/or high risk information

What we asked and why it is important

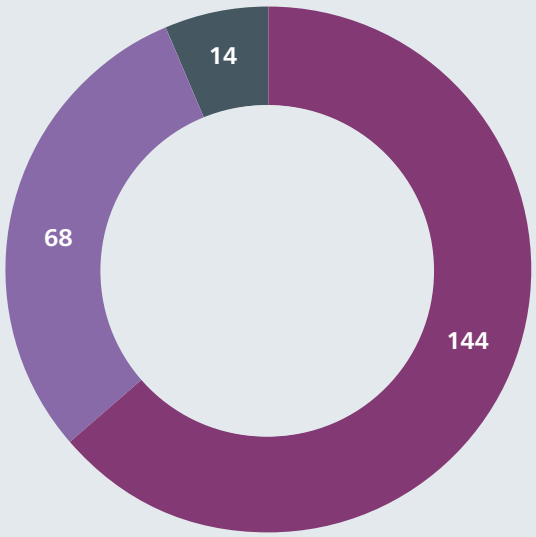
We asked whether organisations had identified their high value and/or high risk information (Q.20) and, if they had, what activities they had undertaken in the past 12 months to actively manage this information (Q.21).

How organisations define high value and/or high risk information will depend on the organisation's business. It will include the information needed to carry out core functions, to make key decisions, and to provide future evidence of decision-making, policies and activities. It will also encompass information relating to the people of New Zealand and their rights and entitlements, and information relating to land, infrastructure and research. Protecting these information assets is critical for open, accountable and transparent government.

Findings

Overall, the majority of organisations (144, or 64%) have identified their high value and/or high risk information as shown in Figure 4. Figure 5 shows that when comparing POs with LAs, the findings are different. Half (30) of LAs said they had not identified their high value and/or high risk information, whereas public offices did a lot better, with approximately a quarter (38, or 23%) having not identified their high value and/or high risk information.

Figure 4: Whether organisations have identified their high value and/or high risk information (N=226)



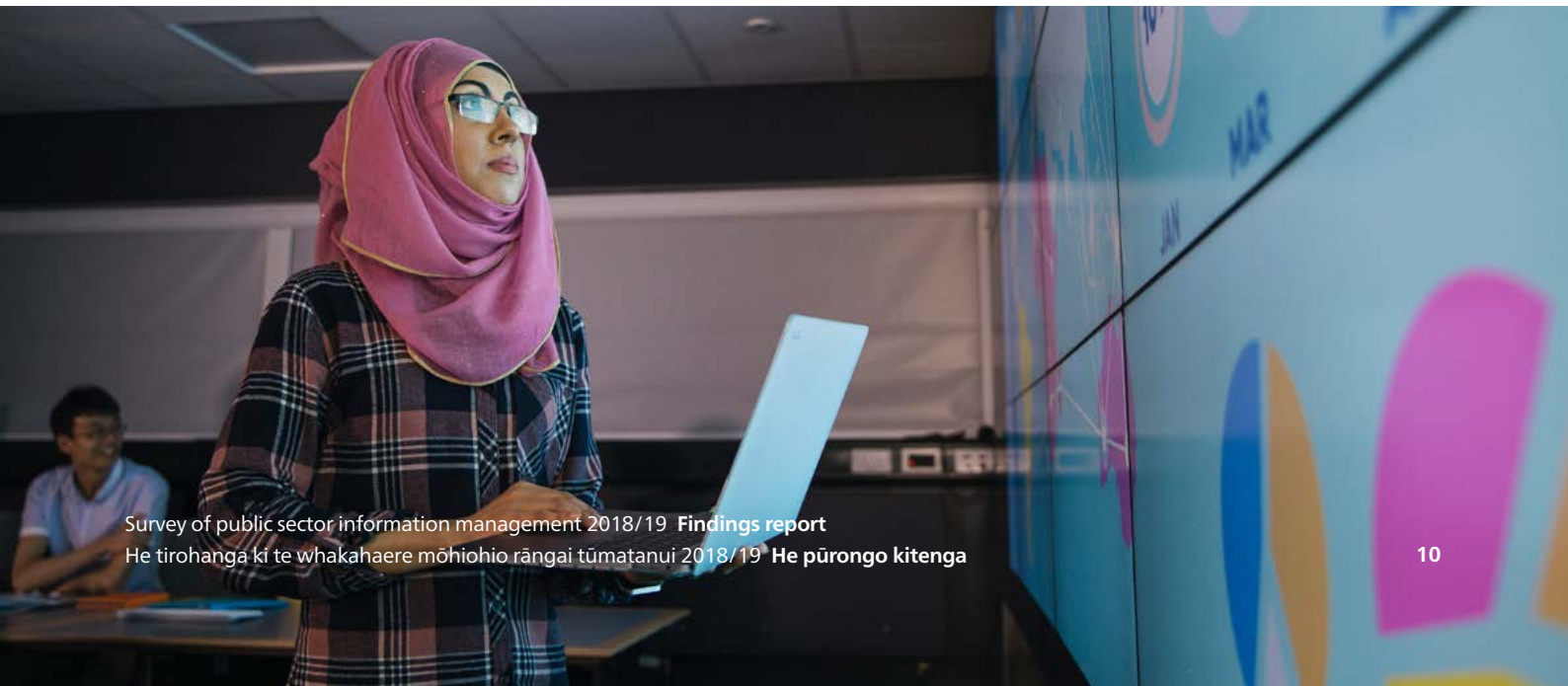
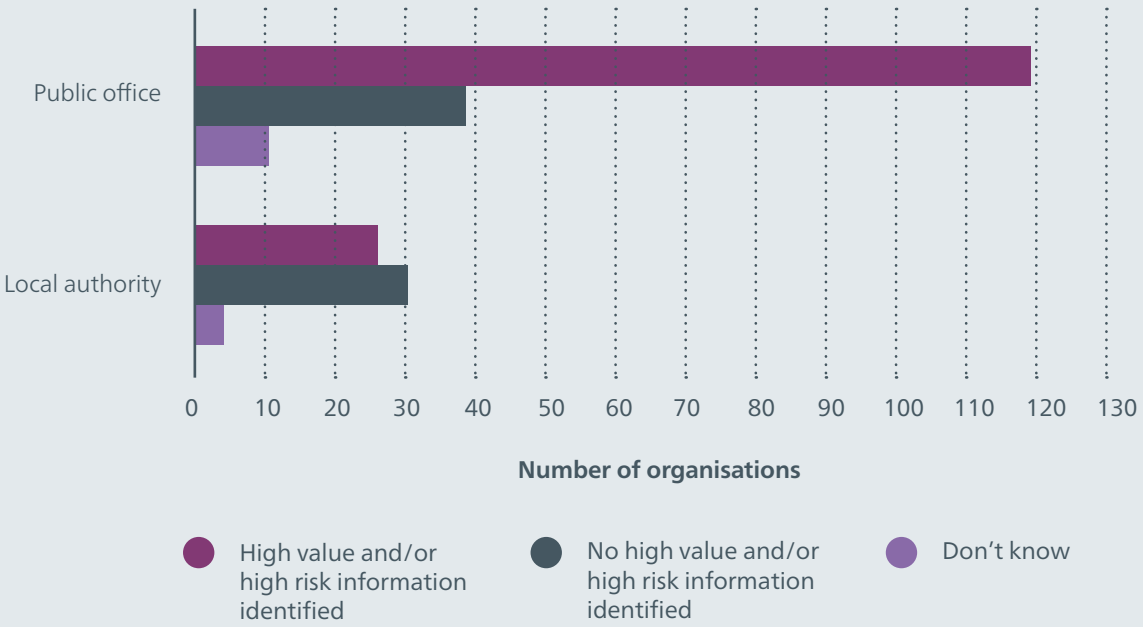
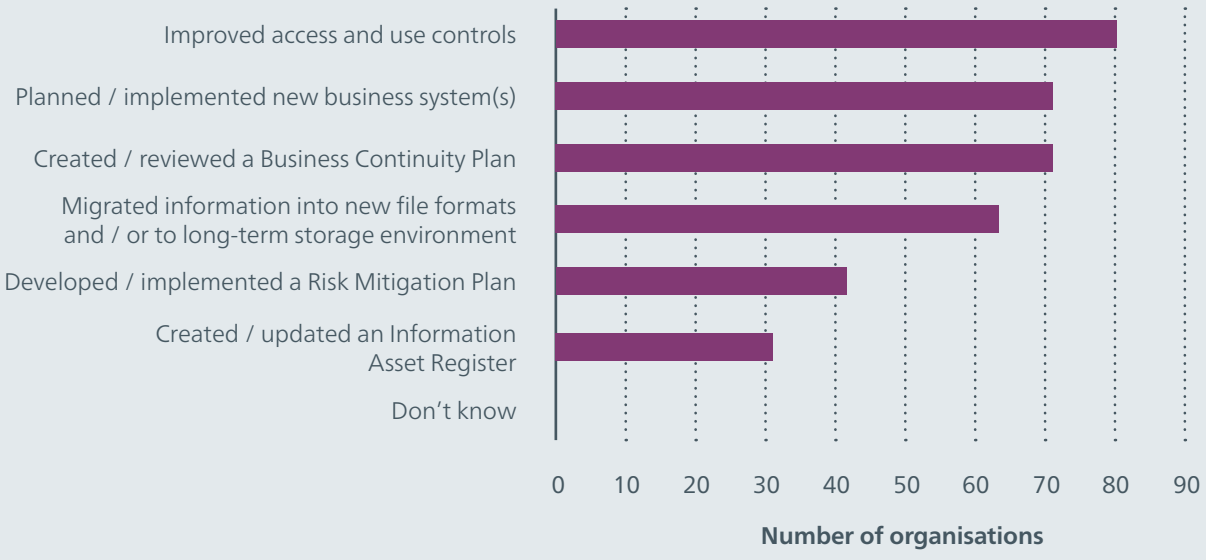


Figure 5: Whether organisations have identified their high value and/or high risk information, by type of organisation (N=226)



Among the 144 organisations that have identified their high value and/or high risk information, 136 (94%) had undertaken activities in the past 12 months to actively manage this information. The activities are shown in Figure 6, along with the number of organisations that undertook each activity.

Figure 6: Activities undertaken to manage the organisation's high value and/or high risk information (N=136)



Recommendations

High value and/or high risk information assets should be clearly identified, and plans put in place to manage them as a priority.

Once an organisation has identified its high value and/or high risk information assets, it should:

- document those assets in an Information Asset Register (IAR) tool, or similar;
- clearly identify the top priority assets and any risks associated with those; and
- build risk mitigation for these information assets into its IM/ Information Communication Technology (ICT) strategies and roadmaps as part of a continuous improvement programme.

Access classification

What we asked and why it is important

We asked how much of each organisation's information over 25 years old had been classified as either 'open' or with 'restricted access' (Q.34).

Knowing the value and risk related to information assets is good IM practice. This also includes the access classification[1]. In support of open and accountable government, organisations have an obligation to ensure public access to information, regardless of where it is held. For information in existence less than 25 years, in current use and in the custody of the organisation, access is usually administered under the Official Information Act 1982, the Local Government Official Information and Meetings Act 1987, and the Privacy Act 1993.

All public records that have been in existence for 25 years or are about to be transferred to the control of the Chief Archivist must be classified as either open or restricted access *(PRA, s.43)*. Similarly, when local authority records become local authority archives, the access classification must be applied *(PRA, s.45).*

1 Classifying access status under the PRA is a different requirement to protecting information using classification and protective markings under national security classifications.

Figure 7: The number of organisations that have classified their information over 25 years old as open or restricted (N=226)

Findings

Forty-six organisations (20%) had classified more than half of their older information as open or restricted. A further 58 organisations (26%) had classified less than half of this type of information. It is a concern that 80 organisations (35%) did not know whether access classifications had been assigned to their organisation's older information.

Recommendations

It is important for accountable and transparent government that information is classified as open unless there are good reasons to restrict it, or restriction is required by other legislation.

Organisations should:

- determine the access classification of information over 25 years old as part of their appraisal process to help manage access from when the information is created, and regardless of format and location;
- periodically review the access status of records held in any repositories; and
- facilitate public inspection of open access records, as required by the PRA.

3.0

IM Environment

This section looks at overarching drivers and challenges for IM across government. It also looks at how organisations transition from paper to digital business processes, and how much they preserve the integrity of the information when responding to organisational changes.

Drivers for IM

What we asked and why it is important

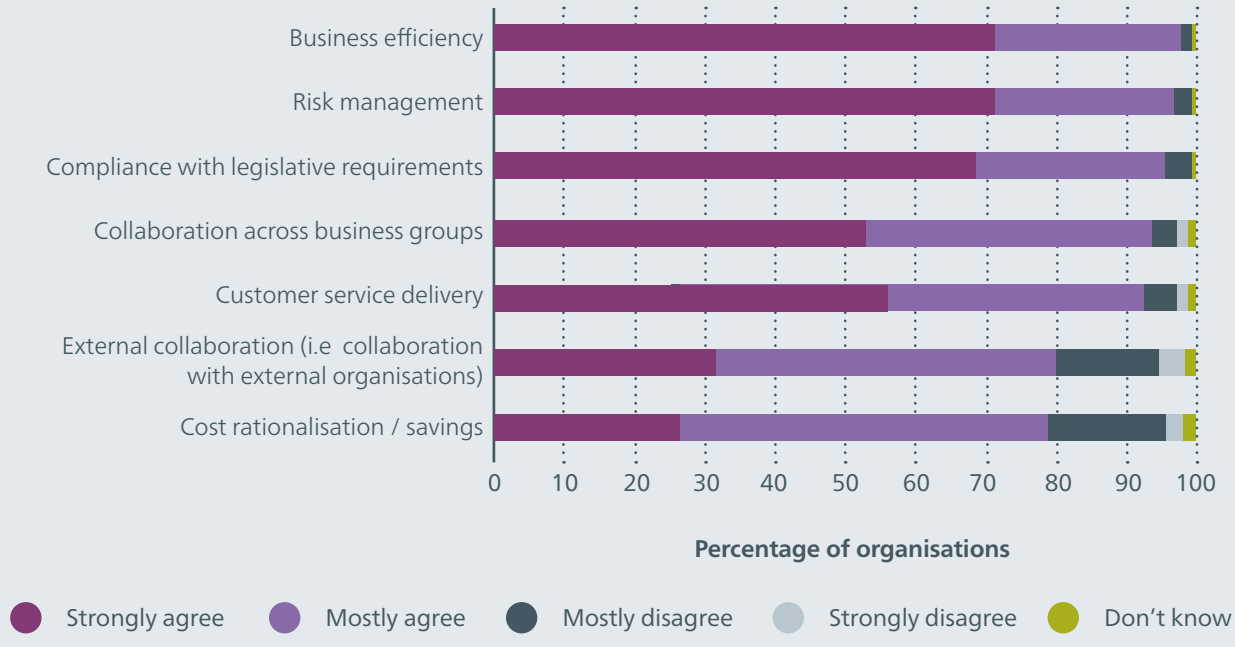
We wanted to understand the drivers for good IM practice and processes within the public sector and what benefits are expected from effective and efficient management of information (Q.6).

Effective IM enables good business practices in the present and in the future. Organisations can then ensure they have meaningful, reliable and usable information available when their business needs it. The mechanisms for ensuring accountability and managing risk can be based on sound IM practices.

Findings

Most of the drivers for good IM that were available as picklist options were relevant to those organisations who responded (Figure 8). Other drivers listed in the 'other(s)' category included staff satisfaction and organisational effectiveness.

Figure 8: Drivers for good IM (N=226)



Observations

Organisations should consider why, when business efficiency and risk management are acknowledged as top drivers for IM, more organisations do not place a similar importance on the regular disposal of redundant/obsolete information. Regular disposal of this kind of information provides benefits such as business efficiency, risk management and cost savings, as explained in the *Disposal section.*

IM challenges

What we asked and why it is important

We asked what challenges organisations face so we could understand what barriers exist for good IM (Q.7).

Organisations often face multiple IM challenges at once and, when combined, these challenges may have an overall negative impact on IM. For example, the lack of a high profile for IM in an organisation may trigger a lack of resources directed towards IM and training users. Another example is that the volume of information, combined with the diversity of formats and legacies from the past, creates challenges for IM staff and end users.

Understanding the challenges specific to an organisation will inform which topics to focus on for discussion between Executive Sponsor and IM staff, and what to bring to the leadership team table.

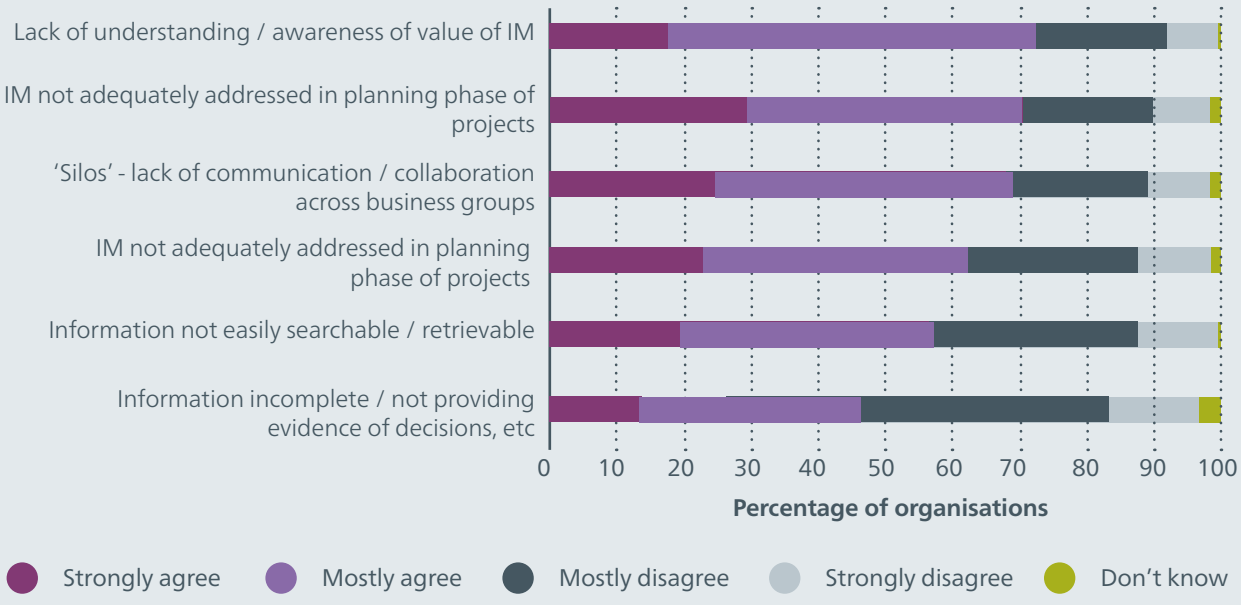
Findings

Most of the challenges listed in the picklist are applicable to all organisations who responded (Figure 9). Only one challenge, *'Information incomplete/not providing evidence',* had less than 50% support (from a combined total of 'mostly' and 'strongly agree').

Other challenges mentioned by respondents in the 'other(s)' category include:

- roll-out of Office 365
- transition to digital
- lack of awareness/technology literacy amongst users
- shadow IT and alternative tools.

Figure 9: IM challenges (N=226)



Observations

Management issues, rather than financial considerations, are identified as the biggest challenges to progressing good IM. This could indicate that improvements could still be made even with a lack of adequate funds or resources, though this is still a significant problem. Executive Sponsors could consider how to increase understanding and awareness of the value of IM at the top levels of their organisations to mitigate many of these challenges. A formal IM governance group would be one way to achieve this. Just under half of survey respondents did not have an *IM governance group.*

Transition from paper to digital

What we asked and why it is important

Most organisations have been conducting digitisation activities for some time, as an ongoing routine activity and/or as a one-off back-capture programme. We asked what other activities organisations are doing to transition from paper-based to digital business processes (Q.18). This question was asked in the wider context of digital transformation and the push to have a 'digital by design' approach embedded across the New Zealand public sector.

The value of moving away from ad-hoc digitisation to re-thinking overall processes, procedures and workflows is that organisations will eventually reach the stage where paper is largely no longer needed and routine business processes can be conducted entirely digitally. The transition to digital processes should not lose sight of the requirements of the PRA and IRM standard, and privacy/security considerations.

Findings

From the number of respondents currently undertaking activities to transition to digital business processes (208 in total), 160 organisations are *'Re-designing business processes and services to remove the paper component'* (Figure 10). It is encouraging to see that 130 organisations are also *'introducing digital authorisation and/or approval in business processes'.*

Figure 10: Activities to transition from paper-based to digital business processes (N=208)

Observations

Redesigning business processes to operate in an entirely digital environment can transform the user and customer experience. This can include streamlining IM by automating the application of *metadata*, so its creation is not an imposition on users. The efficiency, effectiveness and customer service gains offered by digital business processes won't be achieved where methods from the paper-based age are retained and applied to a digital setting.

Organisational change and measures to secure and preserve integrity of information

What we asked and why it is important

Administrative and business changes are part of the normal life of the public sector. While change can create opportunities, it also can be disruptive and introduce new risks. We wanted to measure how much organisations guarantee the security and preserve the integrity of the information impacted by those changes (Q.30 and Q.31).

Public sector organisations undergoing change to their administrative functions have responsibilities for the management of the associated information. When a function is disestablished, the organisation responsible for the information must still retain and manage the information until it is due for disposal. Information relating to a function that is being transferred should be transferred with that function. When business changes occur, for example when a system is decommissioned, the information assets impacted must be appropriately managed, retained or disposed of.

Findings

Figure 11 shows the major system, service and business changes organisations have undergone. Implementation of new business systems and migration of information feature as the most common changes.

Figure 11: Organisational changes (N=226)

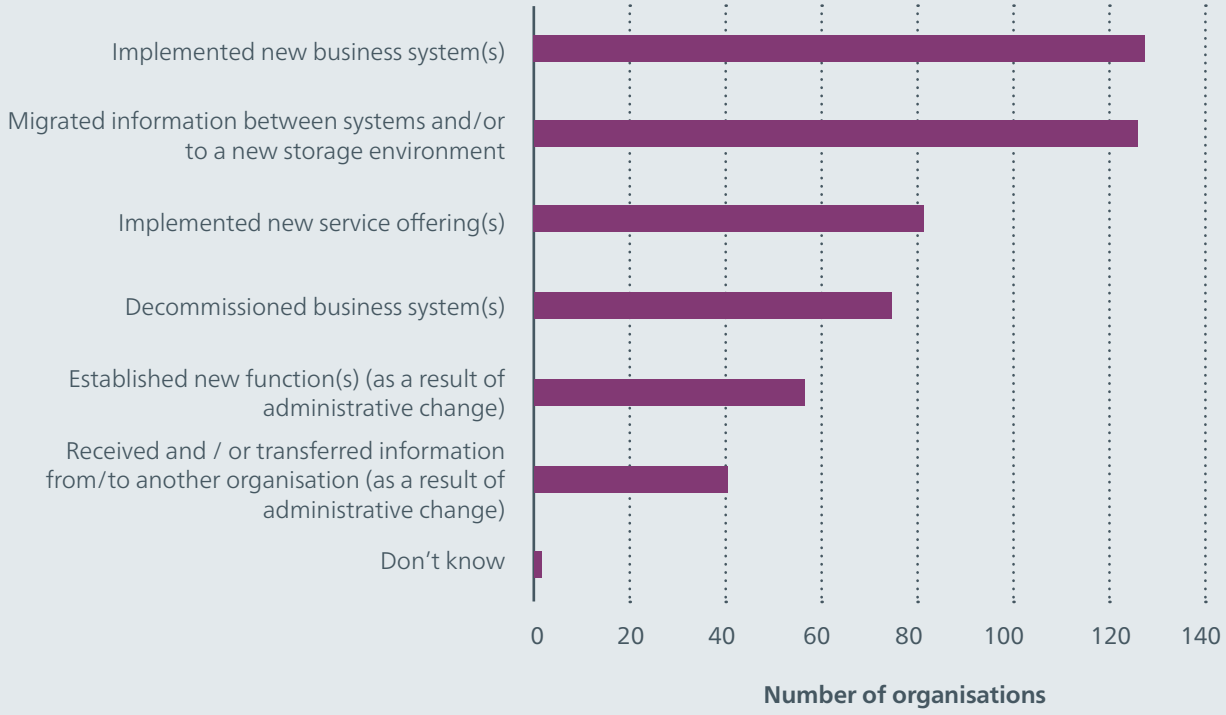
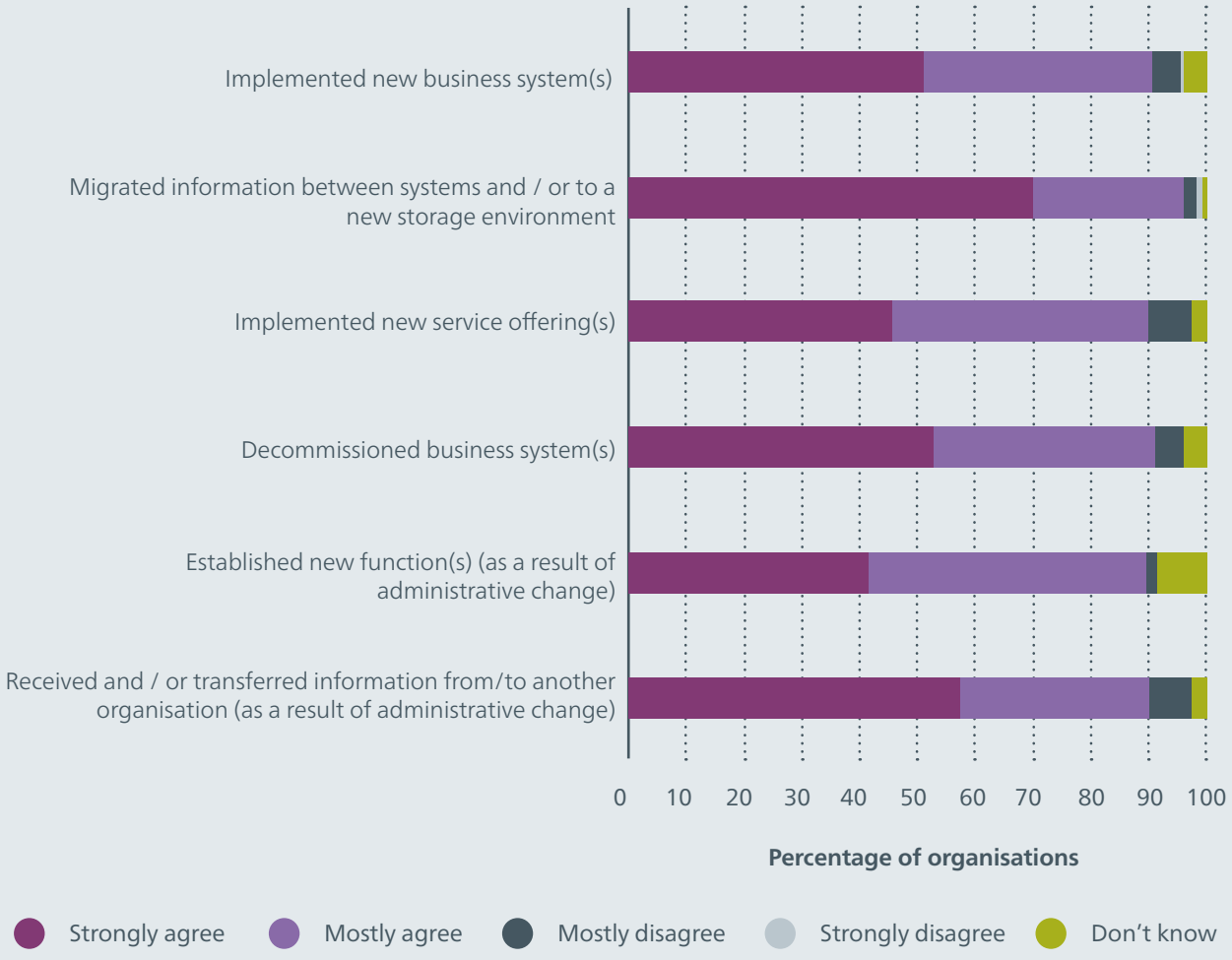


Figure 12 below shows the high percentage of organisations that strongly or mostly agreed that when undergoing change they took measures to guarantee and preserve the integrity of the information impacted by the change.

However, this chart also shows that almost 10% of the organisations undergoing most of these changes did not take measures to guarantee or preserve the integrity of the information impacted by the change (i.e those that mostly or strongly disagreed or didn't know).

Figure 12: Measures taken to mitigate impact on information integrity



Note: The population size (N=) varies by type of change undergone as shown in the previous figure

Observations

When undergoing administrative or business change, we strongly encourage organisations to involve their IM staff, and consider the IM implications of these changes. Considering IM requirements will help mitigate the risk of alteration, inappropriate access, retention or destruction of related information.

Even where there are major legislative, policy or administrative reforms in government, there will be some continuity with previous approaches or a need to rely on information created under them.

4.0

Governance and Capability

This section covers the criteria outlined in Principle 1 of the *Information and records management standard* relating to governance and capability to ensure information and records are able to support all business functions and operations. This includes strategies and policies, assignment of responsibilities, resourcing and monitoring IM activities, systems and processes. Survey questions relating to Te Tiriti o Waitangi were included in this section.

Governance groups and Executive Sponsors

What we asked and why it is important

We asked whether survey participants had an active formal governance group for IM (Q.8). By 'active' we meant a group that met a minimum of twice a year.

A governance framework is critical to the achievement of effective IM that supports business functions and operations. An organisation must set high-level strategy and policies for managing its information.

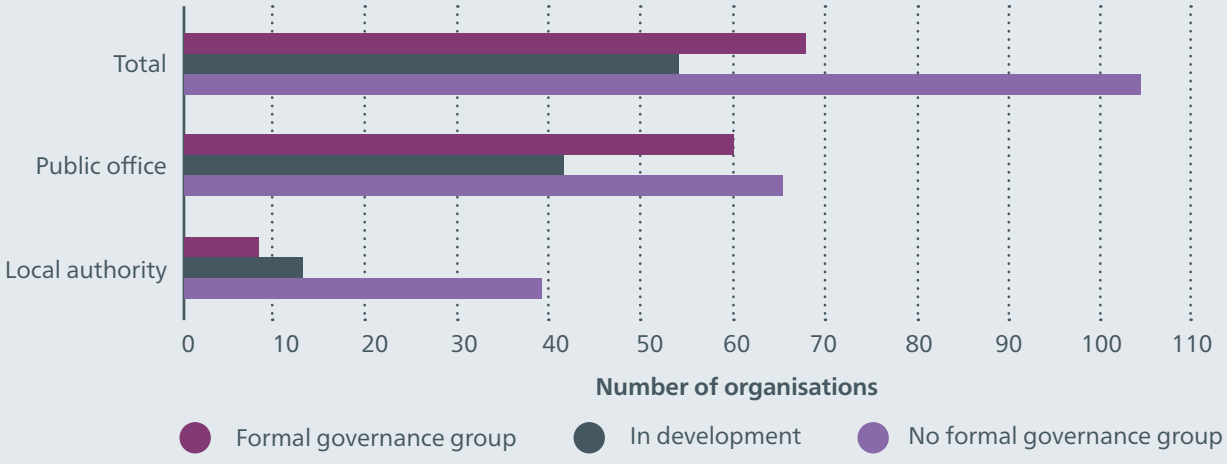
Findings

Figure 13 shows that just over half of the organisations (122, or 54%) have either an active formal governance group or are in the process of developing one. While this is encouraging, it means that nearly half of the organisations do not have a formal governance group and are not developing one.

Figure 13 also shows the response split by the type of organisation. For POs, it is encouraging to note that 101 (61%) either have a formal governance group or are developing one. However, there is still a significant number of POs (65) that do not have a formal governance group.

The picture is less encouraging with LAs. Here we see relatively small numbers that either have a formal governance group or are developing one. Almost two-thirds (39, or 65%) of local authority organisations do not have a formal governance group and are not developing one.

Figure 13: Does the organisation have an active formal governance group for IM? (N=226)



Observations

An active governance group should support the development and implementation of a governance framework for IM and ensure operational practices support business outcomes. A governance framework provides the organisation with a mechanism to develop a consistent, holistic approach to managing information and data. Both information and data should be aligned in terms of security, access, lifecycle management and metadata management. For smaller organisations it may be more practical to absorb IM governance into an existing governance group with a wider scope.

Ideally, the makeup and responsibilities of a governance group should include the following:

- There should be a direct reporting line to the chief executive and the leadership team, and the group should engender support from key senior managers and all relevant business groups.
- IM governance should remain a distinct responsibility even where organisational size, form and function suggest giving IM responsibility to a multipurpose governance group covering related functions.
- The Executive Sponsor and staff with IM expertise should be involved.
- The governance group should have the authority to plan, direct and allocate funding to build and/or improve IM capability and systems.

IM capability

What we asked and why it is important

To get a better picture of current resourcing in public sector organisations, we asked how many dedicated IM staff (full-time equivalent) were currently working in organisations (Q.15). To set the measure apart, we asked respondents to exclude geospatial information systems, business intelligence, data management and medical records staff. We also asked organisations what kind of professional development dedicated IM staff (if any) have undertaken that helped them meet business needs (Q.16).

Organisations should either have IM expertise on staff or have access to appropriate IM expertise. Having sufficient, appropriate and current IM skills available is essential to meet the needs of a dynamic and complex environment. Offering system-specific training to support business needs, and general professional development opportunities, are also an essential part of building robust IM capability.

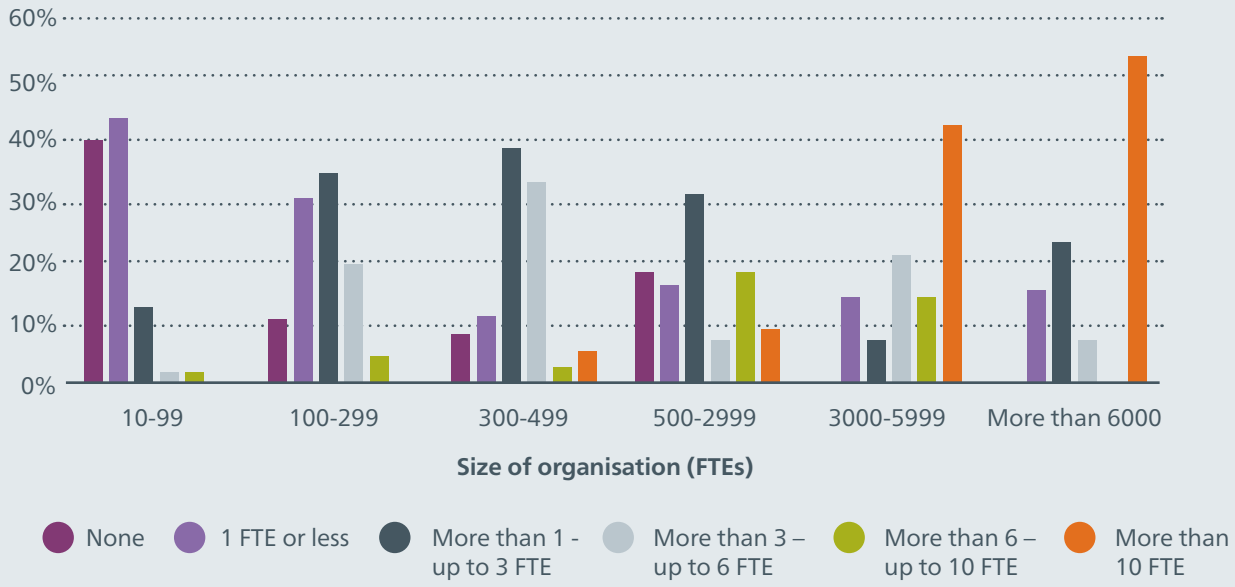
We looked at the results by the size of the organisation so that over the next few years we can benchmark the number of IM employees by size of organisation.

Findings

For small organisations with lighter IM needs we would not necessarily expect there to be a full-time, dedicated IM resource. The organisation might instead manage its IM needs using third-party providers or multi-role administrative support staff. For larger organisations, complexity will generally drive the need for dedicated and specialised IM resources.

Figure 14 shows the number of dedicated IM staff within organisations of different sizes, excluding the small organisations where dedicated staff would not be expected.

Figure 14: Number of dedicated IM FTEs working in the organisation by size (N=219)



From this chart we see that the proportion of organisations with no dedicated IM FTEs tends to decrease as the size of organisation increases, with a higher proportion of staff being present in bigger organisations. Despite this overall trend, it is surprising that of the organisations with 300-499 and 500-2999 staff (FTEs) there is such a high percentage with no dedicated IM FTE resources (8% and 18% respectively).

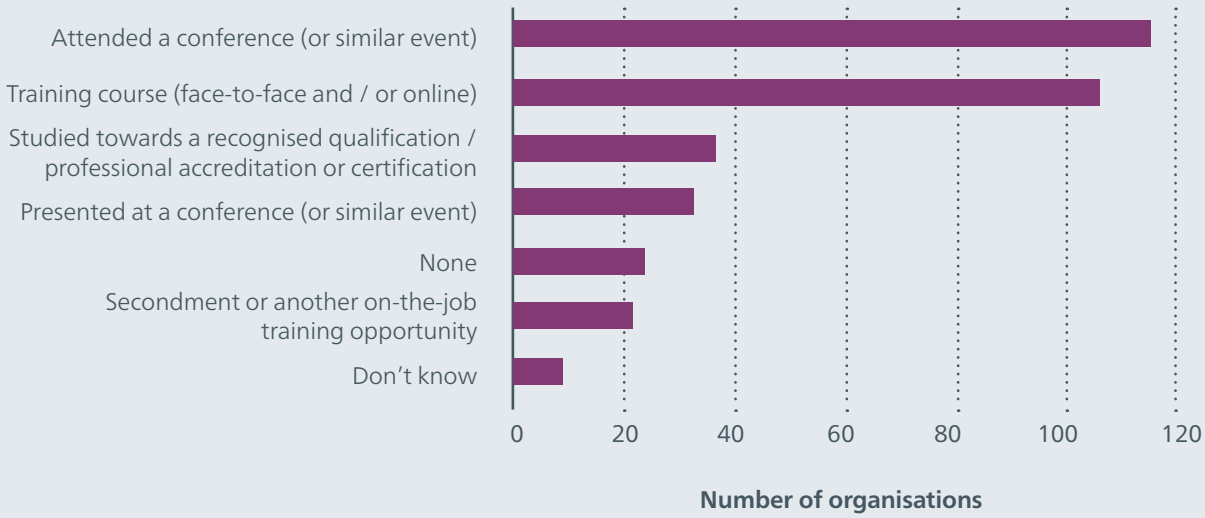
Twenty-seven organisations with staff numbers of 3,000 or more responded. Of the 27 organisations:

- 4 have 1 dedicated IM FTE staff, or fewer;
- a further 4 have between 1 and 3 dedicated IM staff; and
- 13 employ more than 10 dedicated IM staff.

It is concerning that some of the larger organisations seem to be significantly under-resourced in the area of IM. This is particularly concerning where a large volume of high value and/or high risk information is held.

For those organisations with dedicated FTE IM staff (179 organisations), we also asked what professional development activities IM staff have undertaken. Conference attendance and training courses feature as the top two activities. Thirty-three organisations (18%) have either not invested in professional development opportunities or don't know whether their IM staff have received any professional development.

Figure 15: Professional development activities (N=179)



Observations

We encourage Executive Sponsors to ensure that staff with suitable skills to implement IM strategies are employed and upskilled appropriately.

IM staff have the skills and knowledge to contribute to many business activities as well as the typical IM functions, including:

- alignment of IM to corporate objectives and business activities;
- procurement and contract management, especially where functions are outsourced, and IM responsibilities are transferred to third parties;
- training staff and contractors in IM responsibilities;
- development of information asset registers;
- business system implementation and decommissioning; and
- information governance.

We encourage all organisations to fully utilise the skills and knowledge of their specialist IM staff. Recognition of IM professionals' achievements in organisational communications can support staff retention while reinforcing the foundational importance of their role.

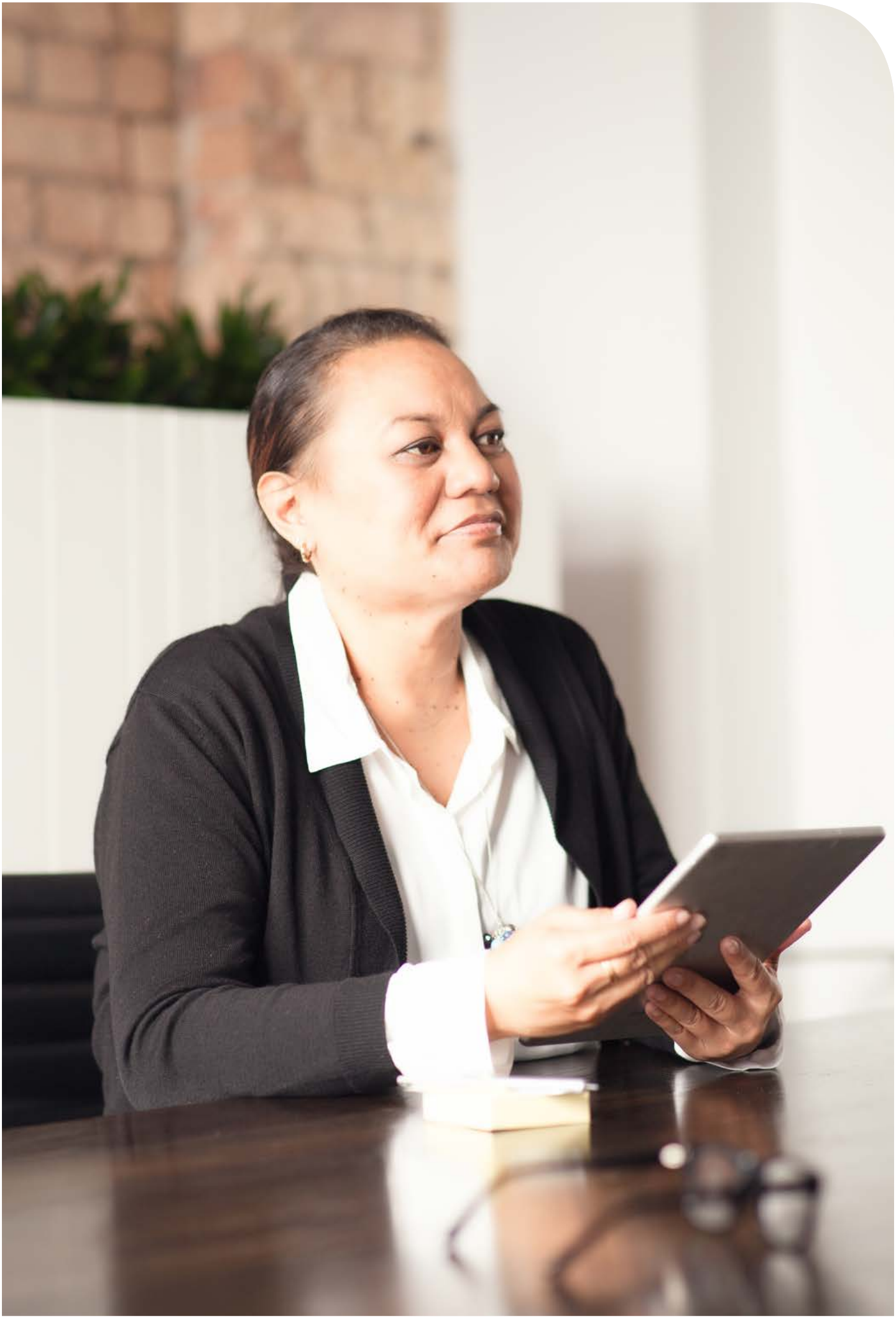
Te Tiriti o Waitangi and IM

What we asked and why it is important

We wanted to find out if organisations had specific commitments related to Te Tiriti o Waitangi (Te Tiriti) that impact on IM, and what activities they had undertaken to ensure IM meets those commitments (Q.10 and Q.11).

Public offices will already be aware and have an understanding of Te Tiriti principles and their application in relation to their respective organisations. Local authorities deliver public services that impact on rights guaranteed to iwi Māori under Article 2 of Te Tiriti. These Te Tiriti obligations make their role also significant in upholding the Crown's responsibilities as a Te Tiriti partner.

The IRM standard supports the rights of Māori, under Te Tiriti, to access, use and reuse information and records that is taonga. Organisations should ensure that information about Māori is accessible.

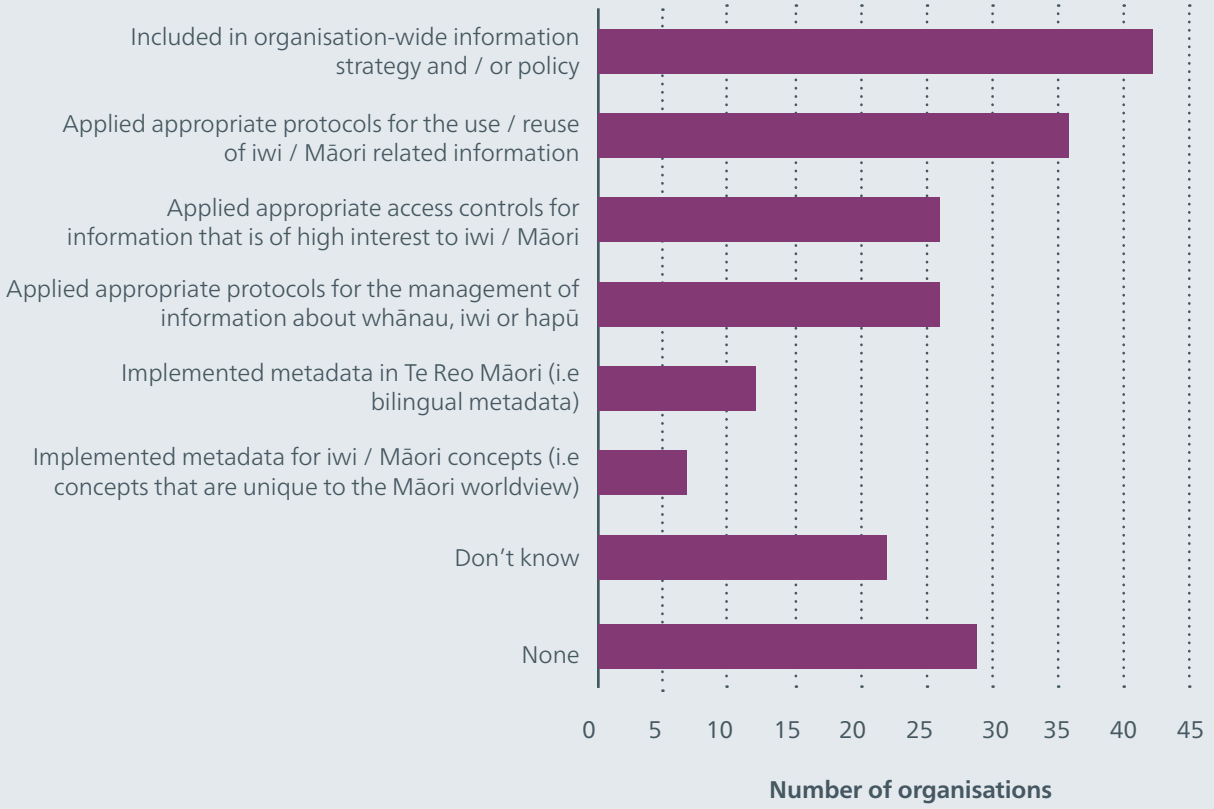


Findings

Of the responding organisations, 141 (62%) stated they had commitments related to Te Tiriti. We were particularly interested in whether organisations that have made a commitment are exploring the use of metadata in Te Reo Māori, and/or metadata for iwi/Māori concepts, as these specifically relate to IM.

These 141 organisations were asked specifically about what they had done in the last 12 months. Fifty-one organisations had either done nothing (29) or said they did not know (22). The activities organisations had done are set out in Figure 16.

Figure 16: Activities that organisations have undertaken to ensure IM meets Te Tiriti commitments (N=141)



Observations

We encourage all public sector organisations to consider adding metadata fields or tagging capabilities for Māori metadata and/or metadata for iwi/Māori concepts. This is particularly important when organisations are implementing new enterprise content management systems, line-of-business systems, or collecting information on land, people and natural resources.

5.0

Technology and Systems

This section summarises the results from the survey questions that relate to Principle 2 in the IRM standard. The topics are building IM requirements into new systems, risks to information, metadata, and the protection of digital information of long-term value. It also covers whether organisations have found it difficult to respond to requests for official information.

IM requirements built into new systems

What we asked and why it is important

We wanted to know if organisations were building requirements for creating, managing, storing and disposing of information into new business information systems (Q.23). We also asked what challenges organisations faced to ensure that IM requirements are built into new systems (Q.24).

Systems are often implemented without an understanding of the business information needs they must support. Without this understanding, the creation and maintenance of key business information may be at risk. These risks can be mitigated by clear governance and planning and involving IM staff early in the process of implementing new systems.

Findings

Only 51 (23%) of respondents indicated they have built IM requirements into new business information systems, as shown in Figure 17.

Figure 17: IM requirements built into new business information systems (N=226)

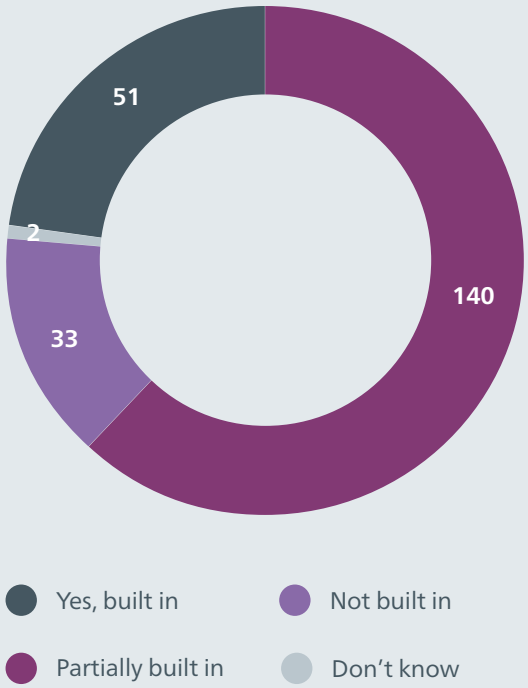
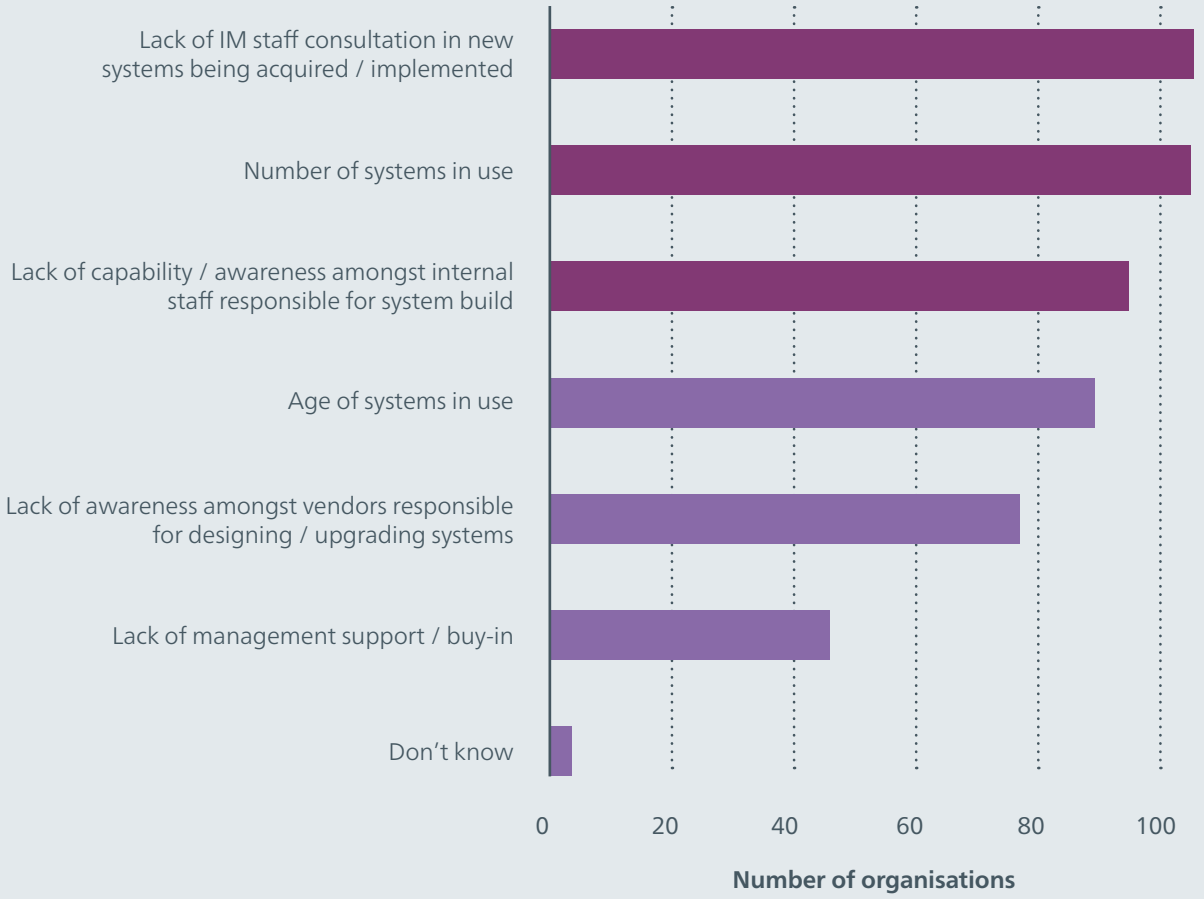


Figure 18 shows the challenges faced by the 175 organisations that stated their IM requirements have not been built into any or all of their systems (i.e they responded 'partially', 'not built in' and 'don't know'. The biggest challenges were the:

- lack of IM staff consultation when new systems are being acquired/implemented;
- number of systems in use; and
- the lack of capability/awareness among internal staff responsible for system build.

Figure 18: Challenges to building IM requirements into new business information systems (N=175)



Observations

To meet the biggest challenges for building IM requirements into business information systems organisations could do the following:

- Involve IM staff early in discussions and decision making about new business information systems. IM staff have the knowledge and skills to ensure that system specifications can provide for the active management of information, that metadata requirements are met, and to ensure the preservation and access of information required for long-term retention. They can also ensure that system design and configuration documentation is retained.
- Plan to reduce the number of systems in use over time.
- Improve the IM capability and skills of staff involved in system builds.
- Executive Sponsors should review their IM team's resourcing needs.

Risks to information

What we asked and why it is important

We asked survey participants what key risks to their organisation's information they had identified (Q.22).

An organisation must identify the likely or potential risks to information so they can manage or mitigate them. Risks can include loss, inaccuracy, tampering and inappropriate disclosure. Risks can also include system or format obsolescence, inadequate security, data corruption, and inaccessibility due to the lack of metadata or deterioration of media.

We also asked (Q.19) whether the organisation had an IAR, because systematically identifying information assets in this way helps organisations understand and manage them. Once organisations have identified the risks to information they can take steps to protect the information and information systems at risk.

Findings

Survey participants agreed there were several risks to their organisations' information (Figure 19). Many of these risks are particularly pertinent to digital information within an organisation's ICT environment and infrastructure. The lack of contextual information to enable discovery and interpretation is also directly related to ensuring metadata is applied and consistent across data and information (Q.25), as discussed in a later section.

We are also concerned about information that may be stored on obsolete or at-risk mediums, particularly if this information also needs to be accessible for a long time.

Figure 19: Risks identified to the organisation's information (N=226)

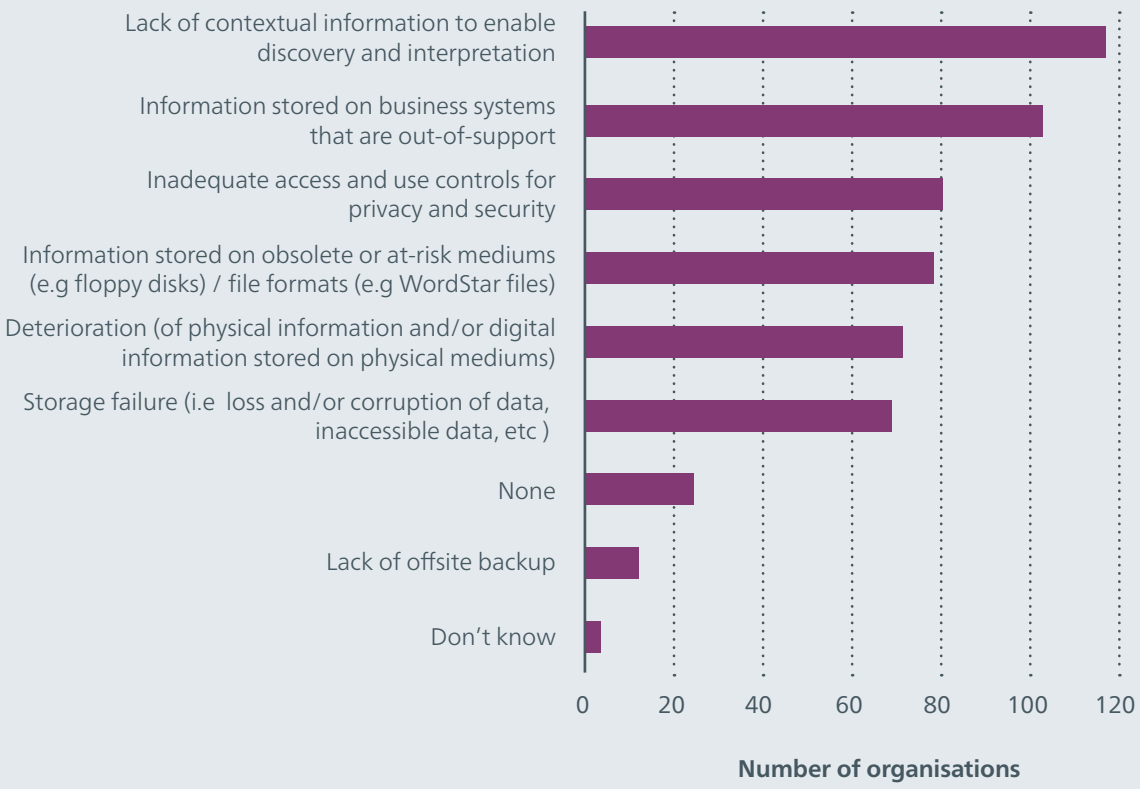
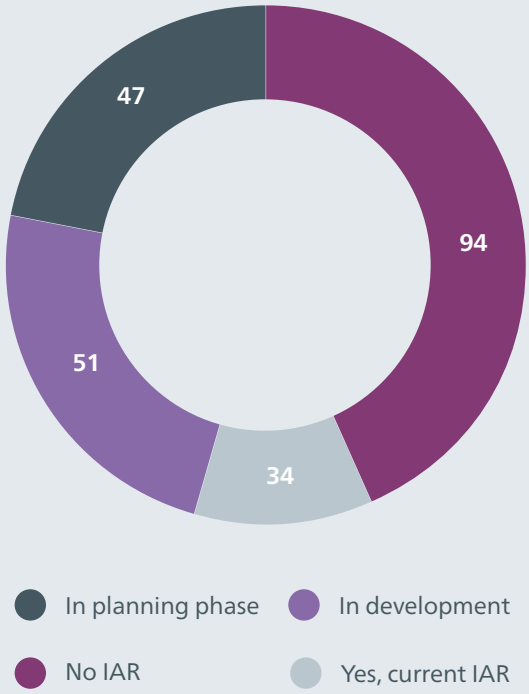


Figure 20 shows that just 34 organisations have an IAR, and a further 98 are currently developing an IAR or planning to develop one. This leaves 94 organisations with no IAR and no plans to develop one.

Figure 20: Whether organisations have an Information Asset Register (N=226)



Observations

With the many risks to information, as identified in Figure 19, developing an IAR is one of the ways to identify information assets and document these risks.

Effective IM practice is a primary risk mitigation strategy. Involving IM staff in the process of developing an IAR and risk management planning can support this strategy.

Integrating IM with the organisation's enterprise risk management practices will allow IM activities to be connected to specific business risks. This is particularly relevant for digital information and business information systems that are being upgraded or decommissioned.

Metadata

What we asked and why it is important

We asked survey participants whether their document and records management system(s) met our minimum requirements for metadata (Q.25) as set out in our IRM standard.

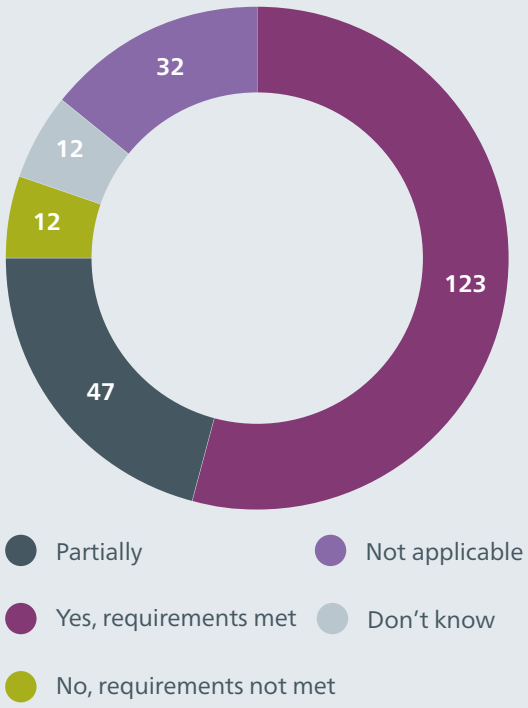
Metadata is information that helps people find, understand, authenticate, trust, use and manage information. If information has metadata, it helps people know what it is, what it has been used for, and how to use it. Without key metadata, the value of information decreases significantly.

Minimum metadata requirements should be applied in all systems that capture and retain information and records, including line-of-business systems.

Findings

Over half of survey respondents (123) told us that their organisations' current document and records management system(s) met our minimum requirements for metadata (Figure 21). A further 47 (21%) said their system(s) partially met our requirements, and 24 respondents (10%) either said they didn't know, or that their system(s) did not meet our requirements.

Figure 21: Whether minimum requirements for metadata are being met (N=226)



Observations

When designing information and records systems, organisations should always consider:

- what metadata will best enable the flow of business, and the creation and management of accessible information;
- what metadata will best ensure the integrity of business information; and
- what metadata will need to be maintained through business system changes and be persistently linked to business information for context and accountability.

Ideally, the creation and capture of metadata should be automated where possible to make systems easy for the end user. Metadata is critical to protect business information and the discovery expectations of our digital world to support open and transparent government. Metadata is particularly important given the fragility of digital information, and the ease with which digital information can be corrupted, altered or deleted.

Digital information of long-term value

What we asked and why it is important

We wanted to understand what activities organisations are undertaking to ensure that digital information of long-term value remains reliable, usable and complete over time (Q.26).

This is important for open, transparent and accountable government. It is also important for organisations to be able to derive value from their information over the long term.

How and where digital information is stored will affect its viability over time. It is probable that some digital information and data in current systems will need to remain accessible and usable beyond the life of those systems.

Findings

Some organisations have taken action to protect digital information of long-term value. However, there is a significant proportion of respondents (44, or 19%) who have not undertaken any activity in the past 12 months, or 'don't know' (18, or 8%).

A few respondents also indicated they were doing 'upgrade and regular testing of backups' as another protection activity for digital information of long-term value. Backups have just one legitimate purpose, and that is the retention of data necessary to get a business information system back up and running in the event of a disaster. This is not the same as making effective provision for the long-term maintenance of information.

Digital information with long-term value should be maintained in an organisation's operational systems until it is ready to be destroyed or transferred to an appropriate digital archive. We do not accept backup tapes for permanent retention as public archives because they are not the authoritative record.

Figure 22: Activities to ensure that digital information of long-term value remains reliable, usable and complete over time (N=226)

Observations

Business system planning must identify what information can be routinely disposed of and when, and what information must be maintained and retained by the system, and how this will be achieved. This will help ensure that an organisation's information and data of long-term value will remain reliable, usable and complete over time.

When planning for information longevity, organisations must mitigate associated risks, such as:

- paying for software licensing and support, hosting and infrastructure costs (servers and maintenance), and offsite storage costs;
- the potential for information duplication and dual processes caused by maintaining legacy systems concurrently;
- the difficulty of extracting information from legacy systems and migrating to new systems; and
- the failure to comply with legislative obligations and requirements for information retention.

To make any upgrades or transitions into new systems as seamless as possible, it is important to consider long-term IM needs early in the systems' planning and development stages.

Digital information no longer accessible

What we asked and why it is important

We wanted to find out if organisations held any digital information they can no longer open (Q.27), and if they do, what the main reasons were (Q.28).

Information must be identifiable, accessible and usable for as long as the information is legally required to be retained. To maintain the accessibility and usability of information, organisations must store and manage it appropriately. For digital information, it is also critical to ensure information is migrated from one system/platform to another, and/or from one format to another in order to maintain it in an accessible form.

Findings

Results shown in Figure 23 indicate that the majority of organisations held information they can either no longer open (72, or 32%) or don't know whether or not they can open it (60, or 27%). Ninety-four organisations responded that they have no digital information that is inaccessible.

Figure 23: Whether organisations hold any digital information they can no longer open (N=226)

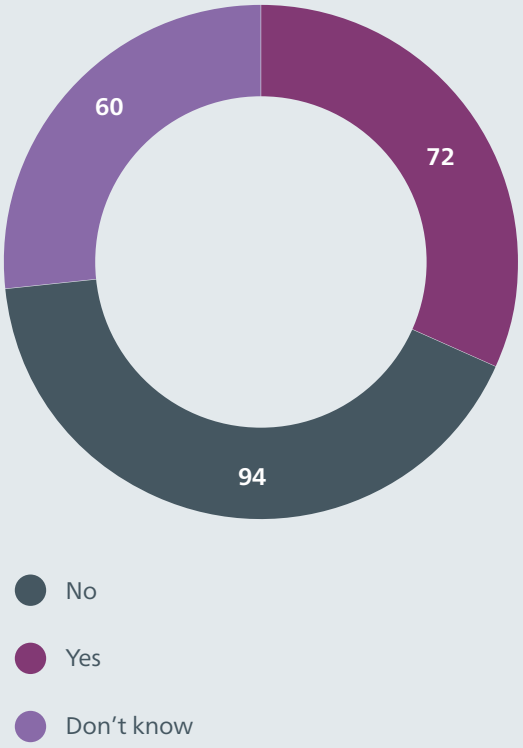
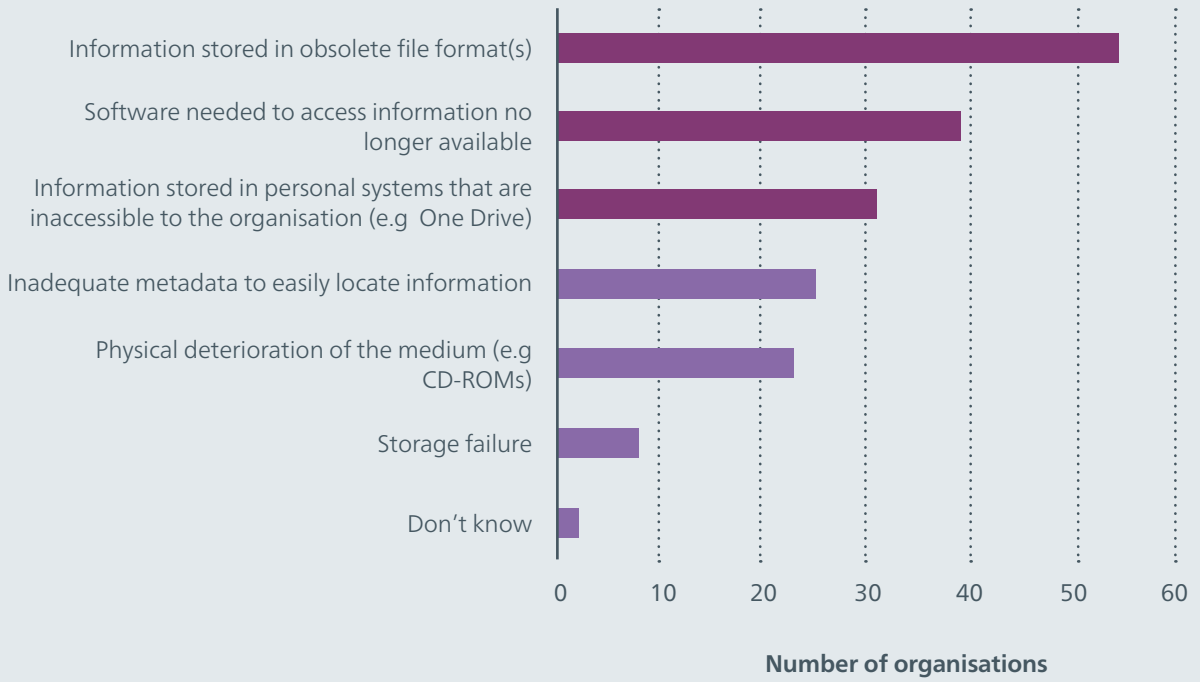


Figure 24: Main reasons organisations can no longer open that information (N=72)



Observations

A collaborative relationship between IM and IT staff is essential to protect and ensure the accessibility of government information of long-term value, and to ensure digital continuity. For those organisations that answered 'don't know' to Q.27, creating an IAR would be one way of establishing what information assets an organisation holds, and where, as well as identifying and managing any risks associated with these assets.

Storage and measures in place to protect information

What we asked and why it is important

We asked survey respondents whether they felt they had adequate protective mechanisms in place to protect both physical and digital information against unauthorised access, alteration, loss, deletion (for digital information) and destruction (Q.32 and Q.33).

Organisations are responsible for protecting information in their custody, whether it is physical or digital, stored onsite or offsite, onshore or offshore. Security policies and mechanisms must be in place at all times and must be regularly monitored and updated. This includes access and use permissions in digital systems, secure physical storage facilities, and protective processes wherever the information is located, including when in transit outside the workplace.

Findings

Responses to our questions of storage for physical and digital information show most organisations are largely satisfied ('mostly' or 'strongly agree') with the current protection mechanisms in place (Figure 25 and Figure 26).

Figure 25: Whether storage facilities for physical information have measures to protect information against unauthorised access, alteration, loss and destruction (N=226)

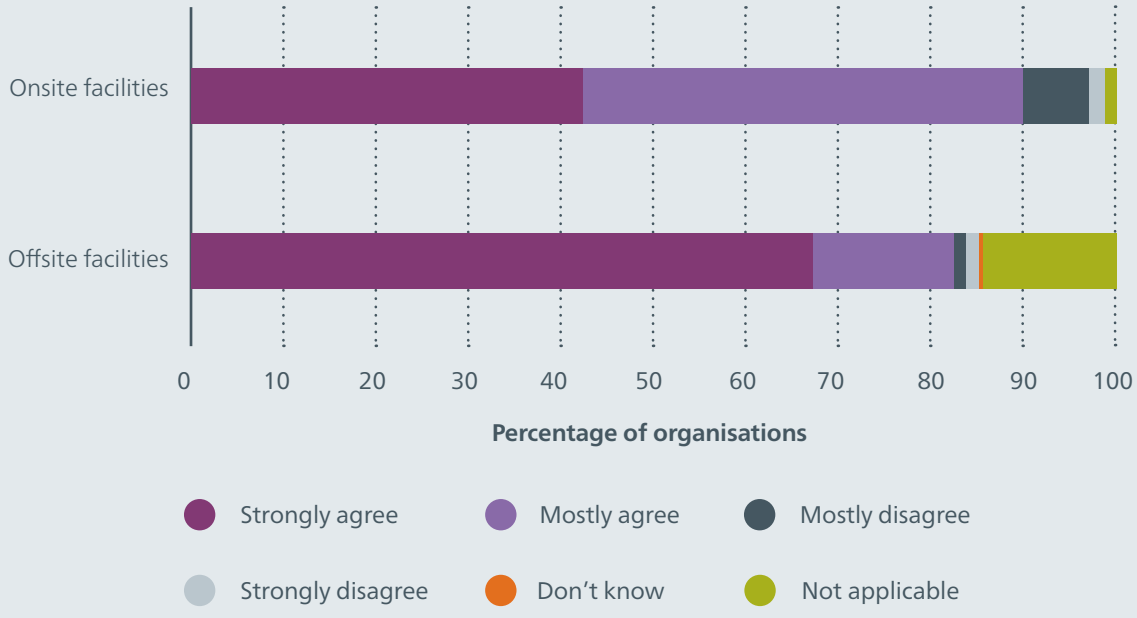
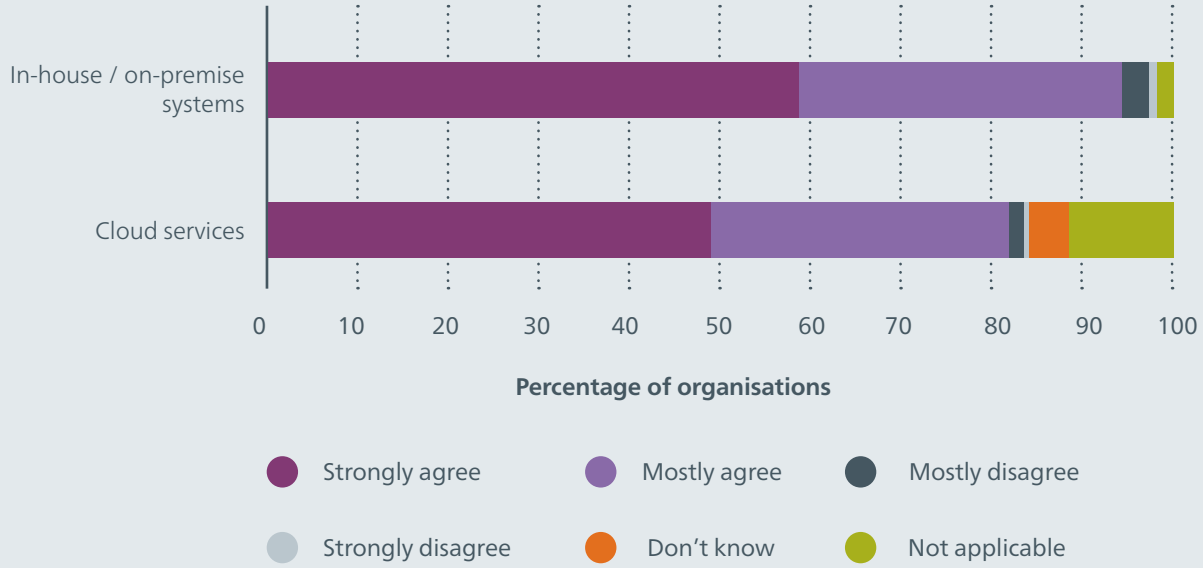


Figure 26: Whether storage for digital information includes mechanisms to protect information against unauthorised access, alteration, loss and destruction (N=226)



Observations

The results show that most organisations are confident they have appropriate measures in place to protect both physical and digital information against unauthorised access, alteration, loss, deletion and destruction. It will be interesting to see more details about the policies and operational processes that support this confidence during the upcoming PRA audit programme.

Requests for official information

What we asked and why it is important

We wanted to know whether, in the past 12 months, any organisations had difficulty responding to requests for information either because the information did not exist, or it existed but could not be found (Q.29).

Section 28(6) of the Official Information Act 1982 (OIA) and section 27(6) of the Local Government Official Information and Meetings Act 1987 (LGOIMA) state:

- *If an Ombudsman receives a complaint that a department or Minister of the Crown or organisation has refused to make official information available for any of the reasons specified in section 18(e) to (g), the Ombudsman may notify the Chief Archivist appointed under the Public Records Act 2005.*
- *If an Ombudsman receives a complaint that a local authority has refused to make official information available for any of the reasons specified in section 17(1)(e) to (g), the Ombudsman may notify the Chief Archivist appointed under the Public Records Act 2005.*

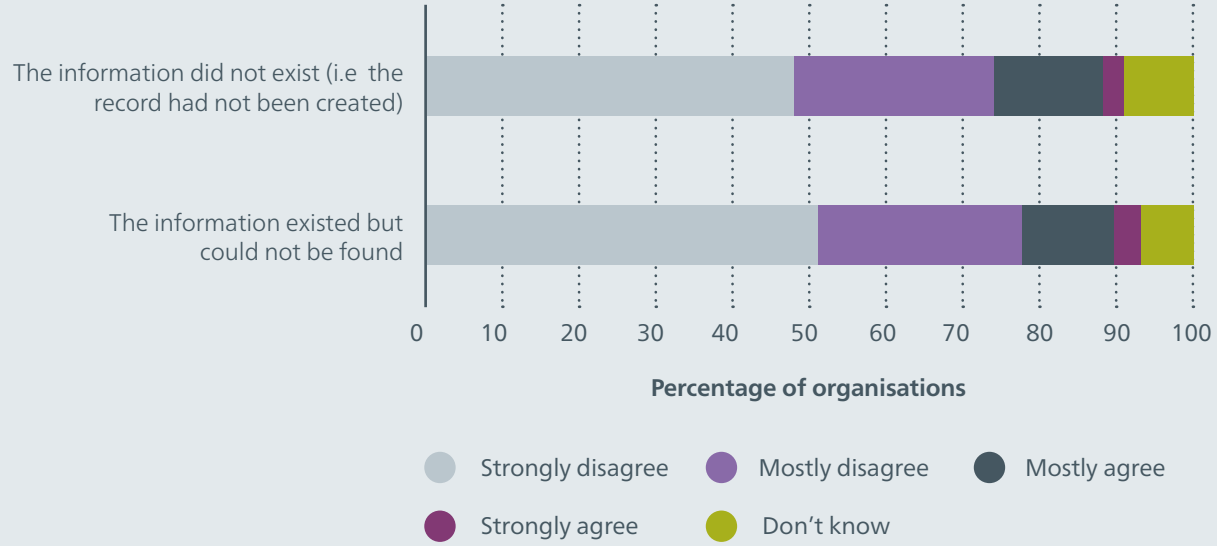
The reasons specified permit an organisation to refuse a request where the document alleged to contain information does not exist or, despite a reasonable search, cannot be found.


2535
878
MODEL:428

Findings

Almost three-quarters (74%) of those that responded to this question 'strongly' or 'mostly' disagreed they could not respond to requests for information because the information did not exist. A similar percentage (78%) 'mostly' or 'strongly' disagreed they could not respond to requests for information because the information could not be found (Figure 27).

Figure 27: Whether organisations had difficulties responding to requests for official information (N=226)



Observations

This confidence does not reflect the impression we take from information from the Office of the Ombudsman about complaints. We understand that in 2017/18 the Ombudsman received 189 notifiable complaints. Of those:

- 63 complaints related to a refusal under section 18(e) of the OIA; and
- 19 complaints related to a refusal under section 17(e) of the LGOIMA.

While the Ombudsman's statistics relate to the year before our survey, they are recent enough to be valid for comparison. The high proportion of complaints related to IM matters that can be referred to the Chief Archivist suggests that the confidence from survey participants that they do not have difficulty responding to OIA requests may be overstated.

The Office of the Ombudsman identified two common themes observed when investigating complaints:

- There was a disconnect between official information practitioners and IM staff about whether search tools actually find all relevant information.
- Organisations did not have mechanisms for dealing with information held on legacy systems or in formats that were not readable by current systems.

We will continue to work together with the Office of the Ombudsman to strengthen our relationship with the aim of improving organisations' responses to OIA and LGOIMA requests through improving IM capability and capacity.

6.0

Disposal

The survey included several questions relating to disposal, which is covered in Principle 3 of our IRM standard.

Authorised and timely disposal improves an organisation's control over their information. Under the PRA, 'disposal' is usually carried out by destruction, or by transferring control to an archival repository or another public office. Disposal can also include selling or discharging the public or local authority record, provided there is authorisation from the Chief Archivist.

By removing redundant information from systems, staff find it easier to find information, costs for storage and management are contained, and systems work more efficiently. Active disposal, for example, can ensure draft or superseded versions of documents are destroyed, thereby allowing easier access to, and sharper focus on, the records that best support business need and accountability.

Disposal coverage

What we asked and why it is important

We asked organisations how much of their information is covered by disposal authorities (Q.35). With full coverage under single or multiple disposal authorities and retention and disposal schedules, organisations can perform authorised disposal across all their information. Conversely, without full coverage, an organisation's ability to dispose of both digital and physical information is constrained due to lack of authorisation.

For organisations that do not have full coverage, we asked whether they have plans to appraise their information (Q.36). Appraisal is the analysis of an organisation's business context, business activities and risks to determine:

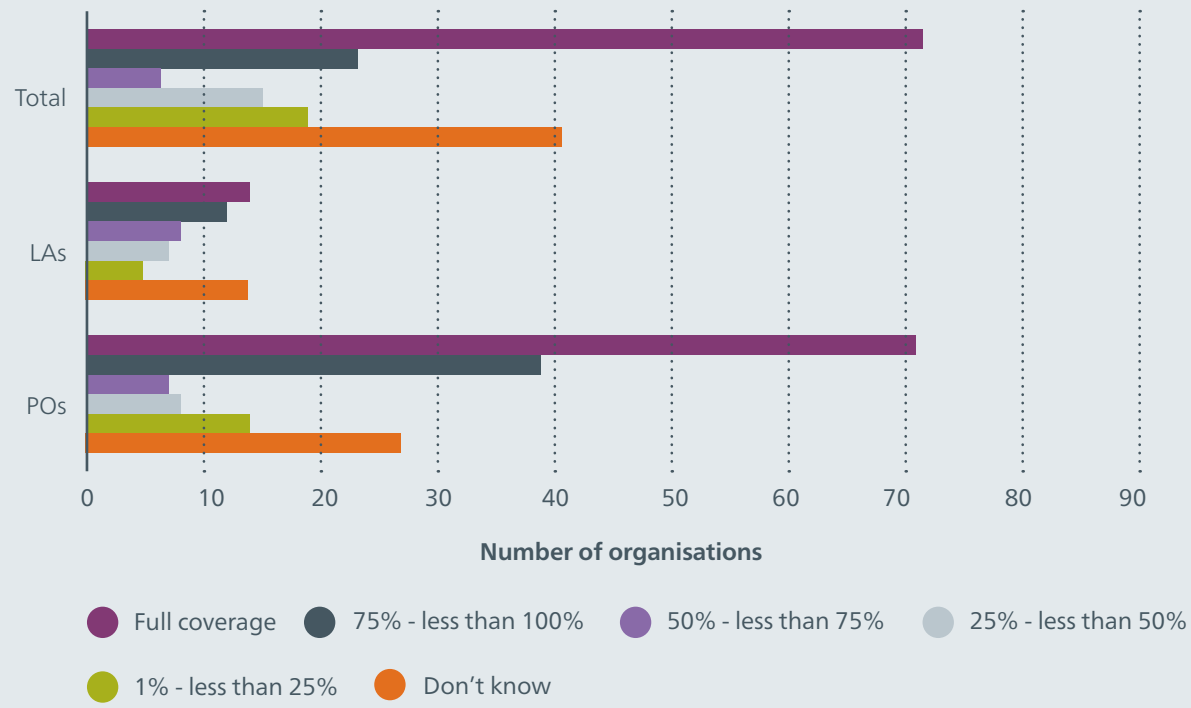
- what information and records to create;
- what information and records are high risk, high value, or both; and
- how long an organisation must manage information and records to meet business and community needs and expectations.

Findings

Figure 28 shows what percentage of information created and maintained by organisations is covered by applicable disposal authorities. Only 85 organisations are fully covered, with a significant difference in coverage between POs. Of the 176 POs surveyed, 71 have full coverage (43%) while just 14 LAs have full coverage (23%).

POs generally have a higher level of coverage than LAs, as is also shown in the chart, while there is a significant number of both POs and LAs that don't know their coverage.

Figure 28: Disposal coverage (N=226)



For POs and LAs without full coverage (141 in total), 45 organisations are either currently appraising their information, or planning to address the gap in the coming 12 months. This leaves a further 70 organisations still to work toward full coverage in coming years, and 26 organisations that don't know their plans.

Observations

For organisations that don't know their level of disposal coverage, and for those with disposal coverage for less than 25% of their information, Executive Sponsors and IM staff are encouraged to prioritise work to clarify the level of coverage and expand it. This will improve business efficiency, contain costs, protect their organisation's reputation, and help to achieve the organisation's requirements under the PRA.

Local authorities that are members of the Association of Local Government Information Management and have adopted the current ALGIM Retention and Disposal Schedule will have full coverage.

Disposal activities

What we asked and why it is important

We wanted to understand what type of disposal activities organisations are engaged in (Q.37).

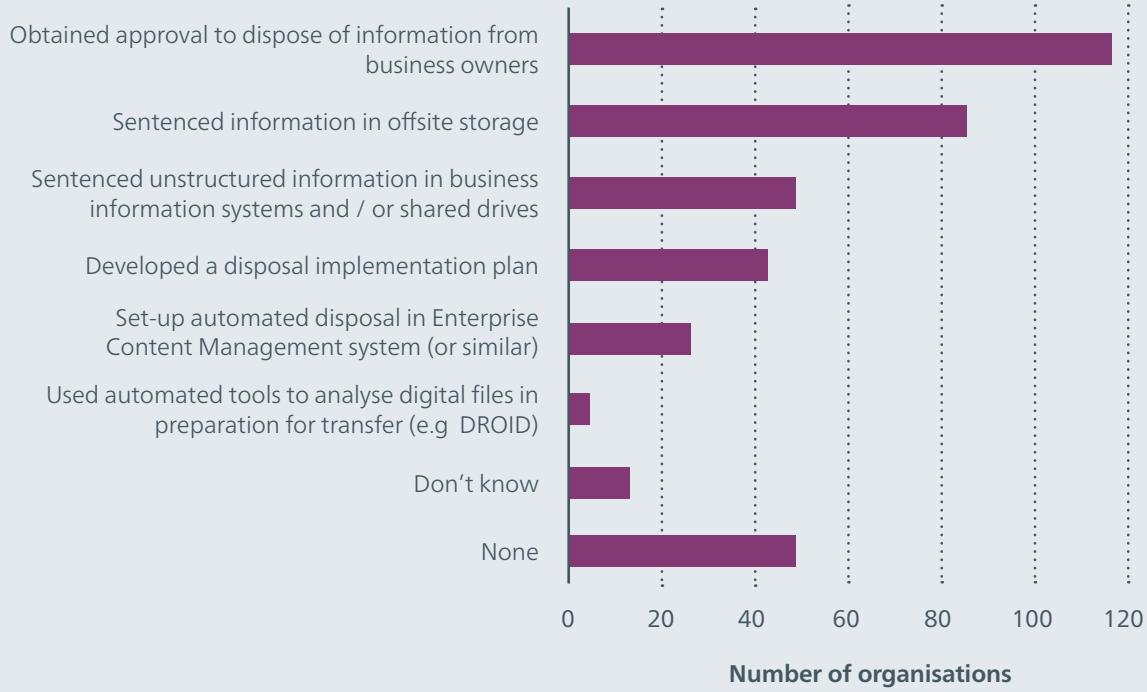
Disposal authorities and retention and disposal schedules must be implemented, maintained and regularly reviewed to be effective. In the absence of full coverage, organisations can still implement the general disposal authorities to start actively disposing.

Findings

One hundred and seventeen organisations have obtained approval from business owners to dispose of information, and 85 organisations have sentenced information held in offsite storage.

Of the 226 survey respondents, 48 organisations have undertaken no disposal activities, and a further 13 do not know whether they have done any disposal activities.

Figure 29: Disposal activities organisations engaged in (N=226)



Observations

While all the activities listed contribute to the disposal process, it is important to note that a planned approach to disposal is essential for a successful and effective outcome. Establishing a disposal implementation plan should be the first step organisations take.

Attention should also be given to enabling automated disposal activities to make the disposal process consistent, achievable and sustainable. Manual processes applied to disposal activities are more reliant on individual actions and subjective decisions, making the processes even more time and resource consuming, with a higher risk of inconsistent outcomes.

Sentencing

What we asked and why it is important

We asked organisations what percentage of their information had been sentenced (Q.38). Sentencing is the process of applying a disposal authority and its disposal actions across an organisation's information.

Once organisations have established a disposal implementation plan, the first step to action the plan is to sentence the information using applicable disposal authorities.

Findings

The top three bars of Figure 30 show that two-thirds of organisations either don't know how much sentencing has been done or have done no sentencing, or have done only a minimal amount of sentencing.

Figure 30: Percentage of information sentenced (N=226)

Observations

These results, combined with the challenges identified in Figures 34 and 35 below, indicate that organisations need to dedicate more attention and resources to sentencing activities. Sentencing is a necessary step towards active disposal, including the transfer of information.

Methods of disposal

What we asked and why it is important

In this section we looked at destruction and transfer – two methods of disposal for both physical and digital information. We asked organisations if they have done any destruction of information in the past 12 months (Q.39) and if they were planning any transfer of either physical or digital information over the next 12 months (Q.41 and Q.42).

An organisation that keeps information and records for longer than required is exposed to risks, including unnecessary storage costs, lack of business efficiency, and reputational damage. Routine authorised destruction helps organisations mitigate those risks.

The PRA mandates the transfer of public records of long-term value that have been in existence for 25 years. They must be transferred to the control of the Chief Archivist as public archives, unless the PO applies for a deferred transfer (deferrals should be in place, even when these are a result of Archives New Zealand's storage and processing constraints). The PRA does not specifically mandate the transfer of local authorities' records to a local authority archive. Rather, the PRA changes the status of local authority records into local authority archives when they are 25 years old or no longer in current use. It also requires the access status to be set to open access, unless there are good reasons to restrict access.

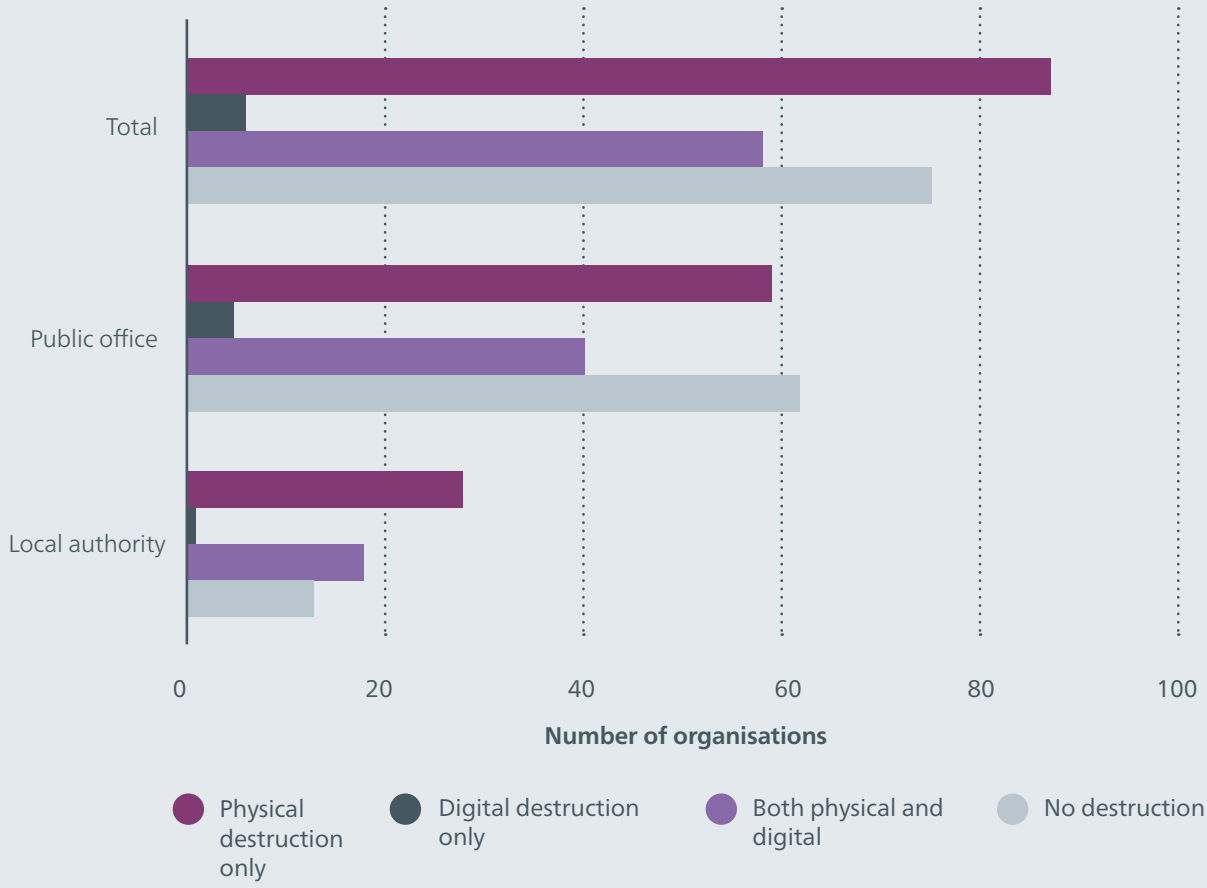
Destruction

Findings

Figure 31 shows that of the 166 POs, 104 (63%) are doing some form of authorised destruction of information. This destruction mostly concerns physical information only, or both physical and digital information. For LAs, 78% of the survey participants are destroying some information.

Overall, 75 organisations (33% of the 226 public and local authority organisations) stated they destroyed no information in the last 12 months.

Figure 31: Whether organisations have done destruction in the past 12 months (N=226)



Transfer

This includes the transfer of either physical or digital information to us or an approved repository. We note that while Archives New Zealand's Wellington repository is closed for physical transfers, our Dunedin, Christchurch and Auckland repositories are open, and digital transfer to our Government Digital Archive is available.

Findings

From Figure 32, the majority of organisations have no plan to transfer physical information to any repository within the next 12 months. Fifty-seven POs and LAs are planning to transfer physical information to an Archives New Zealand repository, an approved repository or a local authority archive. For 42 organisations, the question is not applicable, either because our Wellington repository is not available or there is no local authority archive to transfer to.

Figure 32: Whether organisations are planning physical transfers in the next 12 months (N=226)

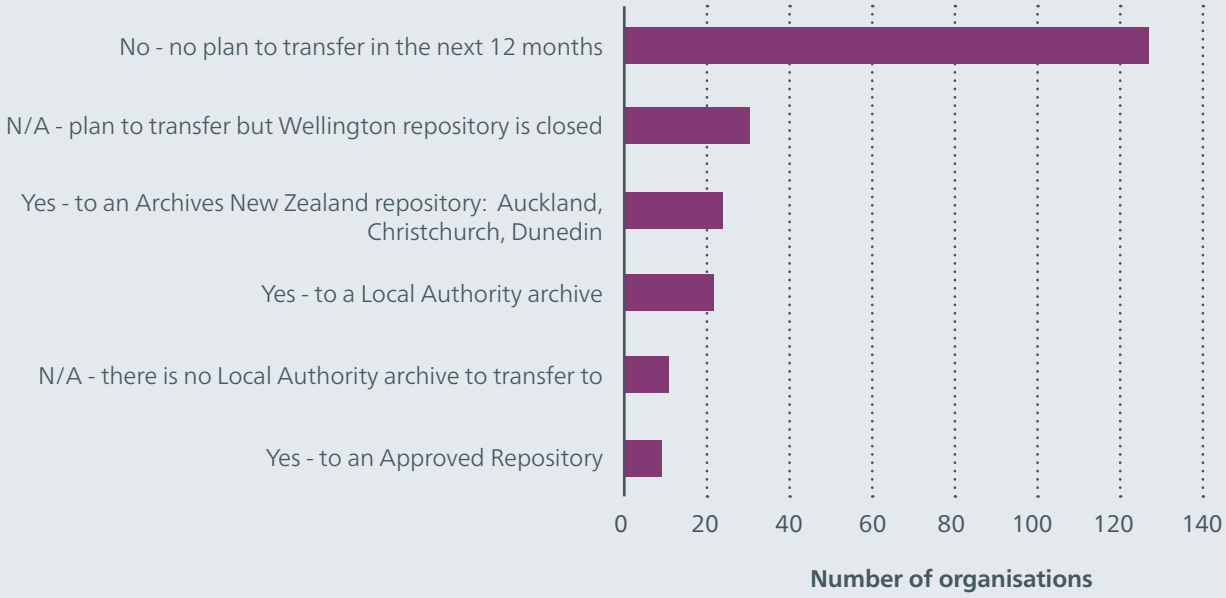
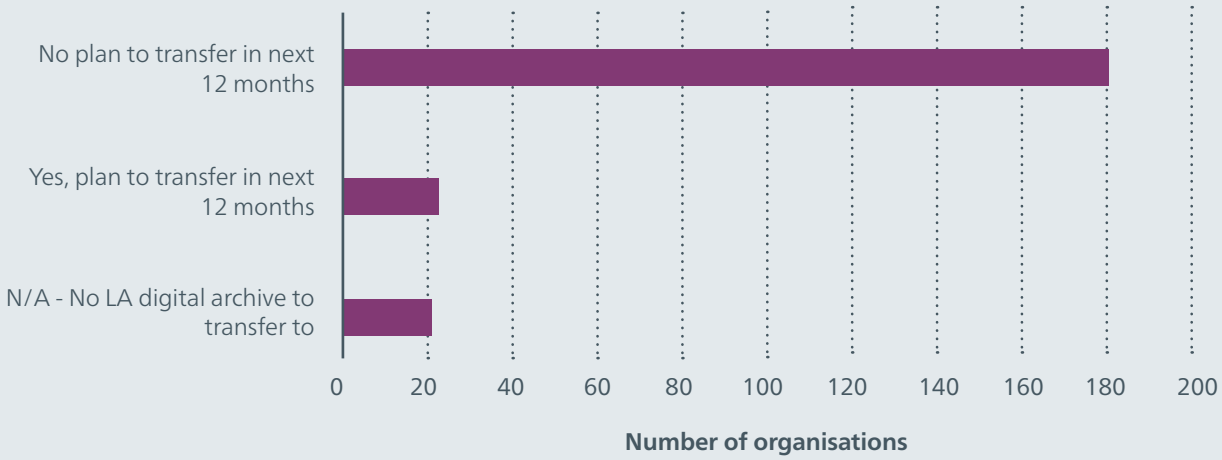


Figure 33 clearly shows that the majority of respondents (181) are not planning on making any transfers of digital information.

Figure 33: Whether organisations are planning digital transfers in the next 12 months (N=226)



Observations

We recognise it is currently not possible for Wellington-based POs to transfer physical records because the Wellington repository cannot accommodate these. However, POs headquartered in the upper North Island or in the South Island are still able to transfer physical records to our offices in Auckland, Christchurch and Dunedin. We are open for digital transfers from POs wherever they are located.

Executive Sponsors and IM staff should now be proactively planning to protect and preserve digital information of long-term and/or archival value.

Challenges to regular destruction and transfer

What we asked and why it is important

We wanted to understand what challenges organisations encountered with regular destruction and transfer activities (Q.40 and Q.43).

Understanding barriers to destruction and transfer allows organisations to tailor their disposal implementation plan to their current situation, allocate resources and concentrate effort where it is most needed.

Findings

Results from our survey show that systems setup, lack of resources, and lack of prioritisation are the top three challenges for regular destruction (Figure 34). Figure 35 shows that the challenges impeding regular transfers include a lack of resources for sentencing activities, resources and/or tools, and a lack of experience and/or skills to do digital transfers.

Figure 34: Challenges for undertaking regular (approved and authorised) destruction of information (N=226)

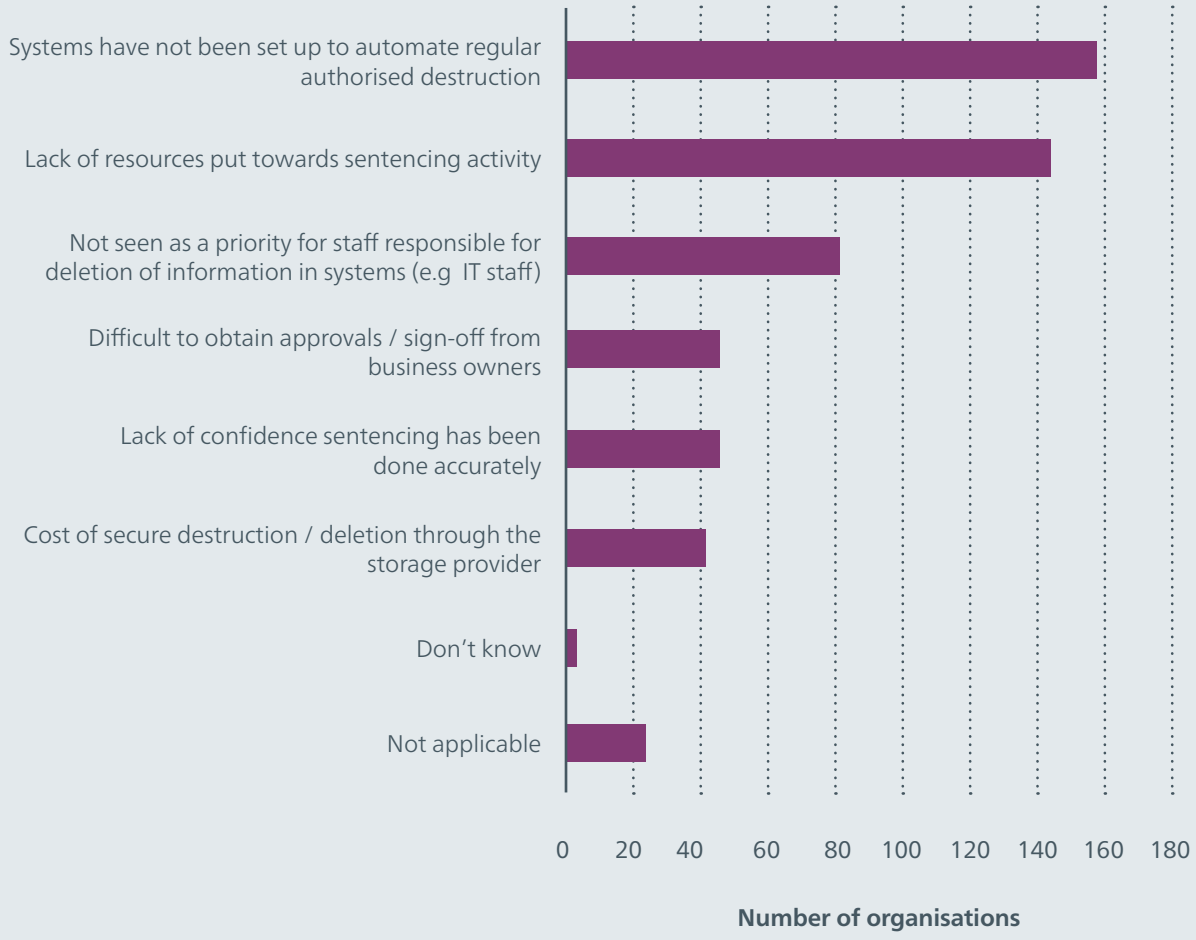
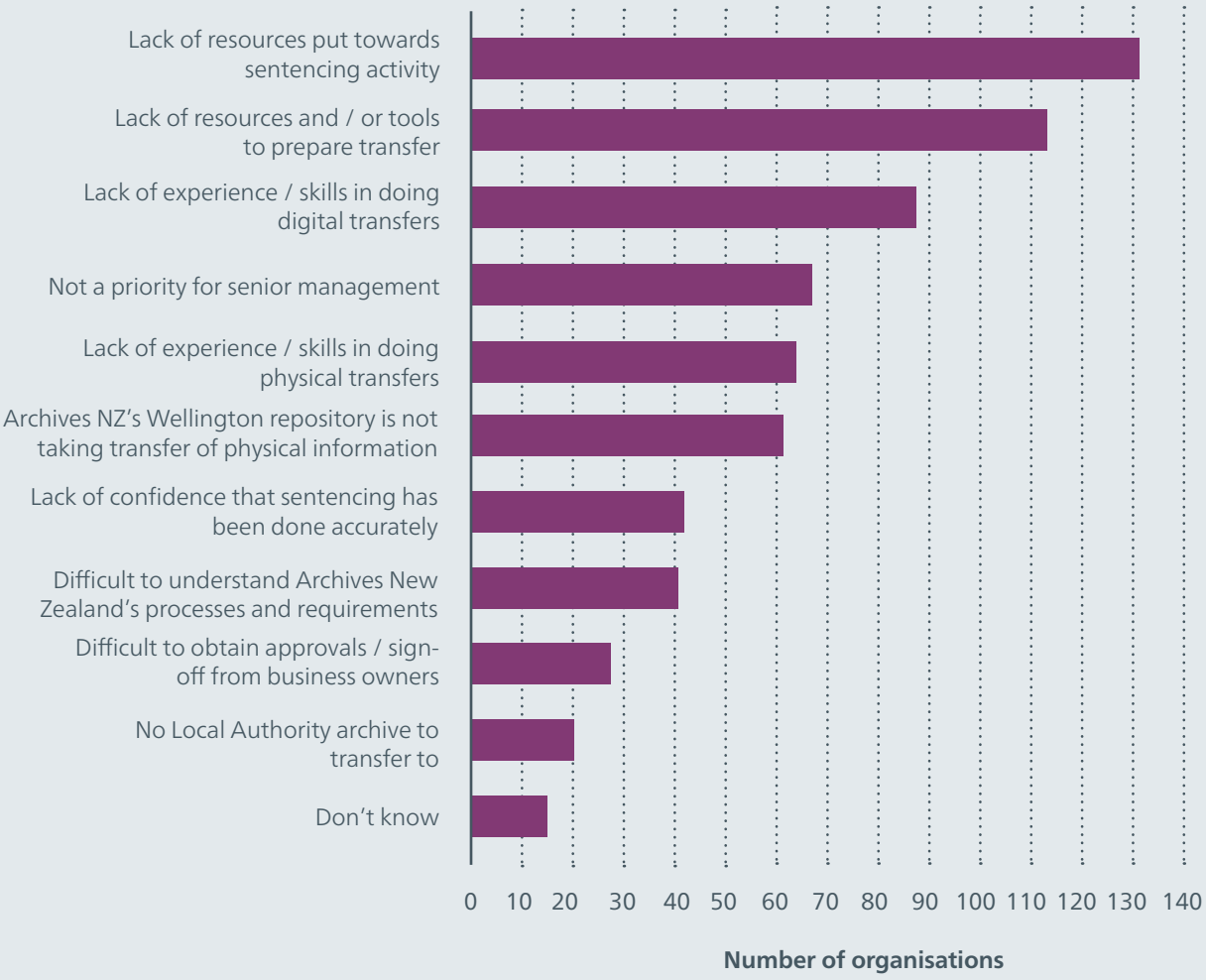


Figure 35: Challenges for undertaking regular transfer of information (N=226)



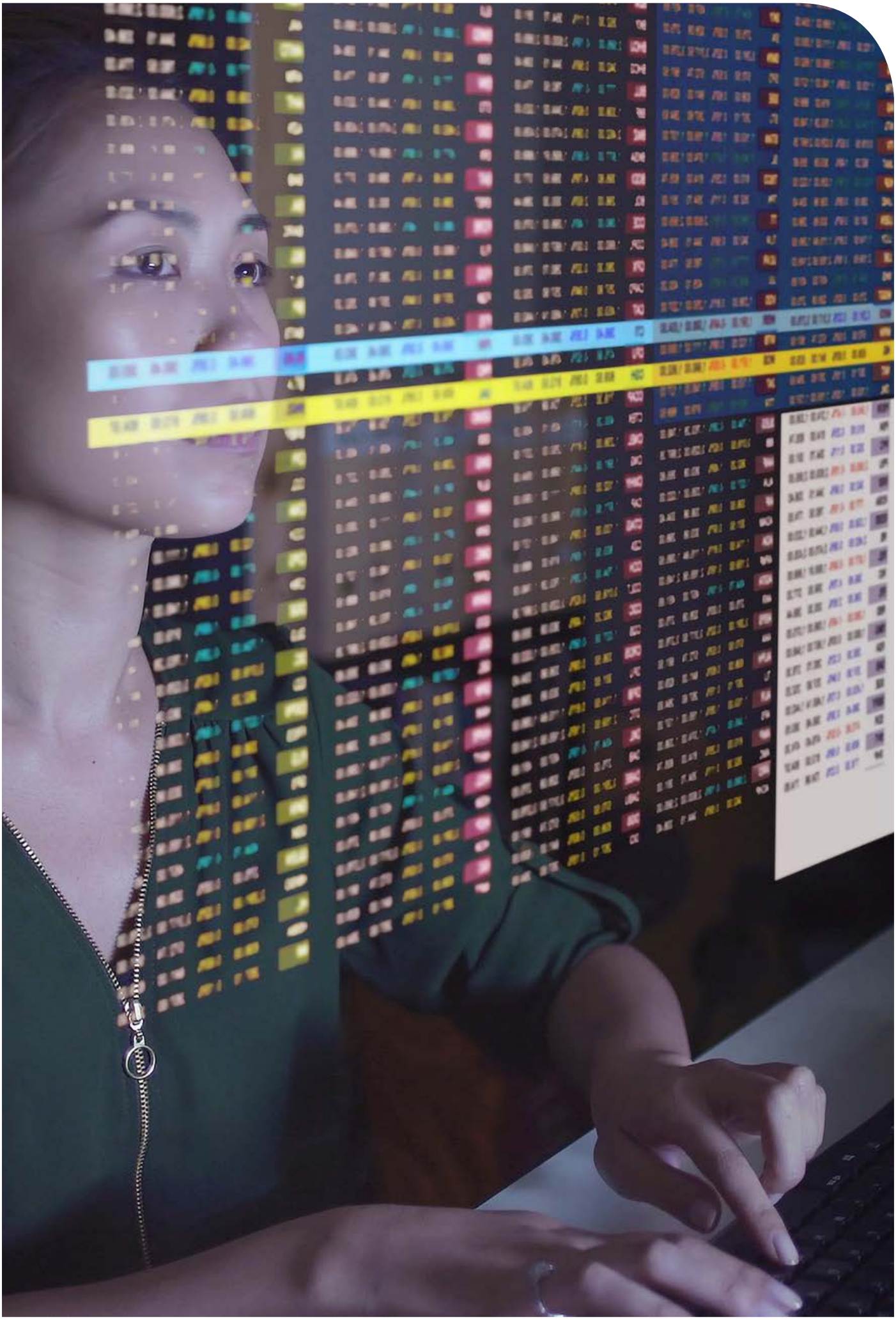
Observations

There are many opportunities to improve the regular implementation of disposal. These include:

- investing in and embedding appropriate automated tools for managing the information lifecycle;
- upskilling IM staff in the application of automated tools;
- understanding the value of sentencing from the point of creation;
- applying risk management techniques to disposal decision points; and
- supporting IM staff to effectively manage their organisation's information.

Upskilling staff in doing digital transfers would help improve regular disposal. This could include structuring digital assets in such a way to facilitate digital transfer.

With the challenges resulting from exponential growth in digital information, automating digital destruction would realise long-term benefits for organisations. It is important to note this transformation would also require the commitment of the organisation from the governance level.



Appendix 1

Public offices

The list below is the **176 Public Offices** surveyed. **168 have responded**. The response rate is **95.4%**. The eight public offices that did not respond before the close-off date for the survey were followed up. All offices apart from one contacted did submit a full or partial survey response, but none of the late responses could be included in the survey's analysis.

Organisation name	Response
Accident Compensation Corporation	Complete
Accreditation Council (Telarc SAI Ltd)	Complete
AgResearch Limited	Complete
Airways Corporation of New Zealand Limited	Complete
Animal Control Products Limited (Pestoff)	Complete
Ara Institute of Canterbury	Complete
Arts Council of New Zealand Toi Aotearoa (Creative NZ)	Complete
AsureQuality Limited	Complete
Auckland DHB	Complete
Auckland University of Technology	Complete
Bay of Plenty DHB	Complete
Broadcasting Commission (NZ On Air)	Complete
Broadcasting Standards Authority	Complete
Callaghan Innovation	Complete
Canterbury DHB	Complete
Capital and Coast DHB	Complete
Children's Commissioner	Complete
Civil Aviation Authority of New Zealand	Complete
Commerce Commission	Complete

Organisation name	Response
Counties Manukau DHB	Complete
Crown Irrigation Investments Limited	Complete
Crown Law Office	Complete
Department of Conservation Te Papa Atawhai	Late response
Department of Corrections Ara Poutama Aotearoa	Complete
Department of Internal Affairs	Complete
Department of the Prime Minister and Cabinet	Complete
Drug free Sport New Zealand	Complete
Earthquake Commission	Complete
Eastern Institute of Technology	Complete
Education New Zealand	Complete
Education Review Office Te Tari Arotake Mātauranga	Complete
Electoral Commission	Late response
Electricity Authority	Complete
Energy Efficiency and Conservation Authority	Complete
Environmental Protection Authority	Complete
External Reporting Board (XRB)	Complete
Financial Markets Authority	Complete
Fire and Emergency New Zealand	Complete
Game Animal Council (New Zealand Game Animal Council)	Complete
Government Communications Security Bureau Te Tira Tiaki	Complete
Government Superannuation Fund Authority	Complete
Guardians of New Zealand Superannuation (New Zealand Superfund)	Complete
Hawke's Bay DHB	Complete
Health and Disability Commissioner	Complete
Health Promotion Agency	Complete
Health Quality and Safety Commission	Complete
Health Research Council of New Zealand	Complete

Organisation name	Response
Heritage New Zealand (Pouhere Taonga)	Complete
Housing New Zealand Corporation	Complete
Human Rights Commission	Complete
Hutt DHB	Complete
Independent Police Conduct Authority	Complete
Inland Revenue Department Te Tari Taake	Complete
Institute of Environmental Science and Research Limited (ESR)	Complete
Institute of Geological and Nuclear Sciences Limited (GNS Science)	Complete
Judicial Conduct Commissioner	Complete
KiwiRail Holdings Limited	Complete
Kordia Group Limited	Complete
Lakes DHB	Complete
Land Information New Zealand Toitu te whenua	Complete
Landcare Research New Zealand Limited	Complete
Landcorp Farming Limited (Pāmu Farms of New Zealand)	Complete
Law Commission Te Aka Matua of te Ture	Complete
Lincoln University	Complete
Manukau Institute of Technology	Complete
Maritime New Zealand	Complete
Massey University Manawatu (Turitea)	Complete
Meteorological Service of New Zealand Limited	Complete
MidCentral DHB	Complete
Ministry for Culture and Heritage Te Manatū Taonga	Complete
Ministry for Pacific Peoples	Complete
Ministry for Primary Industries Manatū Ahu Matua	Complete
Ministry for the Environment Manatū Mō Te Taiao	Complete
Ministry for Women Minitatanga mō ngā Wāhine	Complete
Ministry of Business, Innovation and Employment	Complete

Organisation name	Response
Ministry of Defence Manatu Kaupapa Waonga	Complete
Ministry of Education Te Tāhuhu o te Mātaruranga	Complete
Ministry of Foreign Affairs and Trade Manatū Aorere	Complete
Ministry of Health	Complete
Ministry of Housing and Urban Development	Complete
Ministry of Justice – Courts	Complete
Ministry of Justice Tāhū o te Ture	Complete
Ministry of Māori Development (Te Puni Kōkiri)	Complete
Ministry of Social Development Te Manatū Whakahiato Ora	Complete
Ministry of Transport	Complete
Museum of New Zealand Te Papa Tongarewa Board	Complete
National Institute of Water and Atmospheric Research Limited (NIWA)	Complete
Nelson Marlborough District Health Board	Complete
Nelson Marlborough Institute of Technology (NMIT)	Complete
New Zealand Antarctic Research Institute (Antarctica New Zealand)	Complete
New Zealand Artificial Limb Service	Complete
New Zealand Blood Service	Complete
New Zealand Customs Service Te Mana Arai o Aotearoa	Late response
New Zealand Defence Force	Complete
New Zealand Film Commission	Complete
New Zealand Fish and Game Council and Fish and Game Councils	Complete
New Zealand Forest Research Institute Limited (Scion)	Complete
New Zealand Health Partnerships	Complete
New Zealand Lotteries Commission	Complete
New Zealand Parole Board	Complete
New Zealand Police	Complete
New Zealand Post Limited	Complete
New Zealand Productivity Commission	Complete

Organisation name	Response
New Zealand Qualifications Authority	Complete
New Zealand Security Intelligence Service Te Pā Whakamarumaru	Complete
New Zealand Symphony Orchestra	Complete
New Zealand Tourism Board (Tourism New Zealand)	Complete
New Zealand Trade and Enterprise	Late response
New Zealand Transport Agency	Complete
New Zealand Venture Investment Fund Limited	Complete
New Zealand Walking Access Commission (Ara Hīkoi Aotearoa)	Complete
Northland DHB	Complete
NorthTec (Tai Tokerau Wānanga)	Complete
Office of Film and Literature Classification	Complete
Office of the Clerk of the House of Representatives	Complete
Office of the Controller and Auditor-General	Complete
Office of the Ombudsman	Complete
Open Polytechnic of New Zealand	Complete
Oranga Tamariki – Ministry for Children	Complete
Otago Polytechnic	Complete
Pacific Media Network / National Pacific Radio Trust	Complete
Parliamentary Commissioner for the Environment	Complete
Parliamentary Counsel Office	Complete
Parliamentary Service (Te Ratonga Whare Pāremata)	Complete
Pharmaceutical Management Agency (PHARMAC)	Complete
Plant and Food Research	Complete
Privacy Commissioner Te Mana Mātāpono Matatapu	Complete
Public Trust	Complete
Quotable Value Limited	Complete
Radio New Zealand Limited	No response
Real Estate Authority (REA)	Complete

Organisation name	Response
Reserve Bank of New Zealand	Complete
Retirement Commissioner	Complete
Serious Fraud Office Te Tari Hari Tāware	Complete
Social Workers Registration Board	Late response
South Canterbury DHB	Complete
Southern District Health Board	Complete
Southern Institute of Technology	Complete
Sport and Recreation New Zealand (Sport New Zealand)	Complete
State Services Commission Te Komihana O Nga Tari Kāwangatanga	Complete
Statistics New Zealand	Complete
STRMix Limited	Late response
Tai Poutini Polytechnic	Complete
Tairawhiti DHB	Complete
Takeovers Panel	Complete
Taranaki DHB	Complete
Te Kāhui Whakamana Rua Tekau mā Iwa – Pike River Recovery Agency	Complete
Te Mangai Paho – Māori Broadcasting Funding Agency	Complete
Te Taura Whiri i Te Reo Māori (Māori Language Commission)	Complete
Te Wānanga o Aotearoa	Complete
Te Wānanga o Raukawa	Complete
Te Whare Wānanga o Awanuiārangi	Late response
Television New Zealand Limited	Complete
Tertiary Education Commission	Complete
The Māori Trustee (Te Tumu Paeroa)	Complete
The Treasury Kaitohutohu Kaupapa Rawa	Complete
Toi-Ohomai Institute of Technology	Complete
Transport Accident Investigation Commission	Complete
Transpower New Zealand Limited	Complete

Organisation name	Response
Unitec Institute of Technology	Complete
Universal College of Learning	Complete
University of Auckland	Complete
University of Canterbury	Complete
University of Otago	Complete
University of Waikato	Complete
Victoria University of Wellington	Complete
Waikato DHB	Complete
Waikato Institute of Technology (Wintec)	Complete
Wairarapa DHB	Complete
Waitemata DHB	Complete
Wellington Institute of Technology (Weltec)	Complete
West Coast DHB	Complete
Western Institute of Technology at Taranaki (WITT)	Complete
Whanganui DHB	Complete
Whitireia New Zealand (previously Whitireia Community Polytechnic)	Complete
WorkSafe New Zealand	Complete

Local authorities

The list below is the **78 local authorities** surveyed. 60 organisations have responded. The response rate is **76.9%**.

Organisation name	Response
Ashburton District Council	Complete
Auckland Council	Complete
Bay of Plenty Regional Council	Complete
Buller District Council	No response
Carterton District Council	Complete
Central Hawke's Bay District Council	No response
Central Otago District Council	Complete
Chatham Islands Council	Complete
Christchurch City Council	Complete
Clutha District Council	Complete
Dunedin City Council	Complete
Environment Canterbury (Canterbury Regional Council)	Complete
Environment Southland	Complete
Far North District Council	Complete
Gisborne District Council	Complete
Gore District Council	Complete
Greater Wellington Regional Council (Wellington Regional Council)	No response
Grey District Council	Complete
Hamilton City Council	Complete
Hastings District Council	No response
Hauraki District Council	Complete
Hawke's Bay Regional Council	No response
Horizons Regional Council (Manawatu-Wanganui Regional Council)	No response
Horowhenua District council	Complete
Hurunui District Council	Complete

Organisation name	Response
Hutt City Council	Complete
Invercargill City Council	Complete
Kaikoura District Council	No response
Kaipara District Council	No response
Kapiti Coast District Council	Complete
Kawerau District Council	No response
Mackenzie District Council	Complete
Manawatu District Council	Complete
Marlborough District Council	Complete
Masterton District Council	Complete
Matamata-Piako District Council	No response
Napier City Council	Complete
Nelson City Council	Complete
New Plymouth District Council	Complete
Northland Regional Council	Complete
Opotiki District Council	Complete
Otago Regional Council	No response
Otorohanga District Council	Complete
Palmerston North City Council	Complete
Porirua City Council	No response
Queenstown-Lakes District Council	Complete
Rangitikei District Council	Complete
Rotorua Lakes Council	Complete
Ruapehu District Council	Complete
Selwyn District Council	No response
South Taranaki District Council	Complete
South Waikato District Council	Complete
South Wairarapa District Council	No response

Organisation name	Response
Southland District Council	Complete
Stratford District Council	Complete
Taranaki Regional Council	Complete
Tararua District Council	Complete
Tasman District Council	Complete
Taupō District Council	Complete
Tauranga City Council	Complete
Thames-Coromandel District Council	Complete
Timaru District Council	Complete
Upper Hutt City Council	Complete
Waikato District Council	Complete
Waikato Regional Council	Complete
Waimakariri District Council	Complete
Waimate District Council	Complete
Waipa District Council	No response
Wairoa District Council	Complete
Waitaki District Council	Complete
Waitomo District Council	No response
Wellington City Council	Partial
West Coast Regional Council	No response
Western Bay of Plenty District Council	No response
Westland District Council	Complete
Whakatāne District Council	Complete
Whanganui District Council	Complete
Whangarei District Council	Complete

Appendix 2

Data tables

Table: Q3 What type of organisation are you responding on behalf of?

	Number	Percent
Public office	166	73%
Local authority	60	27%
Total	**226**	**100%**

Table: Q4 How many employees (full-time equivalent) currently work for your organisation?

	Number	Percent
Less than 10	7	3%
10 – 99	55	24%
100 – 299	46	20%
300 – 499	36	16%
500 – 2999	55	24%
3000 – 5999	14	6%
More than 6000	13	6%
Total	**226**	**100%**

Table: Q5 Please choose the statement that best describes your organisation's physical location(s)

	Number	Percent
Single location – single office	45	20%
Single location – multiple office in same town	46	20%
Multiple locations – head office and regional and / or international branches	135	60%
Total	**226**	**100%**

Table: Q6 What current drivers for good IM practice and processes are important to your organisation? You must provide an answer for all options.

	Strongly disagree		Mostly disagree		Mostly agree		Strongly agree		Don't know	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Business efficiency	0	0%	4	2%	60	27%	161	71%	1	0%
Risk management	0	0%	6	3%	58	26%	161	71%	1	0%
Collaboration across business groups	3	1%	8	4%	92	41%	120	53%	3	1%
Customer service delivery	3	1%	11	5%	82	36%	127	56%	3	1%
Compliance with legislative requirements	0	0%	9	4%	62	27%	154	68%	1	0%
Cost rationalisation / savings	6	3%	38	17%	118	52%	60	27%	4	2%
External collaboration (i.e. collaboration with external organisations)	8	4%	33	15%	111	49%	70	31%	4	2%

Table: Q7 What current IM challenges are applicable to your organisation? You must provide an answer for all options.

	Strongly disagree		Mostly disagree		Mostly agree		Strongly agree		Don't know	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Lack of understanding / awareness of value of IM	17	8%	45	20%	123	54%	40	18%	1	0%
IM not adequately addressed in planning phase of projects	20	9%	44	19%	93	41%	66	29%	3	1%
IM insufficiently funded / resourced	24	11%	58	26%	90	40%	51	23%	3	1%
'Silos' – lack of communication / collaboration across business groups	21	9%	45	20%	100	44%	56	25%	4	2%
Information incomplete / not providing evidence of decisions, etc	31	14%	84	37%	74	33%	30	13%	7	3%
Information not easily searchable / retrievable	27	12%	69	31%	84	37%	45	20%	1	0%

Table: Q8 Does your organisation have an active formal governance group in place for ensuring that IM requirements are considered at a strategic level?

	Number	Percent
Yes	68	30%
In development	54	24%
No	104	46%
Total	**226**	**100%**

Table: Q9 Is the Executive Sponsor and / or a member of the Information Management team part of this formal governance group?

	Number	Percent
No	3	4%
Yes	65	96%
Total	**68**	**100%**

Table: Q10 Does your organisation have any commitments related to Te Tiriti o Waitangi / the Treaty of Waitangi?

	Number	Percent
No	59	26%
Don't know	26	12%
Yes – Relationship agreement / Whakāetanga with post-settlement iwi	18	8%
Yes – Another type of agreement with iwi / Māori (e.g. Memorandum of understanding)	69	31%
Yes – Other(s) (please specify)	54	24%
Total	**226**	**100%**

Table: Q11 In the past 12 months, what activities has your organisation undertaken to ensure its IM meets Te Tiriti o Waitangi / the Treaty of Waitangi commitment arrangement(s)?

	Number	Percent
None	29	21%
Don't know	22	16%
Applied appropriate protocols for the management of information about whanau, iwi or hap?	26	18%
Applied appropriate protocols for the use / reuse of iwi / Māori related information	36	26%
Applied appropriate access controls for information that is of high interest to iwi / Māori	26	18%
Implemented metadata in Te Reo Māori (i.e. bilingual metadata)	12	9%
Implemented metadata for iwi / Māori concepts (i.e. concepts that are unique to the Māori worldview)	7	5%
Included in organisation-wide information strategy and / or policy	42	30%
Other(s)	30	21%

Table: Q12 In the past 12 months, what activities has your organisation undertaken to self-monitor its compliance with Archives New Zealand's requirements?

	Number	Percent
None	43	19%
Don't know	9	4%
Benchmarking exercise	22	10%
Independent assessment (i.e. assessment by a third party)	35	15%
Internal audit or review	78	35%
Process review	93	41%
Risk assessment	65	29%
Other (please specify)	59	26%

Table: Q13 In the past 12 months, what activities has your organisation undertaken to self-monitor its compliance with its own IM strategy, policy and processes?

	Number	Percent
None	43	19%
Don't know	5	2%
Benchmarking exercise	21	9%
Independent assessment (i.e. assessment by a third party)	37	16%
Internal audit or review	95	42%
Process review	98	43%
Risk assessment	63	28%
Other	60	27%

Table: Q14 What has the Executive Leadership Team and/or the IM Governance Group done with the findings from self-monitoring?

	Number	Percent
Not applicable, i.e. we have not done any self-monitoring	25	11%
Don't know	40	18%
Considered recommendations and begun a resourced action plan	73	32%
Considered recommendations but no action to be taken	6	3%
Considered recommendations but action deferred	11	5%
Considered recommendations but further analysis work required	24	11%
Recommendations yet to be considered	47	21%
Total	**226**	**100%**

Table: Q15 How many dedicated IM staff (FTE) are currently working in your organisation?

	Number	Percent
None	47	21%
1 FTE or less	55	24%
More than 1 – up to 3 FTE	58	26%
More than 3 – up to 6 FTE	30	13%
More than 6 – up to 10 FTE	16	7%
More than 10 FTE	20	9%
Total	**226**	**100%**

Table: Q16 In the past 12 months, what professional development activities have dedicated IM staff undertaken that helped them meet business needs? Tick all that apply

	Number	Percent
None	24	13%
Don't know	9	5%
Attended a conference (or similar event)	114	64%
Presented at a conference (or similar event)	33	18%
Training course (face-to-face and / or online)	106	59%
Secondment or another on-the-job training opportunity	22	12%
Studied towards a recognised qualification / professional accreditation or certification	37	21%
Other(s)	42	23%

Table: Q17 How does your organisation communicate their IM responsibilities to staff (including contractors and consultants) at all levels? Tick all that apply.

	Number	Percent
IM responsibilities are not communicated	9	4%
Don't know	3	1%
Contract / Code of conduct	92	41%
Job descriptions	99	44%
Induction training (face-to-face and / or online)	181	80%
Refresher training (face-to-face and / or online)	113	50%
Performance development plans / agreements	49	22%
Other(s)	70	31%

Table: Q18 Is your organisation undertaking any of the following activities to transition from paper-based to digital business processes? Tick all that apply.

	Number	Percent
None	9	4%
Don't know	1	0%
The organisation is already fully digital	9	4%
Making "digital-by-default" an underlining principle of organisational strategies	107	48%
Re-designing business processes and services to remove paper component	160	72%
Introducing digital authorisation and / or approval in business processes	130	58%
Scanning paper-based information at point of receipt as part of workflow	147	66%
Back-scanning of paper-based information (where the digital version becomes the authoritative version)	114	50%
Other(s)	44	19%

Table: Q19 Do you have an Information Asset Register that is current and in use?

	Number	Percent
Yes	34	15%
In development	51	23%
In planning phase	47	21%
No	94	42%
Total	**226**	**100%**

Table: Q20 Has your organisation identified its top high value and/or high-risk information?

	Number	Percent
Yes	144	64%
No	68	30%
Don't know	14	6%
Total	**226**	**100%**

Table: Q21 In the past 12 months, what activities has your organisation undertaken to actively manage its high value and/or high-risk information? Tick all that apply.

	Number	Percent
None	8	6%
Don't know	0	0%
Developed / implemented a Risk Mitigation Plan	41	28%
Created / reviewed a Business Continuity Plan	71	49%
Created / updated an Information Asset Register	31	22%
Planned / implemented new business system(s)	71	49%
Improved access and use controls	80	56%
Migrated information into new file formats and / or to long-term storage environment	63	44%
Other(s)	33	23%

Table: Q22 What key risks to its information has your organisation identified? Tick all that apply.

	Number	Percent
None	25	11%
Don't know	4	2%
Lack of offsite backup	13	6%
Information stored on obsolete or at-risk mediums (e.g. floppy disks) / file formats (e.g. WordStar files)	79	35%
Lack of contextual information to enable discovery and interpretation	118	52%
Information stored on business systems which are out-of-support	103	46%
Inadequate access and use controls for privacy and security	81	36%
Deterioration (of physical information and / or digital information stored on physical mediums)	72	32%
Storage failure (i.e. loss and / or corruption of data, inaccessible data, etc)	69	31%
Other(s)	58	26%

Table: Q23 Are requirements for creating, managing, storing and disposing of information built into your organisation's new business information systems (i.e. automated systems that create or manage data about your organisation's activities)?

	Number	Percent
Yes	51	23%
Partially	140	62%
No	33	15%
Don't know	2	1%
Total	**226**	**100%**

Table: Q24 Which of the following represent challenges for ensuring that requirements for creating, managing, storing and disposing of information are built into those business information systems?

	Number	Percent
Don't know	4	2%
Number of systems in use	106	61%
Age of systems in use	91	52%
Lack of awareness amongst vendors responsible for designing / upgrading systems	78	45%
Lack of capability / awareness amongst internal staff responsible for system build	96	55%
Lack of IM staff consultation in new systems being acquired / implemented	107	61%
Lack of management support / buy-in	47	27%
Other(s)	40	23%

Table: Q25 Does your organisation's current document and records management system (Enterprise Content Management, Electronic Document and Records Management, and / or Document Management systems) meet Archives New Zealand's Minimum requirements for metadata (16/G7)?

	Number	Percent
Yes	123	54%
Partially	47	21%
No	12	5%
Don't know	12	5%
Not applicable	32	14%
Total	**226**	**100%**

Table: Q26 In the past 12 months, what activities has your organisation undertaken to make sure digital information of long-term value (i.e. required beyond ten years) remains reliable, usable and complete over time? Tick all that apply.

	Number	Percent
None	44	19%
Don't know	18	8%
Developed / implemented a digital storage management plan	35	15%
Addressed long-term retention and access requirements during system changes	79	35%
Migrated to new file formats	47	21%
Migrated to long-term digital storage environment	55	24%
Monitored integrity of static information using checksums	11	5%
Tested capability of systems to create and maintain information and associated metadata	48	21%
Other(s)	49	22%

Table: Q27 Does your organisation hold any digital information that it can no longer open?

	Number	Percent
Yes	72	32%
No	94	42%
Don't know	60	27%
Total	**226**	**100%**

Table: Q28 What are the main reasons you cannot open that digital information? Tick all that apply.

	Number	Percent
Don't know	2	3%
Inadequate metadata to easily locate information	25	35%
Information stored in obsolete file format(s)	54	75%
Information stored in personal systems which are inaccessible to the organisation (e.g. One Drive)	31	43%
Software needed to access information no longer available	39	54%
Physical deterioration of the medium (e.g. CD-ROMs)	23	32%
Storage failure	8	11%
Other(s)	16	22%

Table: Q29 In the past 12 months, has your organisation had difficulty responding to requests for official information under the OIA 1982 or the LGOIMA 1987 because:

	Strongly disagree		Mostly disagree		Mostly agree		Strongly agree		Don't know	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
The information did not exist (i.e. the record had not been created)?	109	48%	59	26%	32	14%	6	3%	20	9%
The information existed but could not be found?	116	51%	60	27%	27	12%	8	4%	15	7%

Table: Q30 In the past 12 months, what major system, service and/or other business change has your organisation undergone that had implications for IM? Tick all that apply.

	Number	Percent
None	45	20%
Don't know	2	1%
Established new function(s) (as a result of Administrative Change)	58	26%
Received and / or transferred information from / to another organisation (as a result of Administrative Change)	40	18%
Implemented new business system(s)	129	57%
Decommissioned business system(s)	76	34%
Implemented new service offering(s)	81	36%
Migrated information between systems and / or to a new storage environment	126	56%
Other(s)	20	9%

Table: Q31 Did your organisation take measures to guarantee security and preserve the integrity of the information impacted by those changes (as selected in the previous questions)? You must provide an answer for all options.

	Strongly disagree		Mostly disagree		Mostly agree		Strongly agree		Don't know	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Established new function(s) (as a result of Administrative Change)	0	0%	1	2%	28	48%	24	41%	5	9%
Received and / or transferred information from / to another organisation (as a result of Administrative Change)	0	0%	3	8%	13	32%	23	57%	1	2%
Implemented new business system(s)	1	1%	6	5%	51	40%	66	51%	5	4%
Decommissioned business system(s)	0	0%	4	5%	29	38%	40	53%	3	4%
Implemented new service offering(s)	0	0%	6	7%	36	44%	37	46%	2	2%
Migrated information between systems and / or to a new storage environment	1	1%	3	2%	33	26%	88	70%	1	1%
Other(s)	1	6%	2	11%	6	33%	9	50%	0	0%

Table: Q32 Do the facilities your organisation uses to store physical information have measures in place to protect against unauthorised access, alteration, loss and destruction? You must provide an answer for both options.

	Strongly disagree		Mostly disagree		Mostly agree		Strongly agree		Don't know		Not applicable	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Onsite facilities	4	2%	16	7%	107	47%	96	42%	0	0%	3	1%
Offsite facilities	3	1%	3	1%	34	15%	152	67%	1	0%	33	15%

Table: Q33 Do the systems and/or services your organisation uses to store digital information include mechanisms to protect against unauthorised access, alteration, loss, deletion and destruction? You must provide and answer for both options.

	Strongly disagree		Mostly disagree		Mostly agree		Strongly agree		Don't know		Not applicable	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent	Number	Percent
In-house / on-premise systems	2	1%	7	3%	80	35%	133	59%	0	0%	4	2%
Cloud services	1	0%	4	2%	75	33%	110	49%	10	4%	26	12%

Table: Q34 How much of your organisation's information over 25 years old has been classified as either open or restricted?

	Number	Percent
100	16	7%
75 – less than 100	18	8%
50 – less than 75	12	5%
25 – less than 50	8	4%
1 – less than 25	50	22%
Don't know	80	35%
Not applicable	42	19%
Total	**226**	**100%**

Table: Q35 What percentage of information created and maintained by your organisation is covered by applicable disposal authorities?

	Number	Percent
1 – less than 25	19	8%
25 – less than 50	15	7%
50 – less than 75	15	7%
75 – less than 100	51	23%
Don't know	41	18%
Full coverage	85	38%
Total	**226**	**100%**

Table: Q36 When does your organisation plan to appraise / identify and assess the value of the information not covered by applicable disposal authorities?

	Number	Percent
We are currently appraising	24	17%
In the next 12 months	21	15%
In the next 1 to 3 years	58	41%
In the next 4 to 5 years	11	8%
In over 5 years time	1	1%
Don't know	26	18%
Total	**141**	**100%**

Table: Q37 In the past 12 months, what disposal activities has your organisation undertaken to implement the authorised disposal of information? Tick all that apply.

	Number	Percent
None	48	21%
Don't know	13	6%
Developed a disposal implementation plan	42	19%
Sentenced information in offsite storage	85	38%
Sentenced unstructured information in business information systems and / or shared drives	49	22%
Set-up automated disposal in Enterprise Content Management system (or similar)	26	12%
Used automated tools to analyse digital files in preparation for transfer (e.g. DROID)	4	2%
Obtained approval to dispose of information from business owners	117	52%
Other(s)	45	20%

Table: Q38 What percentage of your organisation's information has been sentenced using applicable disposal authorities?

	Number	Percent
100	16	7%
75 – less than 100	22	10%
50 – less than 75	16	7%
25 – less than 50	22	10%
1 – less than 25	61	27%
None	41	18%
Don't know	48	21%
Total	**226**	**100%**

Table: Q39 In the past 12 months, has your organisation undertaken (approved and authorised) destruction of information?

	Number	Percent
No	75	33%
Yes – Both physical and digital	58	26%
Yes – Digital only	6	3%
Yes – Physical only	87	38%
Total	**226**	**100%**

Table: Q40 Which of the following challenges for undertaking regular (approved and authorised) destruction of information apply to your organisation? Tick all that apply.

	Number	Percent
Not applicable	24	11%
Don't know	4	2%
Lack of resources put towards sentencing activity	144	64%
Lack of confidence sentencing has been done accurately	46	20%
Cost of secure destruction / deletion through the storage provider	42	19%
Difficult to obtain approvals / sign-off from business owners	46	20%
Not seen as a priority for staff responsible for deletion of information in systems (e.g. IT staff)	82	36%
Systems have not been set-up to automate regular authorised destruction	157	69%
Other(s)	41	18%

Table: Q41 In the next 12 months, is your organisation planning to transfer any physical information (as identified for transfer in applicable disposal authorities)?

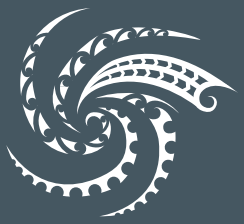
	Number	Percent
Yes – to an Archives New Zealand repository: Auckland, Christchurch, Dunedin	24	11%
Yes – to an Approved Repository	10	4%
Yes – to a Local Authority archive	23	10%
No – no plan to transfer in the next 12 months	127	56%
Not applicable – plan to transfer but Wellington repository is closed	31	14%
Not applicable – there is no Local Authority archive to transfer to	11	5%
Total	**226**	**100%**

Table: Q42 In the next 12 months, is your organisation planning to transfer any digital information (as identified for transfer in applicable disposal authorities) to the Government Digital Archive (if you are a public office) or to a Local Authority digital archive (if you are a local authority)?

	Number	Percent
No	181	80%
Yes	23	10%
Not applicable	22	10%
Total	**226**	**100%**

Table: Q43 Which of the following represent challenges for undertaking regular transfer of information by your organisation?

	Number	Percent
Don't know	15	7%
Lack of resources put towards sentencing activity	132	58%
Lack of confidence that sentencing has been done accurately	42	19%
Not a priority for senior management	68	30%
Lack of resources and / or tools to prepare transfer	114	50%
Lack of experience / skills in doing physical transfers	64	28%
Lack of experience / skills in doing digital transfers	88	39%
Difficult to obtain approvals / sign-off from business owners	28	12%
Difficult to understand Archives New Zealand's processes and requirements	41	18%
Archives New Zealand's Wellington repository is not taking transfer of physical information	62	27%
No Local Authority archive to transfer to	20	9%
Other(s)	53	23%



Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

New Zealand Government