Findings report

Survey of public sector information management 2019/20

He pūrongo kitenga

He tirohanga ki te whakahaere mōhiohio rāngai tūmatanui 2019/20

Te Rua Mahara o te Kāwanatanga
ARCHIVES NEW ZEALAND

New Zealand Government

Contents

Chief Archivist's foreword

Tēnā koe

One of the key roles of Archives New Zealand is to support democratic and accountable government. Records capture the processes, decision-making and actions of government. Therefore, access to reliable, accessible and complete information helps New Zealanders to hold government to account and participate in democratic processes. An important part of our mahi is regulating how government organisations create and manage their information and keeping track of how well they're doing it. Audits and annual surveys are the primary tools we use to measure this.

This findings report highlights several areas for improvement across government information management (IM). These range from informing outsourced providers about their IM responsibilities, to actively maintaining the usability of digital information with long-term value, and removing roadblocks to regular, routine and transparent disposal.

It's also timely to revisit the key indicators for the survey that were reported in the recent Report on the State of Government Recordkeeping. They show an increase in the number of governance groups for IM and decreases in the number of agencies identifying their most important information and building IM requirements into new business systems. The findings about digital recordkeeping are particularly concerning. Only half of respondents that implemented a new business system in the past 12 months have built in IM requirements, yet this has been mandatory for over a decade.

Collectively, these findings provide a basis for us to target or adapt our regulatory work. One of my top priorities as Chief Archivist is preserving the digital record of government. If digital information isn't well looked after before it comes under my control, chances are there won't be anything much to preserve or access. We risk 'digital amnesia' and a gap in the memory of government. So, addressing the findings around usability and persistence of digital information, as well as the technology wrapped around it, are of utmost importance.

The findings from the survey help to shape our work over the coming year and what we engage on with the organisations we regulate. Although there was a good overall response rate to this year's survey, I want to remind public offices that they have a legal obligation to respond to my directions to report. It gives us an evidence base for understanding where we need to better support organisations, so it ultimately delivers value to those who participate.

Ngā mihi nui

Stephen Clarke
Chief Archivist Kaipupuri Matua

1.0 Overview

Monitoring is a key regulatory tool for assuring that public sector information is being well-managed. It is critical for maintaining confidence in the quality and stewardship of information, and for empowering public sector organisations to lift their performance.

Regular surveys are one of the core mechanisms that Archives New Zealand uses to collect information for monitoring purposes. They are part of our *Monitoring Framework*, which guides our monitoring activities and outputs.

Key findings from this year's survey are covered at the end of each main section:

- *Governance, capability and self-monitoring*
- *Creation and management*
- *Disposal*
- *IM environment*

Purpose of the report

Each year, we produce two publications that present analysis of the latest survey: the *Chief Archivist's Annual Report on the State of Government Recordkeeping* and a full findings report.

The Chief Archivist's Annual Report is the primary commentary and the main driver for the survey. It focuses on five key indicators that we use to measure and track the overall state of public sector information management (IM) over time. It also includes recommendations for public sector organisations and Archives New Zealand.

The purpose of this findings report is to present analysis of the full dataset for the 2019/20 survey. The survey data is published as a companion to this report and is available on *data.govt.nz*.

Survey objectives

The annual survey helps us to:

- Form a picture of how well public sector organisations are performing as-a-whole against the requirements of the Public Records Act 2005 (PRA) mandatory standards and good practice IM.
- Track improvements in organisations' performance over time.
- Identify risks, challenges, opportunities and emerging trends affecting IM in organisations, so we can feed this intelligence into responsive regulation.
- Provide public visibility of organisations' IM performance.

Survey questionnaire

The survey questionnaire (Appendix 1) consists of:

- A core set of questions that are based on the monitoring criteria (Appendix 2) from our Monitoring Framework. Most of these questions are repeated from survey-to-survey. They form the bulk of this report.
- A set of questions concerning risks, challenges, opportunities and emerging trends that are affecting IM in organisations. These questions are designed to help us be a more responsive regulator and can change from survey-to-survey. They are addressed in the IM Environment section of this report.

Organisations surveyed

Archives New Zealand's remit covers both central and local government, which we refer to collectively as public sector organisations. We use different monitoring mechanisms for different types of organisation within our remit.

The annual survey covers all central government organisations, referred to by the Public Records Act 2005 (PRA) as 'public offices', except for Ministers of the Crown and school boards of trustees. It also covers local authorities (i.e. councils) but excludes council-controlled organisations.

This year the survey was sent to 270 public sector organisations, including:

- 192 public offices, which were required to respond by direction to report (s31, PRA).
- 78 local authorities, which were invited to respond.[1]

The questionnaire was delivered via the online survey tool SurveyMonkey and was open from 20 July to 7 August 2020. Executive Sponsors from organisations in scope were invited to participate and were asked to coordinate their organisation's response.

1 These figures vary slightly from those reported in the recent Chief Archivist's Report on the State of Government Recordkeeping. A coding error in the survey distribution list was identified post-publication, whereby a public office had been incorrectly coded as a local authority. This error was not replicated in the survey data and did not impact other analysis reported on in either publication.

Response rates

The survey recorded an 80% response rate. We received one unsolicited response, two late responses and five incomplete responses, all of which were excluded from the analysis. We also received one response from a council-controlled organisation which was included in the overall analysis but was excluded from any analysis specific to local authorities.

A total of 47 organisations did not respond, comprising 22 public offices and 25 local authorities. Complete responses were received from the Government Communications Security Bureau and New Zealand Security Intelligence Service, but these have been excluded from the analysis.

A list of respondents and non-respondents is included in Appendix 3.

Acronyms and definitions

We use the following acronyms throughout the report:

AV – audio-visual

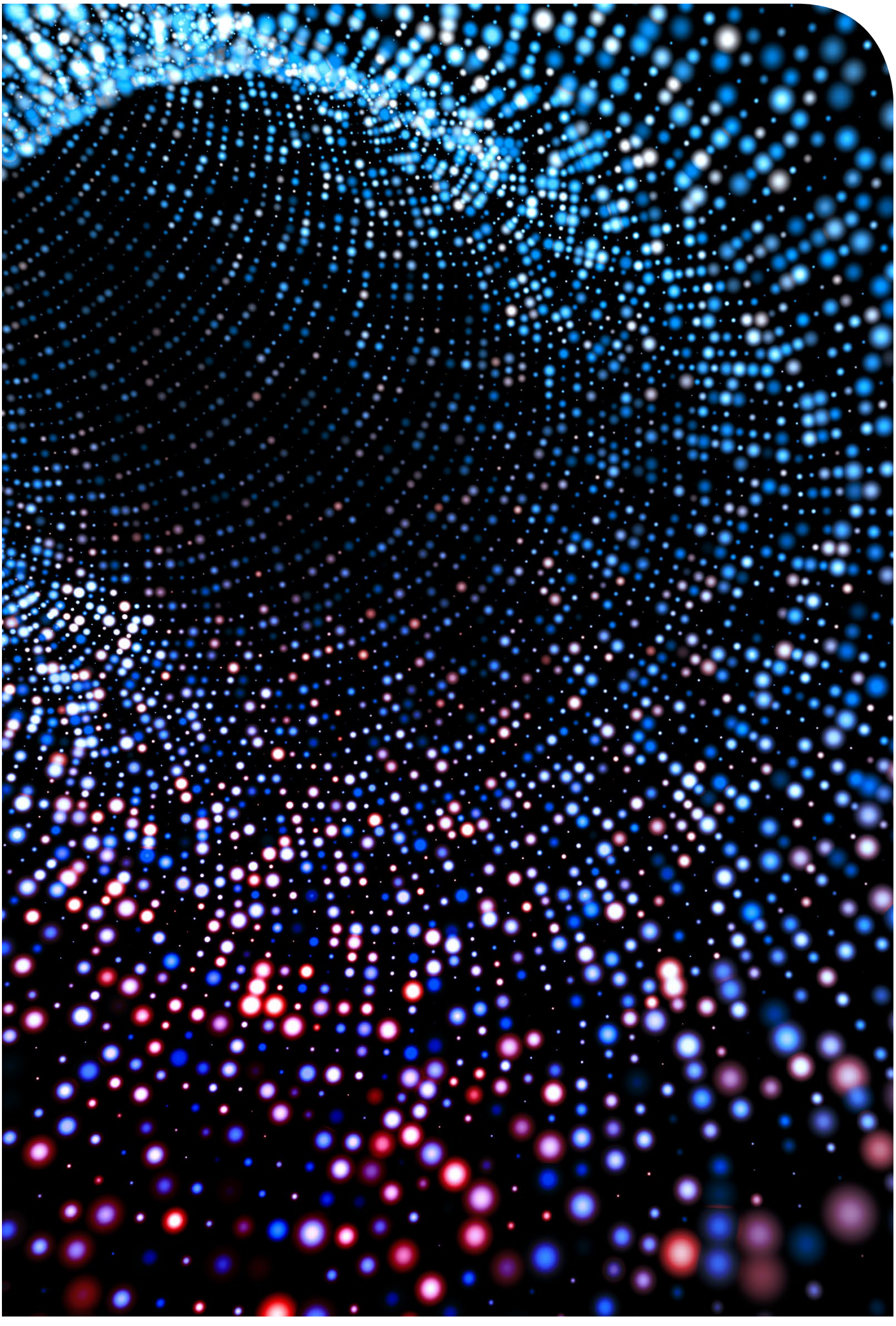
IAR – information asset register

IM – information management

FTE – full-time equivalent

PRA – Public Records Act 2005

Shadow IT – the use of unapproved systems, applications or services



2.0

Governance, capability and self-monitoring

This section covers the people component of IM:

- The people within an organisation who set the direction for IM, specialise in IM, or have IM responsibilities.
- The rights of people outside the organisation, specifically iwi/Māori, that must be acknowledged and addressed.
- The routine self-monitoring that supports the ongoing health of IM in an organisation.

Governance groups and Executive Sponsors

Why it is important

The role of an active governance group is to make sure, at a strategic level, that IM requirements are considered when developing organisational strategies and policies and implementing systems and processes. It is a foundation for elevating the importance of IM in organisations and integrating it into business operations.

An Executive Sponsor holds responsibility for the oversight of IM in their organisation and reports to the administrative head (usually the Chief Executive). They champion IM at a strategic level and are our main point of contact for monitoring and reporting on compliance. As such, we expect to see them actively involved in IM governance groups.

Ideally an IM governance group should:

- Meet a minimum of twice a year to be considered 'active'.
- Have a direct reporting line to the Chief Executive and senior leadership team.
- Involve staff with IM expertise and facilitate partnership between IM and related business activities, such as ICT, privacy, security and data management.
- Have the authority to plan, direct and allocate funding to IM.

Not all organisations need to have a group that is solely dedicated to IM governance. For smaller organisations, it may be more practical to bring IM governance within the mandate of an existing governance group that has wider responsibilities.

What we asked

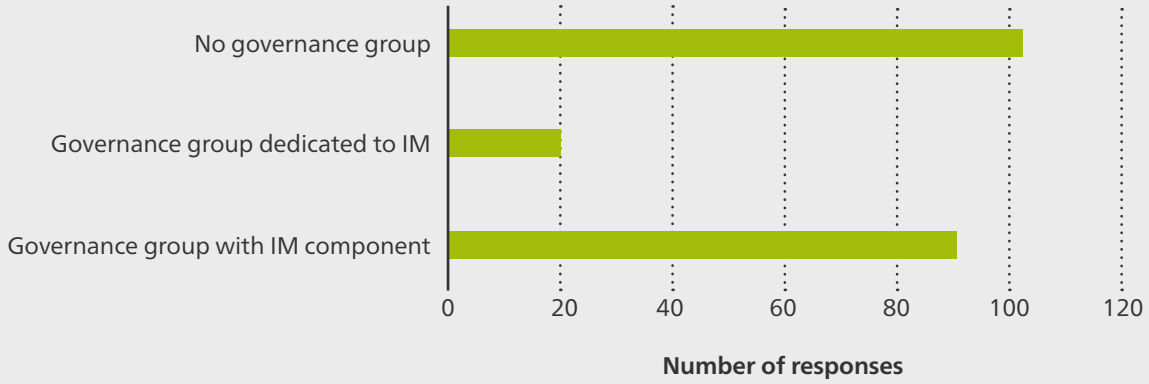
We asked survey participants if:

- They have a formal governance group which is either dedicated to IM or has IM oversight as part of its mandate (Q.9.).
- That group meets at least twice a year (Q.10).
- The Executive Sponsor is part of that group (Q.11).

Findings

Figure 1 shows the frequency and type of governance groups in place. Just over half of all respondents (52%) have a formal governance group in place. Notably, only 9 out of 52 (37%) local authorities have a governance group in place. Most of the respondents that do have a formal governance group in place said that the group meets at least twice a year (92%) and that their Executive Sponsor is part of the group (86%).

Figure 1: Frequency and type of IM governance groups



IM capability

Why it is important

To implement effective IM, an organisation needs to be sufficiently resourced with appropriate and up-to-date IM skills. IM is a distinct, well-established field of expertise. IM specialists interact with a wide range of other business activities to help an organisation meet IM requirements.

Resourcing IM can be achieved by employing dedicated IM staff and/or contracting third-party providers as required. For smaller organisations, it may be more practical to include the IM specialism within a multi-disciplinary role. Whichever way an organisation chooses to resource IM, it needs to make sure that staff have the appropriate experience, qualifications and training to fulfil the IM component of their role.

As new technologies proliferate at speed, the opportunities and challenges for meeting IM requirements also multiply. In this environment, IM specialists need to regularly maintain and grow their knowledge and skills so that they can best support their organisation. We expect senior leaders to enable ongoing professional development for IM specialists.

People and their actions are also an important component of effective IM. Almost everyone employed or contracted by an organisation creates, modifies, accesses and uses information. Some people are also responsible for the systems that hold that information, or the processes and services that generate it and rely on it to function. Senior leaders are responsible for providing direction and support for IM. We expect organisations to make sure that their people know about, understand and meet their responsibilities. This includes contractors and consultants.

What we asked

We asked survey participants:

- How many full-time-equivalent (FTE) staff are dedicated to IM (Q.5).[2]
- What professional development activities those staff have done in the last 12 months (Q.6).
- If and how the organisation informs staff, contractors and consultants about their IM responsibilities (Q.18 and Q.19).

Findings

79 percent of respondents have some dedicated, specialised IM resources and the mean number of IM staff is 2.7.[3] Figure 2 shows the level of IM-focused staff split by organisation size. Although there is a clear trend towards fewer IM-focused staff in smaller organisations (fewer than 300 staff) overall there does not seem to be an obvious relationship between organisation size and level of staff dedicated to IM.

59 percent of respondents said that their IM staff had participated in professional development activities. Conference attendance and training courses are the most common activities (Figure 3).

While most respondents indicated that they inform staff at all levels of their IM responsibilities (94%) the rate is lower for contractors (54%) and consultants (41%). A high proportion of respondents said that they use induction training to communicate responsibilities (80%). Around half of respondents reported using refresher training, contracts and codes of conduct (Figure 4). Job descriptions and performance development plans are used far less frequently. Other communications methods mentioned in the comments, in addition to those listed in Figure 4, include:

- Policies, procedures and processes.
- System-specific training.
- Confidentiality and/or privacy agreements.
- Self-service knowledge bases.
- Regular newsletters.

2 This question specifically excludes staff whose work is in geographic information systems, business intelligence, data management or medical records, as well as staff whose core duties are not IM-focused.

3 To calculate the mean, all responses that specified 'less than 0.5 FTE' were set to 0.25.

Figure 2: Number of IM FTEs compared with organisation size

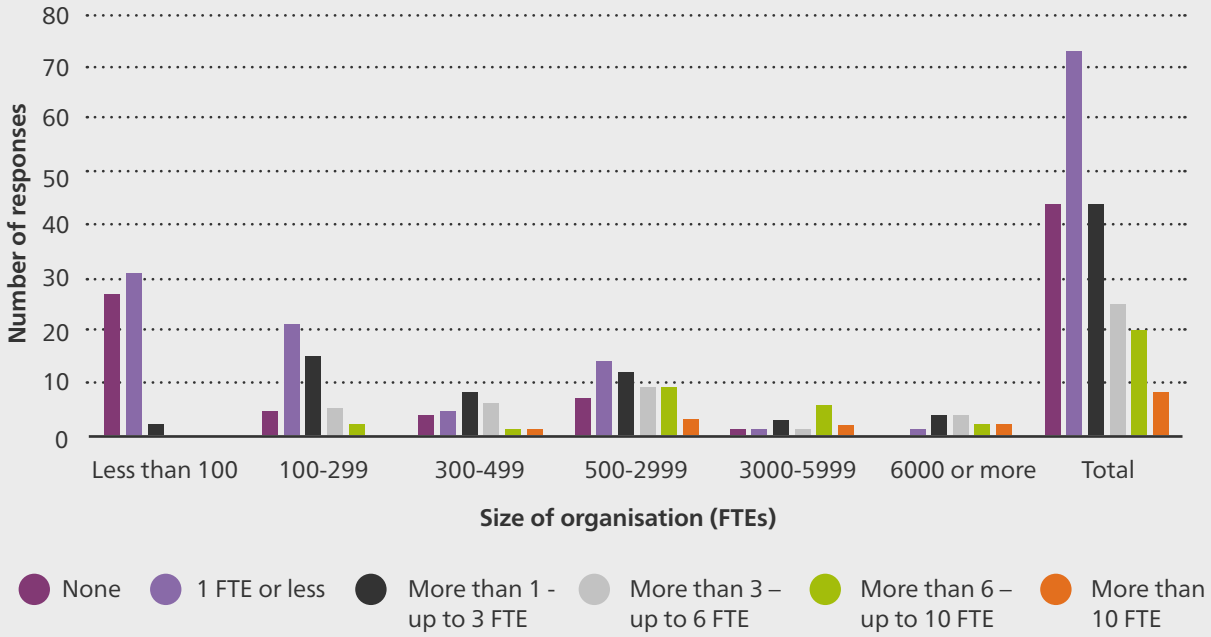


Figure 3: Professional development activities for IM staff

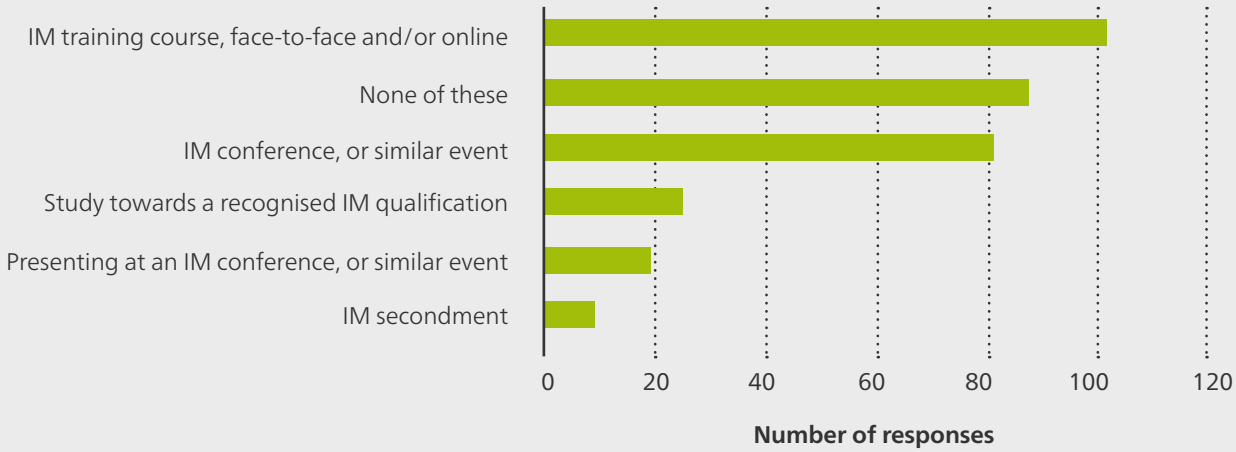
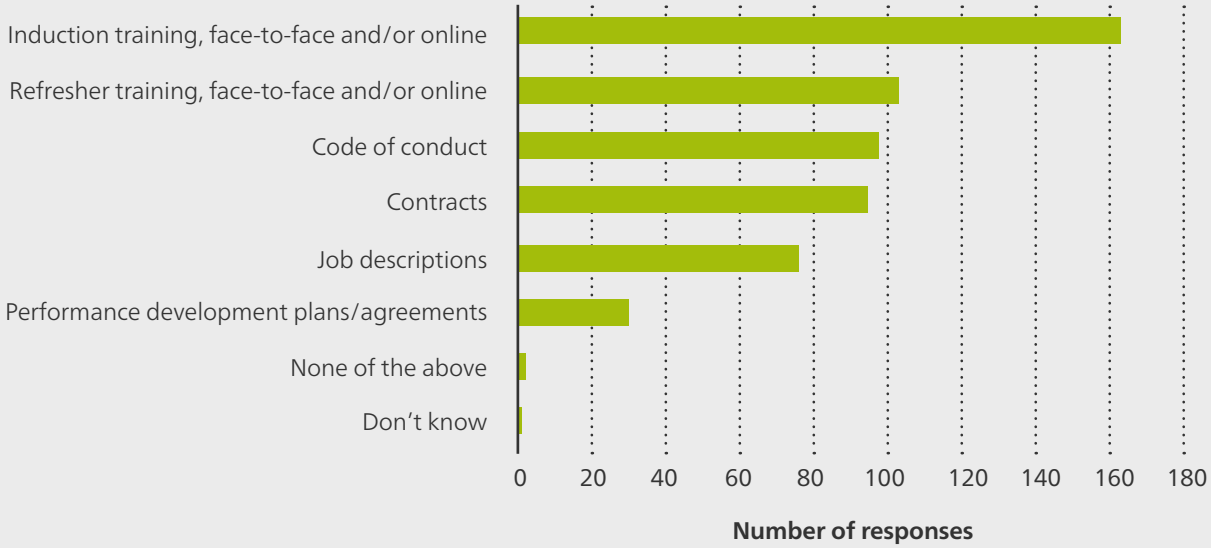


Figure 4: How organisations inform staff, contractors and consultants about their IM responsibilities



Te Tiriti o Waitangi

Why it is important

Te Tiriti o Waitangi (Te Tiriti) and its principles of partnership, participation and protection underpin the relationship between the Government and Māori. As the regulator for government information management, we uphold these principles by supporting the rights of Māori to access, use and reuse information.

Many public sector organisations create and hold information that is important to whānau, hapū and iwi. We expect organisations to:

- Identify what information is important to Māori.
- Manage that information so it is easily identifiable, accessible and usable for Māori.
- Understand the IM implications for the organisation resulting from Treaty settlements or other agreements with Māori.

What we asked

We asked survey participants:

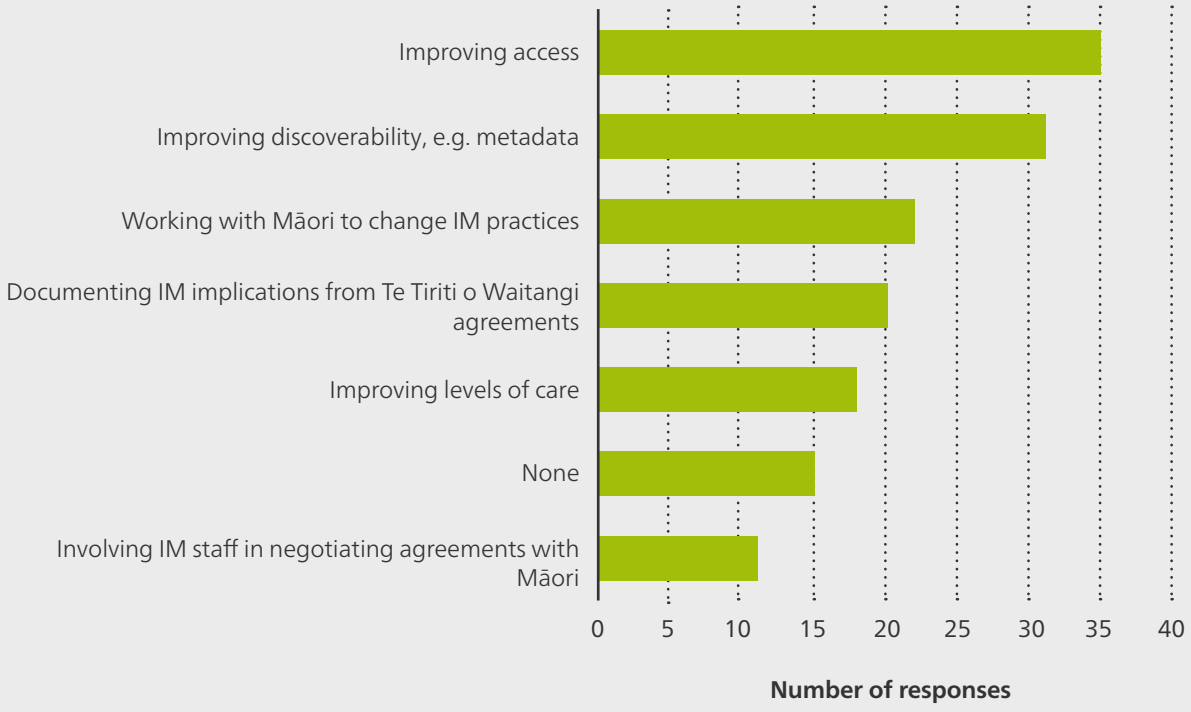
- If the organisation has identified information it holds that is important to Māori (Q.12).
- What the organisation has done to improve use of that information (Q.13).

These questions are different from the questions we asked in last year's survey. Last year we asked about activities organisations were undertaking to meet their commitments under Te Tiriti.

Findings

39 percent of respondents said that they have identified information that is of importance to Māori. Those respondents told us more about what activities they are doing to improve usage (Figure 5). 'Improving access' was the most common activity. A few respondents provided details on what they were doing to improve access, for example, by aggregating information of interest to local iwi into online resources. A significant proportion of the 61 percent of respondents that provided a negative response ('no', 'don't know', or 'don't hold any') conduct business that potentially intersects with the interests of Māori, such as health, education, employment, environment, or natural resources.

Figure 5: Activities to improve usage of information that is of importance to Māori



Self-monitoring

Why it is important

Regular self-monitoring is critical for ensuring that an organisation's IM continues to be compliant and fit-for-purpose. Over time, there are inevitable changes to an organisation's internal and external environment that can impact its IM and information needs. Even the most effective IM is susceptible to change. Types of change include:

- New or amended legislation, standards and other regulatory instruments.
- New business functions, risks, technologies, or services.
- Changes to government policy or the organisation's strategic priorities.
- Privacy or security breaches.
- New commitments for cultural redress made as part of Treaty settlements.

We expect organisations to not only monitor their IM but identify areas for improvement and take action to make those improvements.

What we asked

We asked survey participants:

- If they have done any self-monitoring in the last 12 months and what methods were used (Q.14 and Q.15).
- What actions were taken as a result of self-monitoring (Q.16).

Findings

70 percent of respondents said that they have done self-monitoring in the last 12 months. 51 percent have monitored against our requirements, while 52% have monitored against their own IM policy. A review of processes is the most common activity (Figure 6). Other self-monitoring methods mentioned in the open comments include internal surveys, data and information assessments, IM health checks and maturity assessments.

The majority of 149 respondents that have done self-monitoring in the last 12 months (64%) are focused on developing or finalising action plans (Figure 7). A smaller proportion of respondents (38%) are progressing towards implementing actions or completing implementation.

Figure 6: Methods used to self-monitor

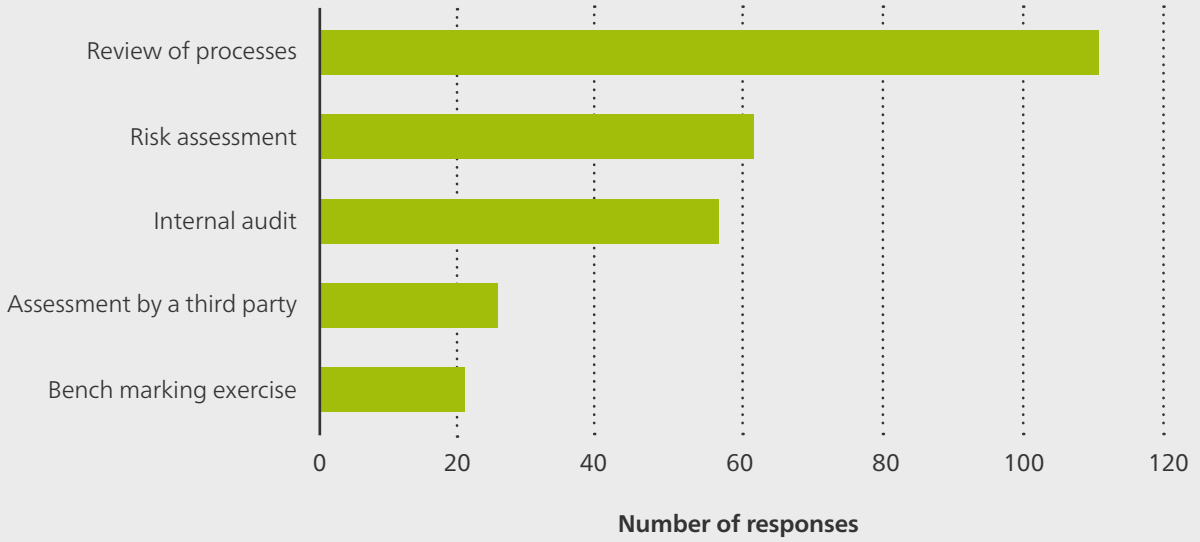
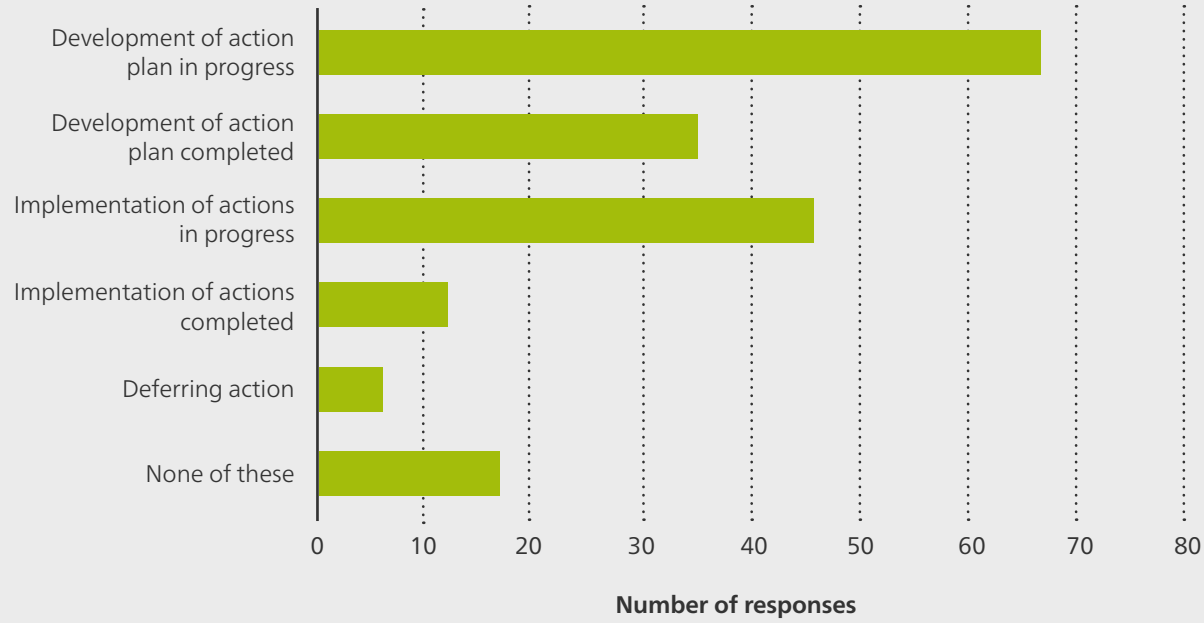
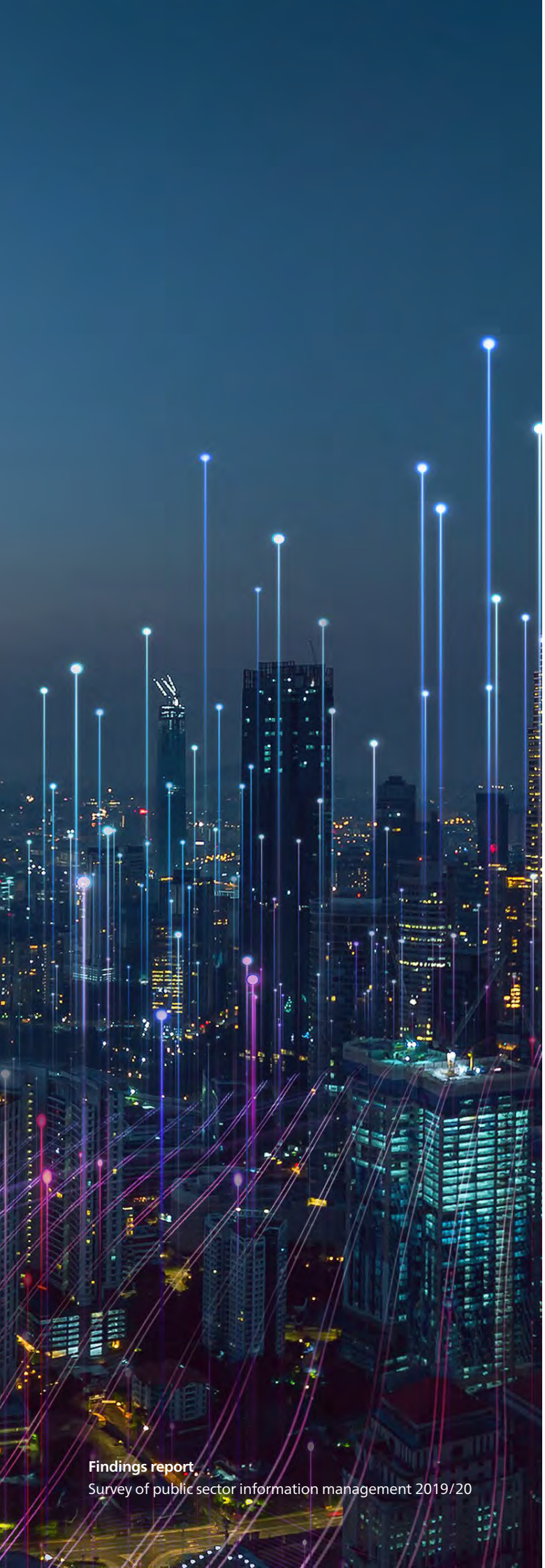


Figure 7: Steps taken as a result of self-monitoring





Key findings

The reported rates at which respondents communicate IM responsibilities for contractors and consultants should be higher. Organisations often employ external parties to perform key business functions and activities. Certain information created, received or generated through outsourced business belongs to the organisation and is subject to the PRA. For this reason, any contract with an outsourced provider should include clauses relating to IM. We recommend that organisations revisit our guidance on *Outsourcing Business*. As part of the audit programme, we have asked auditors to report back to us on organisations that consistently omit IM requirements from their outsourcing contracts.

There seems to be low awareness among respondents about how the information they hold intersects with the interests of Māori. If public sector organisations do not understand the varied information needs of Māori and how those needs connect with the information they hold, then chances are they are not creating and managing that information in ways that support those needs.

Although many respondents are doing self-monitoring, we would like to see more of them using their findings to carry out improvements to IM. We made a similar finding concerning self-monitoring in *last year's survey findings report*, so it stands out as an area of IM practice that may need further encouragement on our part.

For recommendations concerning governance groups and numbers of IM staff, see the *Chief Archivist's Annual Report on the State of Government Recordkeeping 2019/20*.

3.0

Creation and management

This section covers the activities that support the core requirements mandated by the Public Records Act 2005, i.e. the requirements to:

- Create information.
- Maintain (or manage) information.
- Maintain information in accessible form.

Disposal is a component of managing information but for conciseness we have addressed it in a separate section.

High-value/high-risk information

Why it is important

The reason we emphasise high-value/high-risk information in our standard, guidance and monitoring work is to make sure that organisations are targeting their efforts at the information in greatest need of effective management. Exactly what information is considered high-value/high-risk information will depend on an organisation's business. An organisation may have a different perspective on what information is high-value/high-risk than its external customers.

For an organisation, high-value information is information that is critical to performing its core, legislated functions. High-risk information is information that, if mismanaged, could expose the organisation to major financial or material loss, breach of statutory obligations, or loss of reputation.

For New Zealanders, high-value information is information that supports their individual or collective rights, entitlements, identity and aspirations. High-risk information is information that, if mismanaged, could result in public harm. Actions such as improper release of information or barriers to access can have real-world impacts on their lives. Those impacts can include physical, emotional and psychological harm.

We expect details about high-value/high-risk information assets to be captured in some way, so that the organisation can manage accessibility and usability, mitigate risks that might affect the assets and manage their relevance, currency, retention and disposal. It is important that identification and capture is iterative, because change is constant. Using an information asset register (IAR) is one way to capture information assets, but we acknowledge that traditional, spreadsheet-based IARs can be time-consuming to create and maintain. Increasingly, there are technologies available that can make this task easier.

What we asked

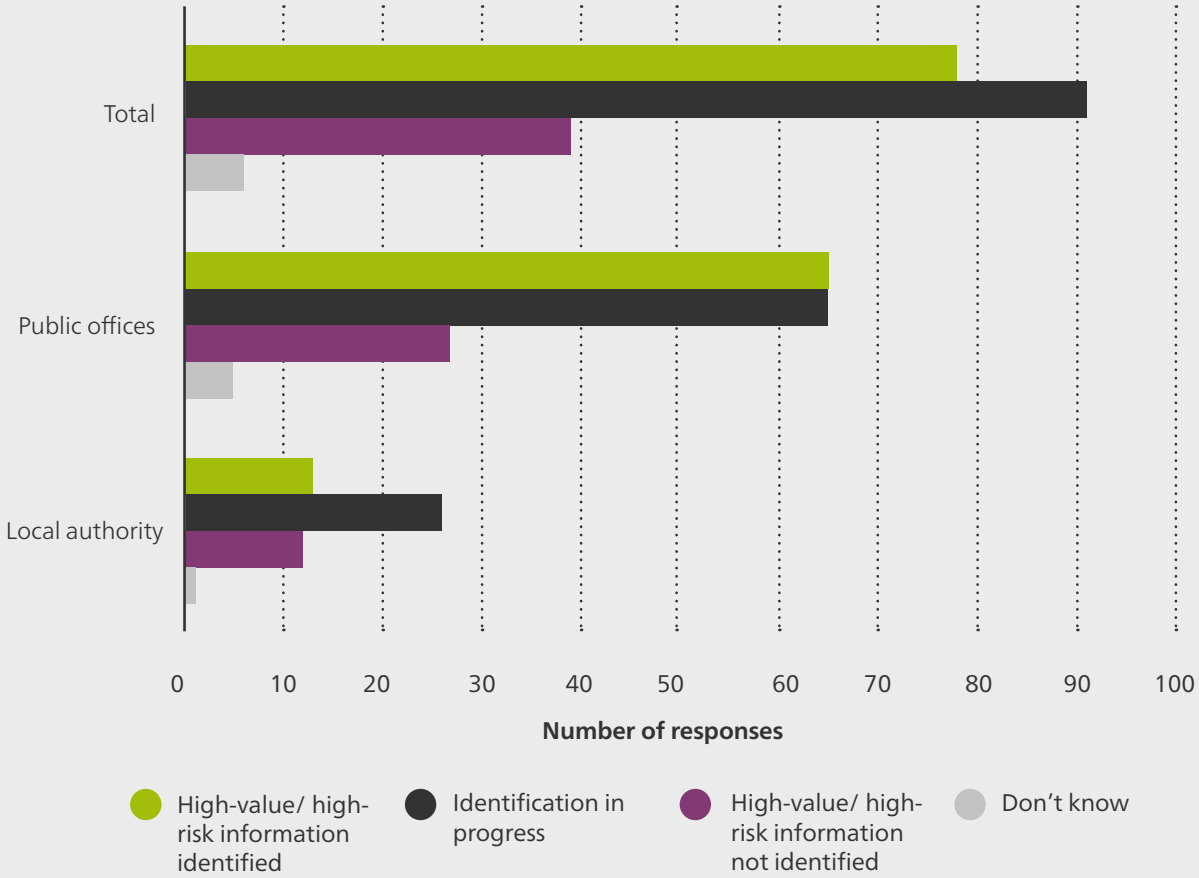
We asked survey participants:

- If the organisation has identified its most important high-value/high-risk information (Q.32).
- What actions the organisation has taken to actively manage that information in the last 12 months (Q.33).
- If the organisation has an information asset register (IAR) or similar tool, and if that tool is current and in use (Q.23 and Q.24).
- If organisations that do not have an IAR or similar tool are planning to develop one (Q.25).

Findings

36 percent of respondents have identified their high-value/high-risk information, while 43% said that work is 'in progress' (Figure 8). Public offices are more likely to have identified their high-value/high-risk information than local authorities, but we do not have a clear indication of why. The rates of identification are a worrying finding, given that this has been an explicit requirement since July 2016.

Figure 8: Identification of high-value/high-risk information compared to tier of government

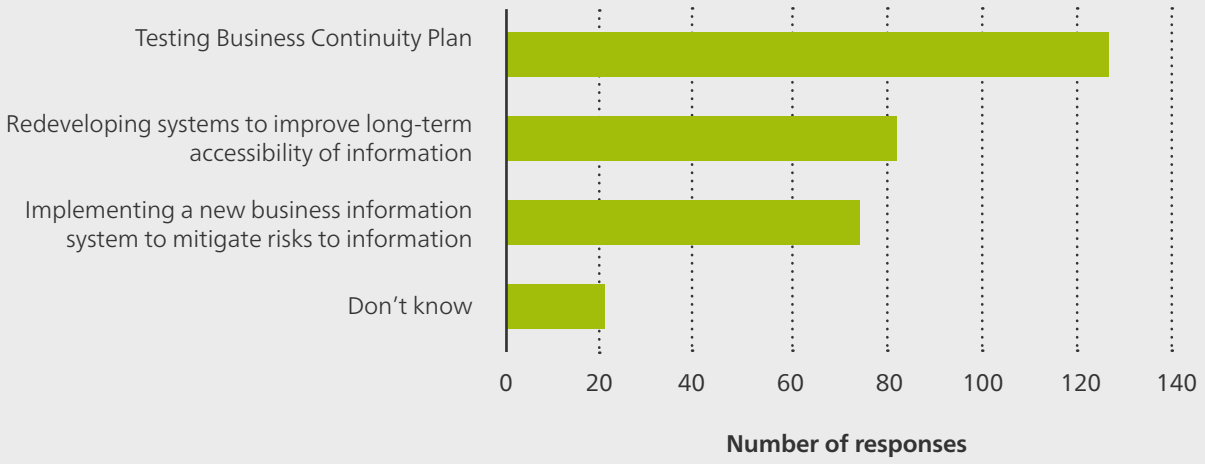


38 percent of respondents said that they do not have an IAR, while a combined 48% responded 'yes' or 'in development', and 14% responded 'work started but deferred'. This suggests that just under half of respondents are moving beyond the discovery stage and making sure that their high-value/high-risk information assets are documented. Of the 47 respondents that said they had an IAR or similar tool, 29 said that it was up-to-date and 34 said it was being used.

For managing high-value/high-risk information, we asked about a small set of common activities (Figure 9). Other activities mentioned in the comments, in addition to those listed in Figure 10, include:

- System and software upgrades or migrations.
- Disposal plans focused on high-value information.
- Employing IM staff.
- Implementing backup capability.
- Creating strategies.
- Reviewing processes.
- Developing information architecture and new search tools.
- Securing funding.

Figure 9: Actions to manage high-value/high-risk information



IM requirements built into new systems

Why it is important

Building IM requirements into a business system from the very beginning is a key enabler for proper management of the information created and stored in that system. This means that the system is optimised to support the creation and maintenance of complete, accurate and accessible information, as well as its eventual, authorised disposal.

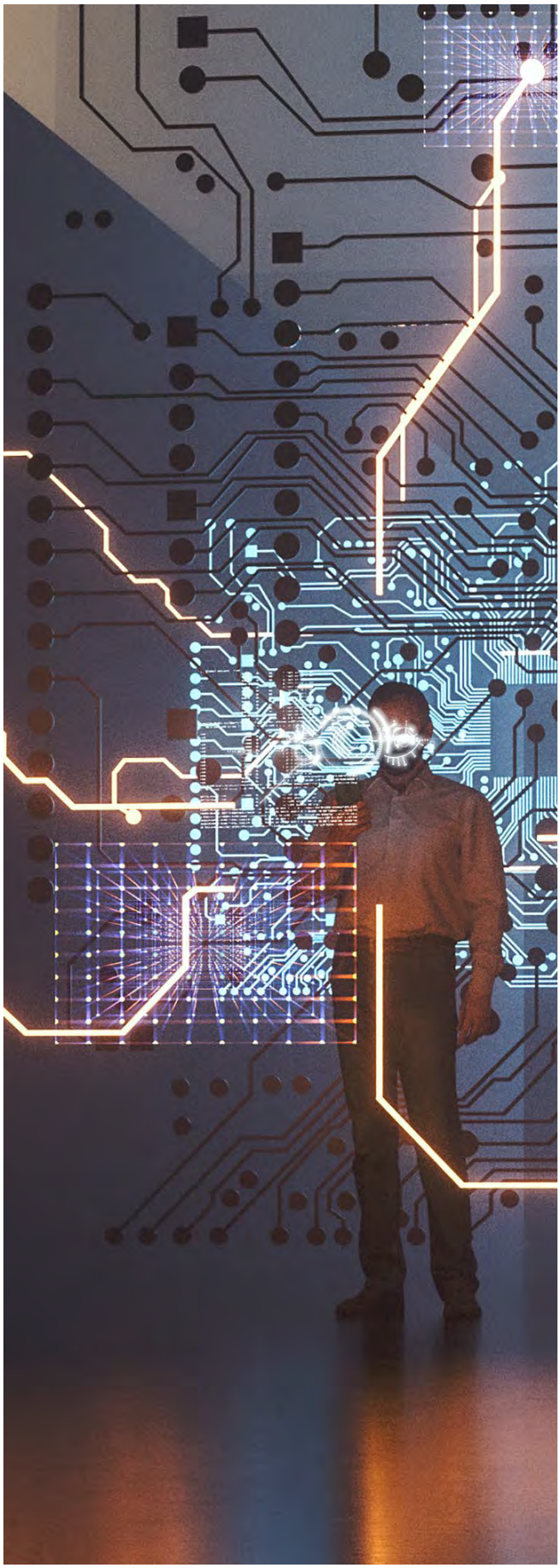
The integration of metadata into business systems is a specific IM requirement that we highlight in our survey questions. That is because metadata is so important for enabling IM specialists to do their jobs and people to find, trust and use information.

We recognise that it can be extremely challenging to retroactively add or plug-in IM requirements to existing systems, particularly when they have already been in operation for an extended period and are bespoke, no longer supported or at end of life. But for new systems we have much higher expectations. The requirement to build metadata into business systems has been mandatory since 2008, so systems implemented since then should be in this category.

What we asked

We asked survey participants:

- If the organisation has implemented any new business information systems in the last 12 months (Q.34).[4]
- If a process for managing information through its lifecycle has been built into those systems (Q.35).
- What challenges affect the organisation's ability to integrate IM requirements into new or upgraded systems (Q.36).
- If the organisation's currents systems meet our *minimum requirements for metadata* (Q.37).



4 A business information system is any system that creates and stores information.

Findings

68 percent of respondents have implemented a new business information system (or systems) in the last 12 months. Of those, half (50%) have built in a process for managing information through its lifecycle, while the other half either have not built in requirements or 'don't know' whether they have (Figure 10).

The most common challenges affecting respondents' ability to build in IM requirements are lack of awareness of the requirements amongst internal staff, the number of systems in use and lack of consultation with IM staff (Figure 11). Other challenges mentioned in the comments, in addition to those listed in Figure 11, include:

- The age of business systems.
- Lack of resourcing and capability.
- The rapidness of implementations.
- Procurement and ICT projects bypassing IM assurance or consulting too late.
- Competing business priorities.
- IM requirements being considered 'nice to have' or de-scoped.
- Archives does not provide relevant guidance.

71 percent of respondents said that 'some' of their business systems meet our minimum requirements for metadata. Far fewer said the all systems meet the requirements (16%), while a combined 13% responded 'no systems do' or 'don't know'.

Figure 10: IM requirements built into new business information systems

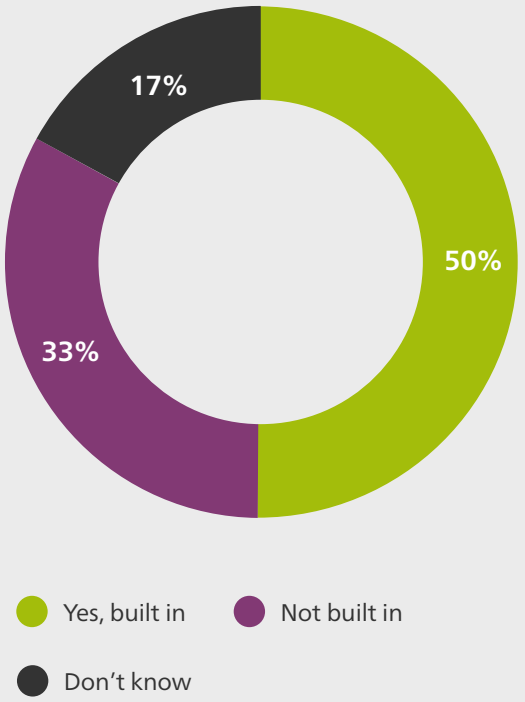
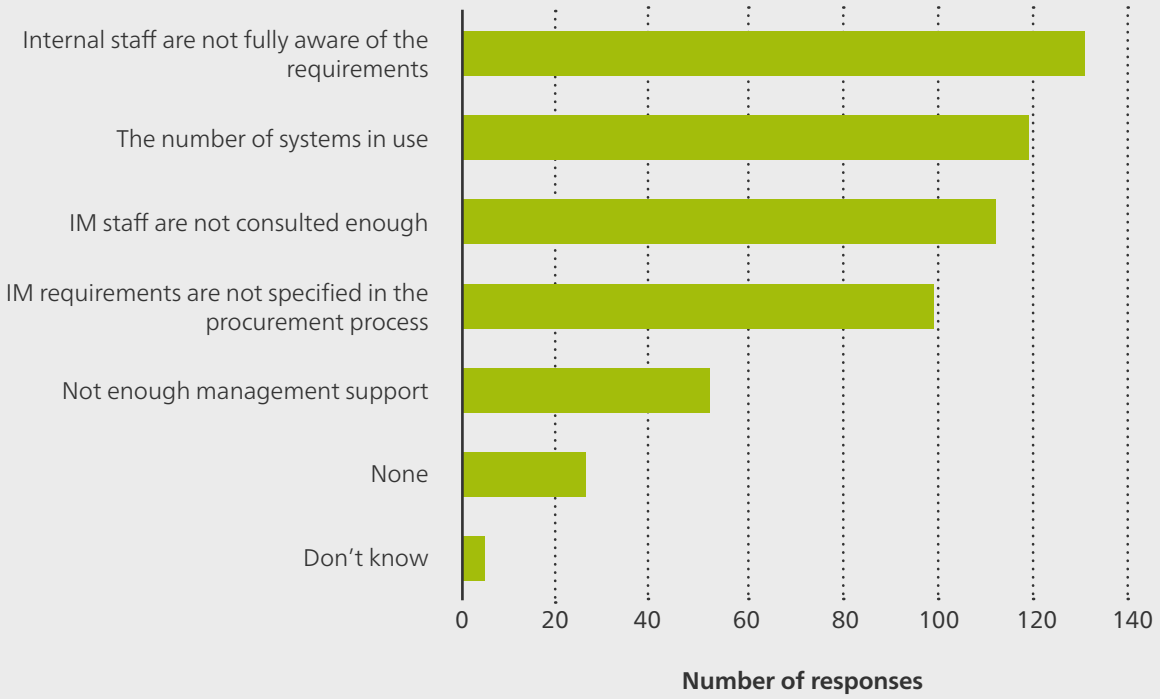


Figure 11: Challenges for building IM requirements into new business information systems



Managing information during change

Why it is important

Change events within an organisation can often put information at risk. Common types of change in the government sector include:

- Structural changes, such as functions moving between organisations, organisations being merged together, or organisations being disestablished.
- Changes to systems and storage environments, such as migrations or decommissioning.
- Implementation of new services.

During change events, information may be moved around within an organisation or between multiple organisations. When it is moved, whether physically or digitally, it can be exposed to risks such as alteration, corruption, unauthorised access, or even loss.

When a system or website is decommissioned, the information it holds may still need to be captured and preserved elsewhere to meet legal requirements. One way to minimise the quantity of information that needs to be relocated during migrations or decommissioning is to dispose of information that is no longer needed for current business, using an authorised disposal authority.

When a completely new business function or service is established organisations should identify what new information needs to be created and maintained to support that business and meet legal requirements. We expect organisations experiencing change to make a concerted effort to protect the integrity of information affected by that change.

What we asked

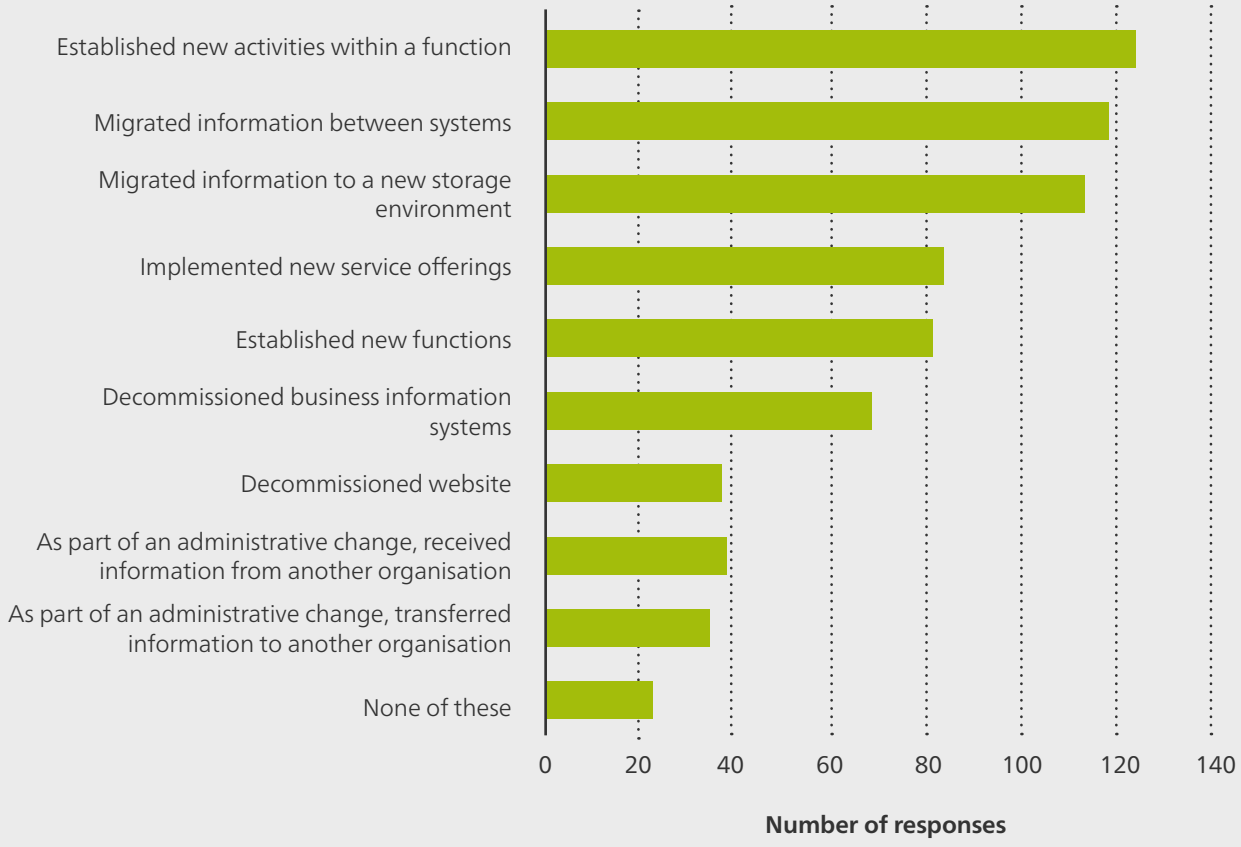
We asked survey participants:

- What business changes have occurred in the last 12 months that have implications for IM (Q.46).
- If the organisation took actions to guarantee the integrity of information during those changes (Q.47).

Findings

Figure 12 shows that the most common types of organisational change reported this year are: establishing a new business activity (58%) migrating information between systems (56%) and migrating information to a new storage environment (53%). In addition to business changes described in Figure 12, several respondents also commented on the impact of COVID-19 on ways of working and business functions. Of the 191 respondents that reported organisational changes listed in Figure 12, over half (58%) said that the integrity of information had been guaranteed in all instances of organisational change, while 34% said that this had been done 'in some cases'.

Figure 12: Organisational changes in the last 12 months



Managing digital information over time

Why it is important

Many organisations have to maintain at least some of their information over extended periods of time before they can destroy it or transfer it. Those maintenance periods can range anywhere from ten years to as long as 100 years. During that time the information has to remain accessible and usable, without loss of integrity. This presents a particular challenge for digital information when we consider:

- The retention period often exceeds the lifespan of the system where the information was originally created and stored.
- As digital information ages, there is a risk that the software or hardware required to open, read and use it will become obsolete.
- Digital information does degrade over time (sometimes referred to as bit rot).

System or file format migrations are a few ways to mitigate these risks, but they also come with their own risks (see Managing information during change). Without basic digital preservation capability in place, it is difficult for organisations to know whether their digital information remains stable and viable over time and put safeguards in place. We expect organisations to:

- Know what digital information they hold that requires long-term retention (i.e. 10 years or more).
- Build collaborative relationships between IM and ICT to support digital continuity.
- Monitor and protect digital information over time.

What we asked

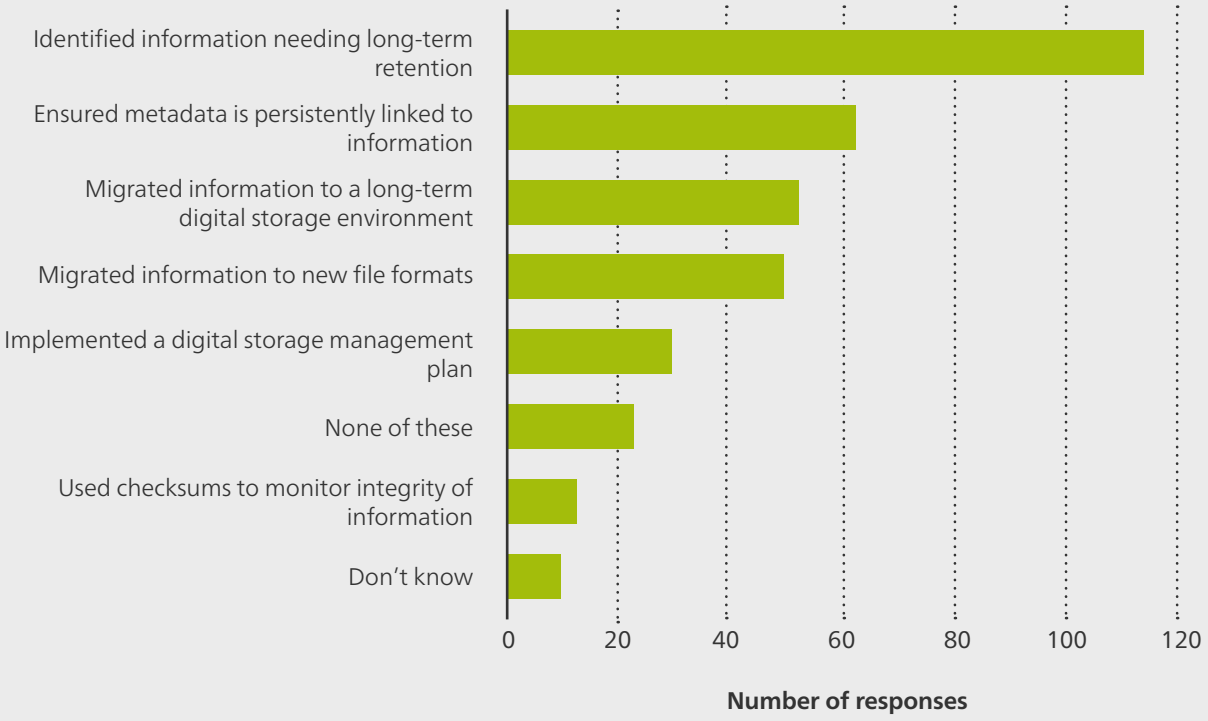
We asked survey participants:

- If they have digital information with long-term value (Q.38).
- What actions the organisation has taken in the last 12 months to make sure that information remains usable (Q.39).
- If the organisation has any digital information that is inaccessible (Q.40).
- Why that information is inaccessible (Q.41).

Findings

83 percent of respondents (178 organisations) told us that they have digital information with long-term value. Of those, the majority (64%) have identified the information that needs to be retained long-term. However, Figure 13 shows that the proportion of respondents taking actions to actively maintain usability, such as migrating file formats, is low.

Figure 13: Actions to maintain usability in the last 12 months



A combined 53% of respondents 'definitely have' or 'possibly have' digital information that is inaccessible (Figure 14). The most common reasons for inaccessibility are information being stored in personal systems, inadequate metadata and obsolete file formats (Figure 15). Other reasons mentioned in the comments, in addition to those listed in Figure 15, include:

- Password protected documents or issues with permissions.
- Expiry of software licences or limited number of licences.
- IM staff unable to access business systems.
- Use of shadow IT.
- Hardware obsolescence.
- Information not being returned by contractors.

Figure 14: Do organisations hold any digital information that is inaccessible?

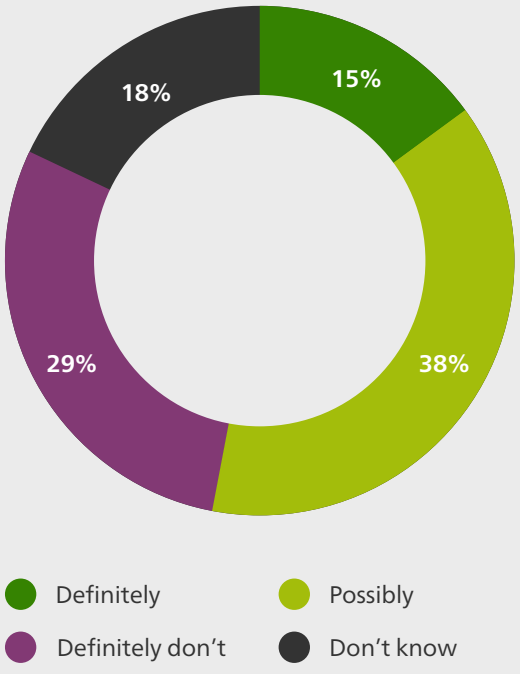
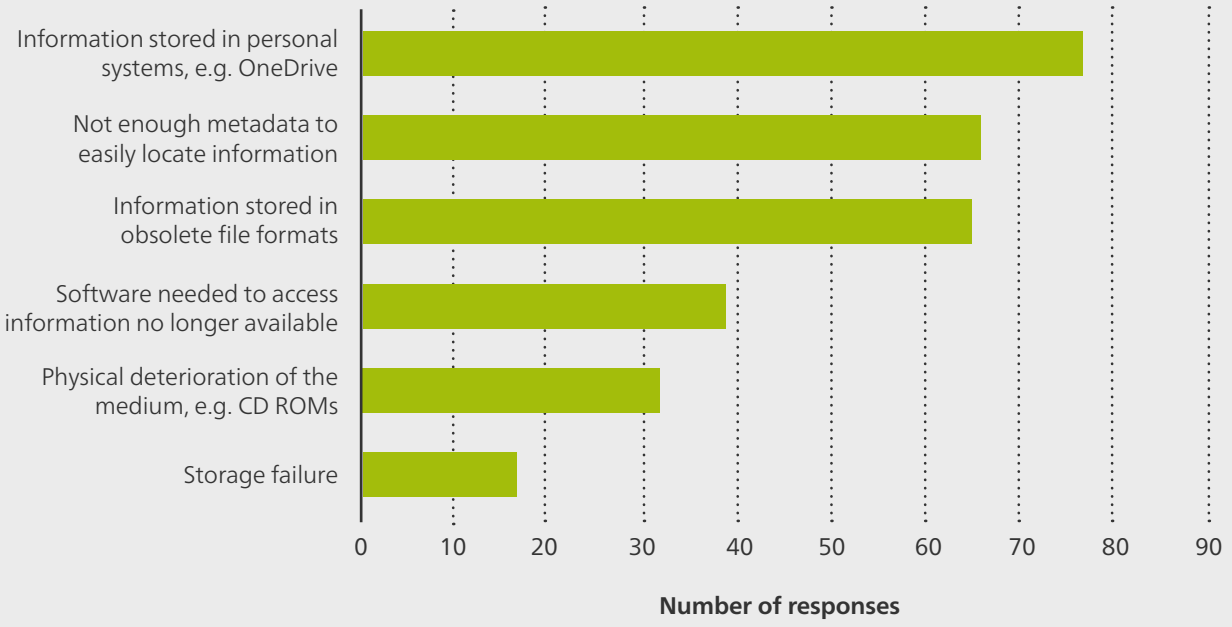


Figure 15: Reasons why digital information is inaccessible



Protecting information against security risks

Why it is important

Yet another risk to the integrity of information is breaches of security that result in unauthorised access, alteration, destruction or loss. This risk applies to both physical and digital information and can occur for any number of reasons, including issues with:

- Access protocols and audit trails.
- Patch and vulnerability management.
- Encryption.
- Secure destruction or permanent deletion.
- Staff using uncertified software/services or shadow IT that has known security risks.

For digital information there is also the ongoing threat of malicious cyber activity to contend with. No public sector organisation wants to end up in the media because of security breaches. This undermines public trust and, in some cases, Ministerial confidence.
We expect organisations to stay on top of security risks and protect information in all formats, wherever it is located.

What we asked

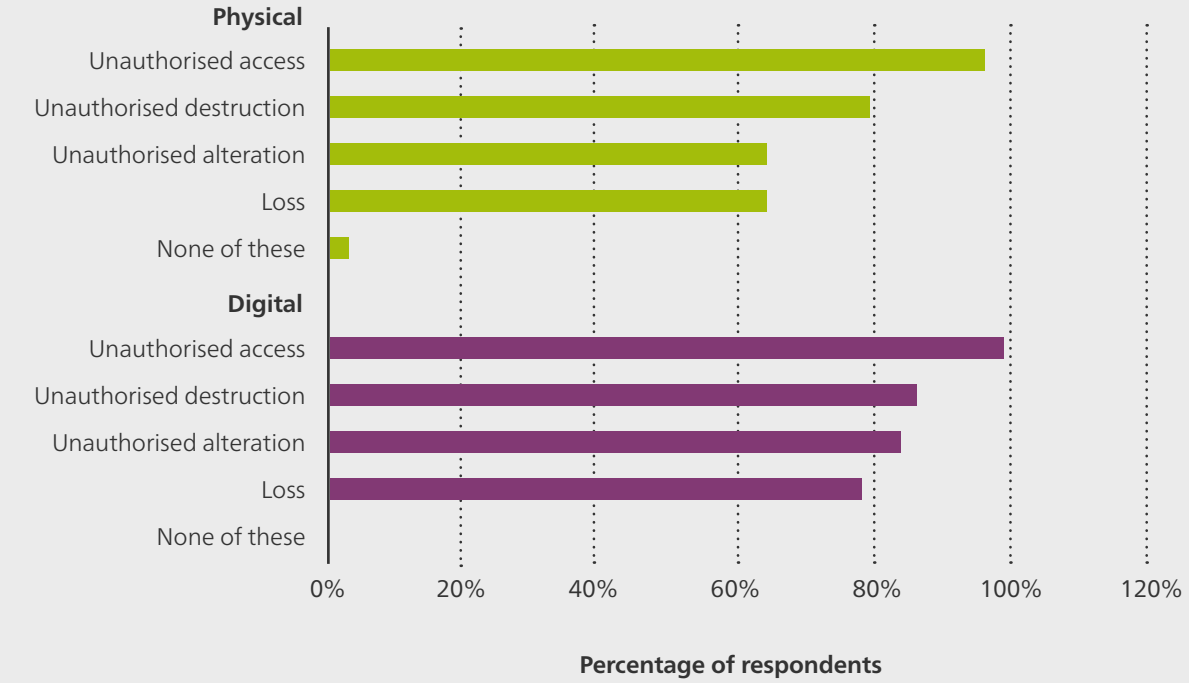
We asked survey participants what security risks they protect their physical and digital information against (Q.48 and Q.49).

These questions are different from the questions we asked in last year's survey. Last year we asked about the extent to which storage environments used by organisations have measures in place to protect information.

Findings

A high proportion of respondents said that they protected both physical and digital information against loss and unauthorised alteration, destruction and access (Figure 16). A small number of respondents said that their physical information was not protected against any of these security risks.

Figure 16: Protection of physical and digital information against specified security risks



Access restrictions for information over 25 years old

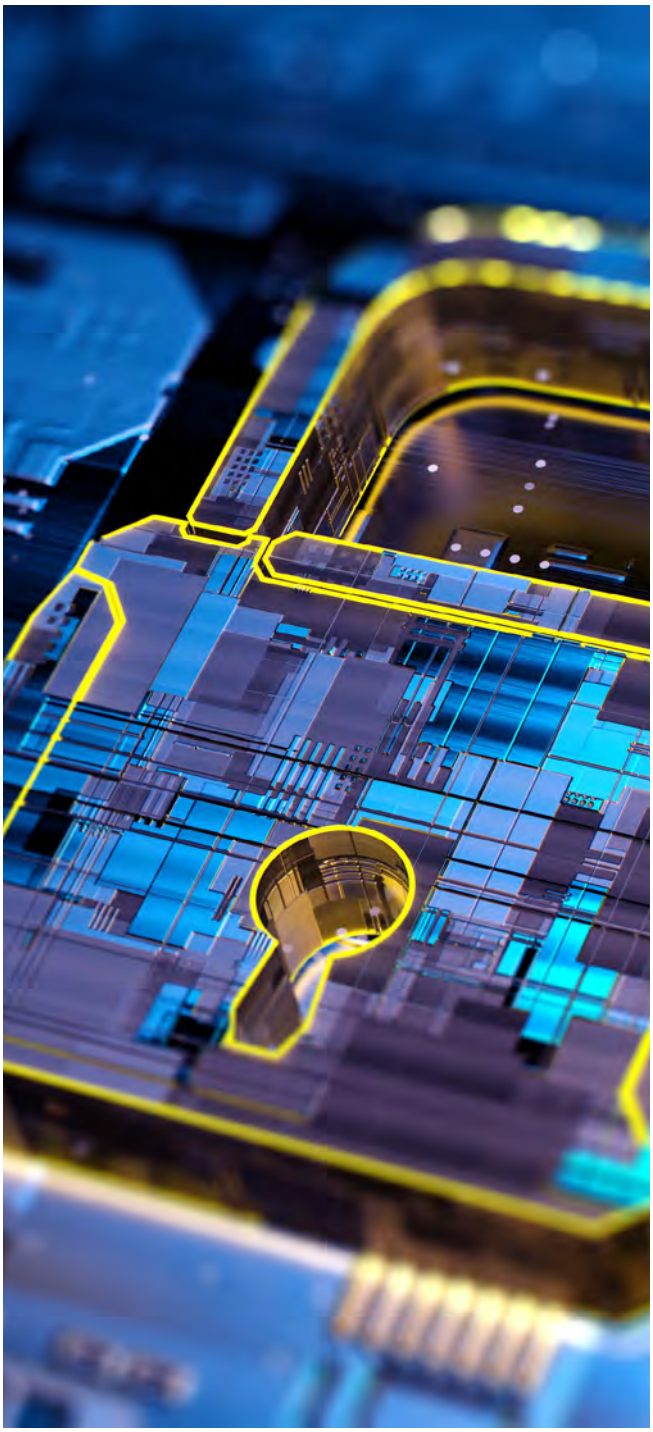
Why it is important

In the words of the Chief Ombudsman and their Australian counterparts: "Public access to information encourages scrutiny and participation in democratic processes, supports better decision-making and strengthens citizen engagement with the public sector."[5] Although public access to central and local government information is largely guided by official and personal information laws, the Public Records Act 2005 also plays a supporting role, by requiring public sector organisations to:

- Create information about their business activities in the first place (also known as 'duty to document').
- Manage that information well, so that it is available in an accessible form.
- Classify the access status of information, which is the focus of the survey questions in this section.

For central government, once information has been in existence for 25 years or is about to be transferred into the control of the Chief Archivist, it must be classified as either open or restricted access (s43, PRA). For local government, the same action must occur when a local authority records becomes a local authority archive (s45, PRA).[6]

Generally, access should be open unless there is a good reason to restrict it or another enactment requires it to be restricted (s44 and s46, PRA). Information that is open access must be made available free of charge and as soon as reasonably practicable (s47, PRA). Restrictions are for a specified time period, so organisations need to periodically review them to check that they are still valid.



5 (2019). Office of the Ombudsman. *Right to know essential to democracy in a digital world*.

6 A local authority archive is a local authority record that is no longer in current use by the controlling local authority, or has been in existence for 25 years or more (whether or not in current use)

What we asked

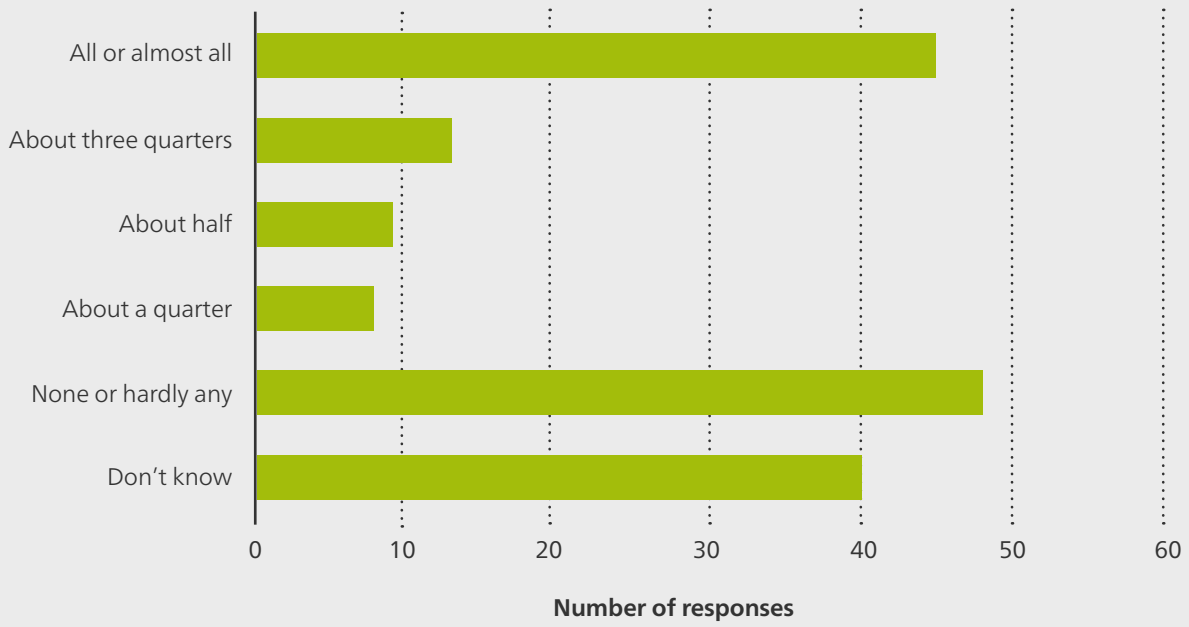
We asked survey participants:

- If they hold information that is more that 25 years old (Q.50).
- How much of that information has been classified as either open or restricted (Q.51).

Findings

76 percent of respondents said that they hold information that is more than 25 years old. Of those, only 28% have classified all or most of that information as open or restricted (Figure 17). Around a quarter of respondents have classified hardly any information (29%) and another quarter (25%) replied 'don't know'.

Figure 17: Proportion of information over 25 years old classified as open or restricted



Key findings

The proportion of organisations building IM requirements into new business systems is too low. It has been mandatory for over a decade and the results raise questions about the compliance of any business systems implemented in this period.

Although many organisations are consistently protecting the integrity of their information during changes events, we want to see a higher proportion doing so. Similarly, we would like to see more organisations reporting active maintenance of digital information with long-term value. Managing risks to digital information through change and over time is critical for meeting the PRA requirement to maintain information.

It is pleasing to see a high proportion of organisations reporting that they protect their information against security risks. This suggests that information security requirements are taken seriously within ICT departments, reflecting the impact of the Protective Security Requirements.

Reported rates for access classification of information over 25 years old should be higher. We made a similar finding concerning access classification in *last year's survey findings report*, so it stands out as an area of IM practice that may need further encouragement on our part. While we recognise that this activity is unlikely to be a business priority for organisations, it is requirement that must be met to support open government and Public Inquiries established under the Inquiries Act 2013.

For recommendations concerning high-value/high-risk information and building IM requirements into new business systems, see the *Chief Archivist's Annual Report on the State of Government Recordkeeping 2019/20*.

4.0 Disposal

This section covers the IM activities that enable the disposal of public sector information when it is no longer required by an organisation. Disposal usually involves one of two actions: secure destruction or transfer to a permanent repository for long-term preservation and access.

Preparing for disposal

Why it is important

There are a range of tools, conditions and actions that need to be in place before disposal can occur. Regular, efficient disposal is dependent on good preparation as well as some of the people components and other IM activities that have already been discussed in this report, such as:

- A governance group that resources and prioritises disposal, and advocates for business systems design that facilitates disposal.
- IM staff with the appropriate knowledge and skills to plan, enable and perform disposal and apply new technologies to resolve disposal challenges.
- Knowing what information the organisation creates and what value it has.
- Having business systems that are set-up to facilitate disposal of the information they store and/or technologies that simplify disposal.

Assuming all these factors are in place, the path towards doing disposal involves:

- Acquiring authorisation from the Chief Archivist in the form of an organisation-specific disposal authority.
- Applying the rules from the disposal authority to the organisation's information.
- Identifying the information that is ready for disposal.
- Getting approval from business owners to proceed with disposal.
- Classifying access status, for information being transferred.

There is always disposal work that organisations can be getting on with. Our general disposal authorities (GDAs) have been developed for the public sector to enable the lawful destruction of common corporate records without requiring organisation-specific authorisation from the Chief Archivist.

What we asked

We asked survey participants:

- How much of their information was covered by authorised disposal authorities (Q.52).
- How soon the organisation planned to improve disposal authority coverage (Q.53).
- What actions the organisations has taken in the last 12 months to prepare for doing disposal (Q.54).

Findings

More than half of respondents (57%) said that all or most of their information was covered by authorised disposal authorities (Figure 18). The majority (65%) did not provide a timeframe for improving coverage for information not covered by a disposal authority, while 21% did provide a timeframe and 14% said that they appraisal to improve coverage was underway.

In terms of actions to prepare for doing disposal, the most common actions were obtaining approval to dispose from business owners and sentencing information in offsite storage, i.e. physical information (Figure 19). The second of these suggests a focus on preparing physical information for disposal. There is far less activity around preparing digital information.

Figure 18: Proportion of information covered by disposal authorities

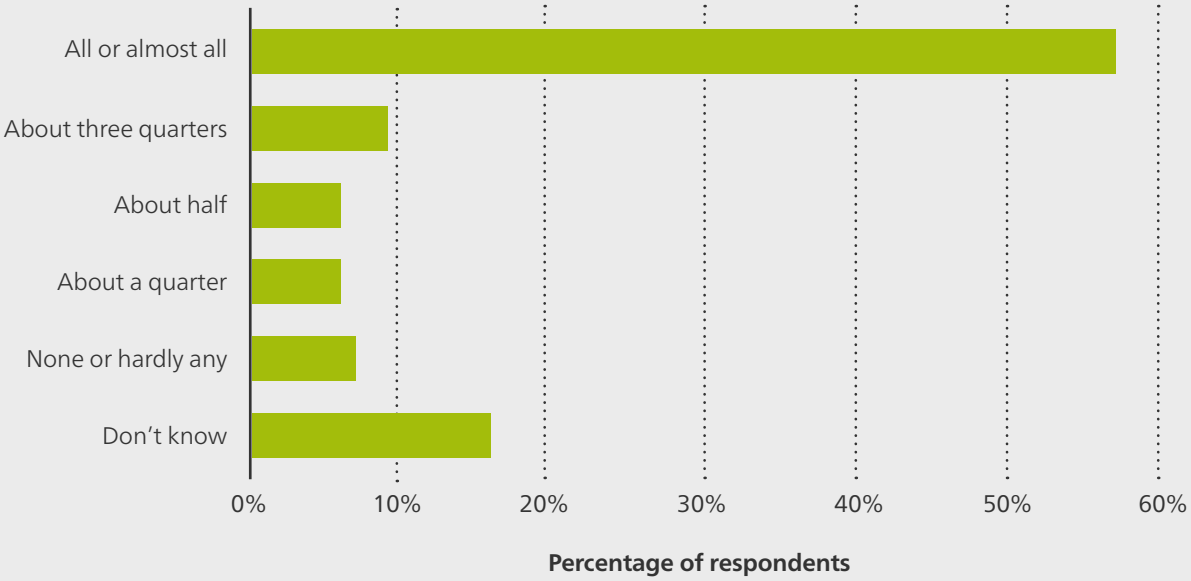
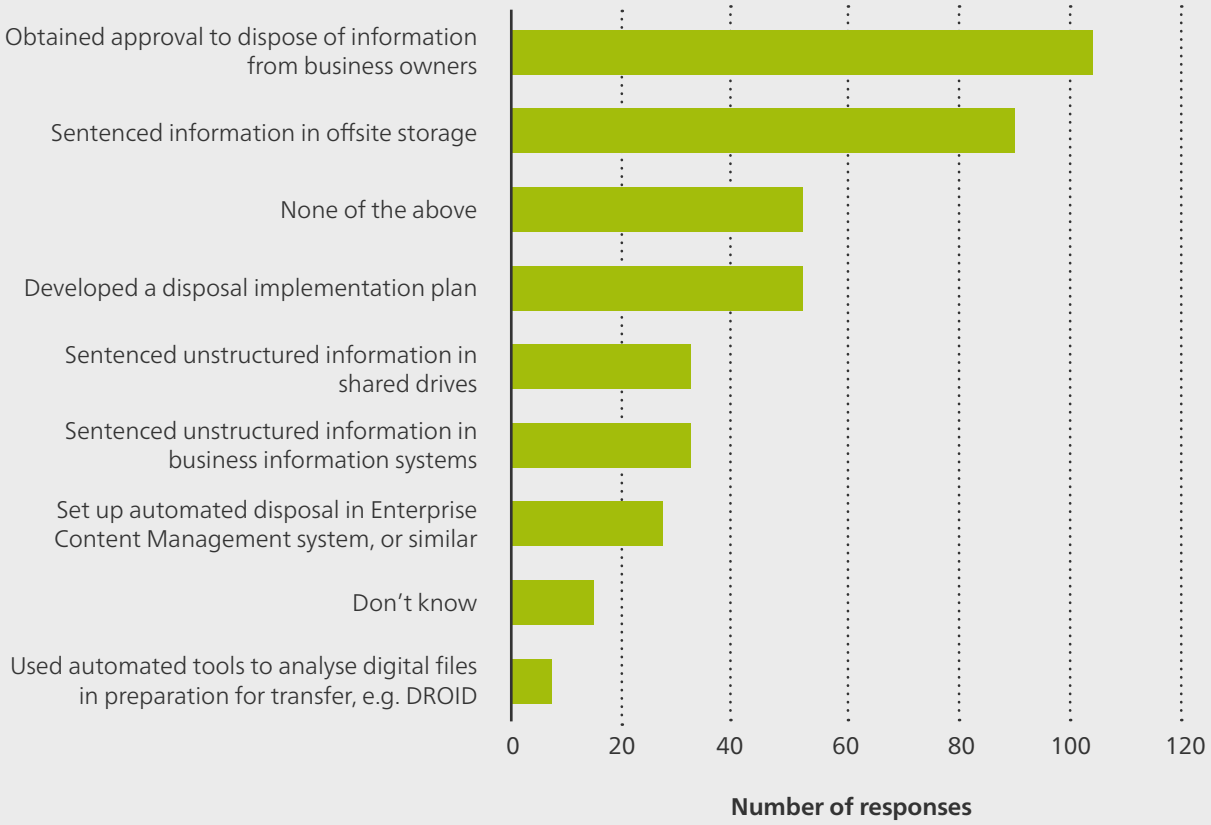


Figure 19: Actions to prepare for disposal in the last 12 months



Doing disposal

Why it is important

Transferring information that has long-term value for New Zealanders to our repositories supports ongoing management, preservation and public access. For information that does not have to be transferred, destruction is an important component of effective IM. The benefits of active, authorised destruction include:

- Mitigating the risks associated with retaining information for longer than required, such as privacy or security breaches and unauthorised access.
- Minimising the quantity of digital information an organisation has to manage, thereby increasing the efficiency of business systems (e.g. fewer irrelevant search results to wade through) and making the organisation's high value information easier to discover and manage.
- Decreased storage costs, for both physical and digital information. The cost of storing digital information over the long-term should not be underestimated. The price per gigabyte combined with the cost of storing back-ups, versioning and vendor costs, such as retrieval charges, may be high.

Organisations in central government are required to transfer information with long-term value into the control of the Chief Archivist after 25 years, unless it has been agreed otherwise (s21, PRA). Organisations in local government do not transfer to Archives, but the status of their information changes to that of 'local authority archive' after 25 years. Archives' Wellington repository is currently closed for physical transfers, but our other repositories are open, as is the Government Digital Archive.

We expect organisations to work towards the goal of regular, routine disposal, rather than tackling it as an ad-hoc activity or project that requires special resourcing.

What we asked

We asked survey participants:

- If they have carried out authorised destruction of physical or digital information in the last 12 months (Q.55 and Q.56).
- What challenges affect their ability to undertake regular, authorised destruction (Q.57).
- If they have plans to transfer physical or digital information in the next 12 months, and if not why not (Q.58, Q.60, Q.61).
- What challenges affect their ability to undertake regular transfer (Q.62).

Findings

58 percent of respondents have done some form of destruction (i.e. either physical or digital). Figure 20 shows that the proportion of respondents that have destroyed physical information is much higher than digital information: 52% have destroyed physical, while only 26% have destroyed digital. The results for digital destruction suggest that some respondents did not include routine, authorised deletion within their business systems into their response.

The most common challenges for doing regular, authorised destruction are system set-up, lack of resources and lack of prioritisation by staff responsible for electronic deletion (Figure 21). Other challenges mentioned in the comments, in addition to those listed in Figure 22, include:

- Delays with approval of disposal authorities.
- Disposal authorities not supporting automated disposal.
- Complexity of setting up automated disposal.
- IM staff unable to access business systems to implement disposal.
- Difficulty of sentencing unstructured information repositories.

Figure 20: Authorised destruction in the last 12 months

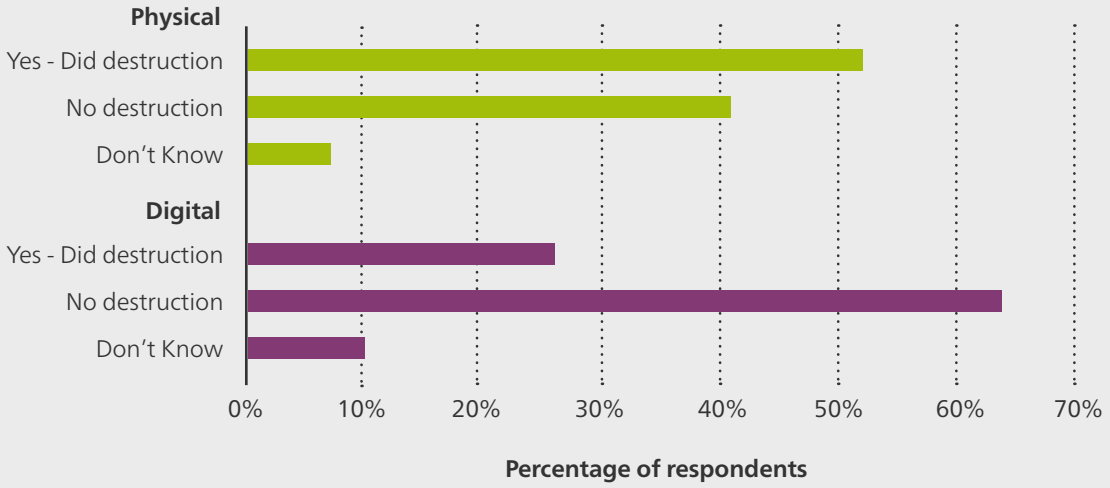
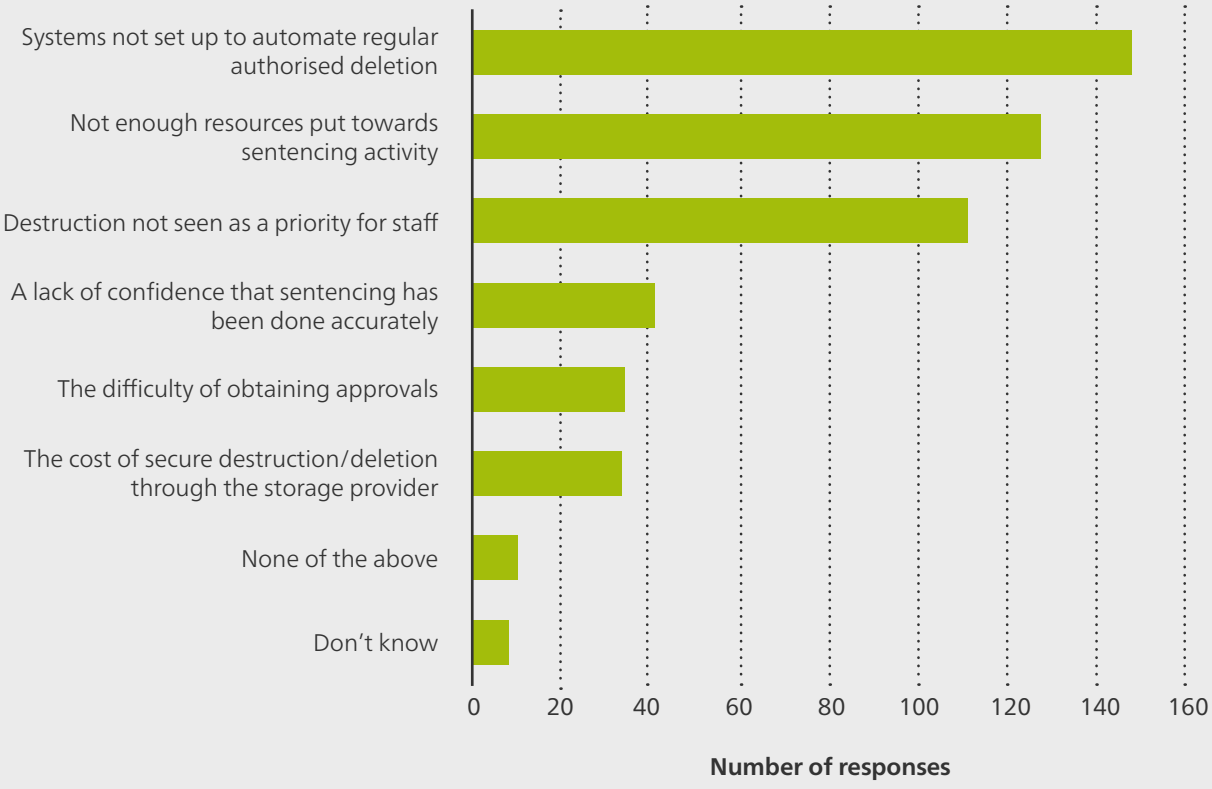


Figure 21: Challenges for doing authorised destruction of information

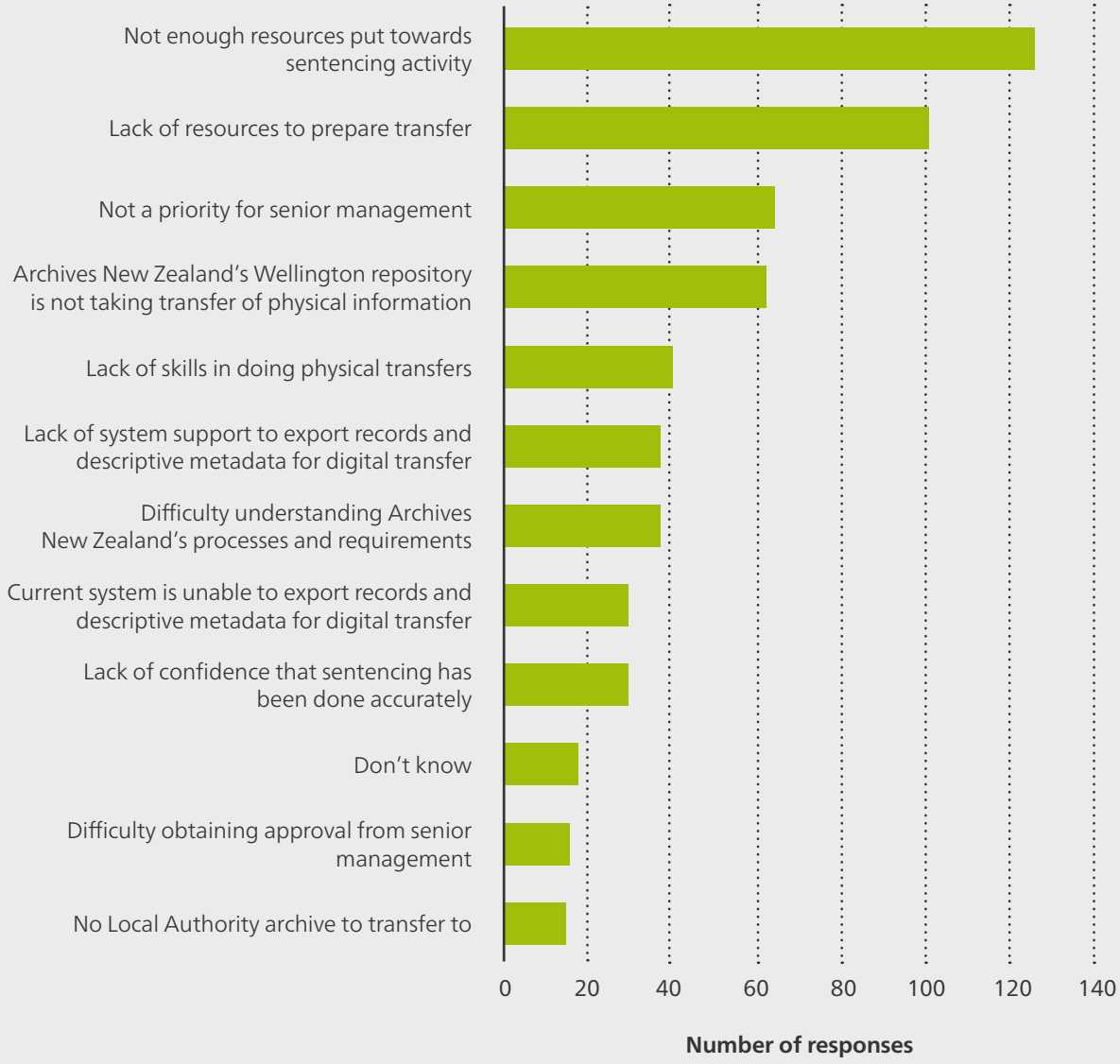


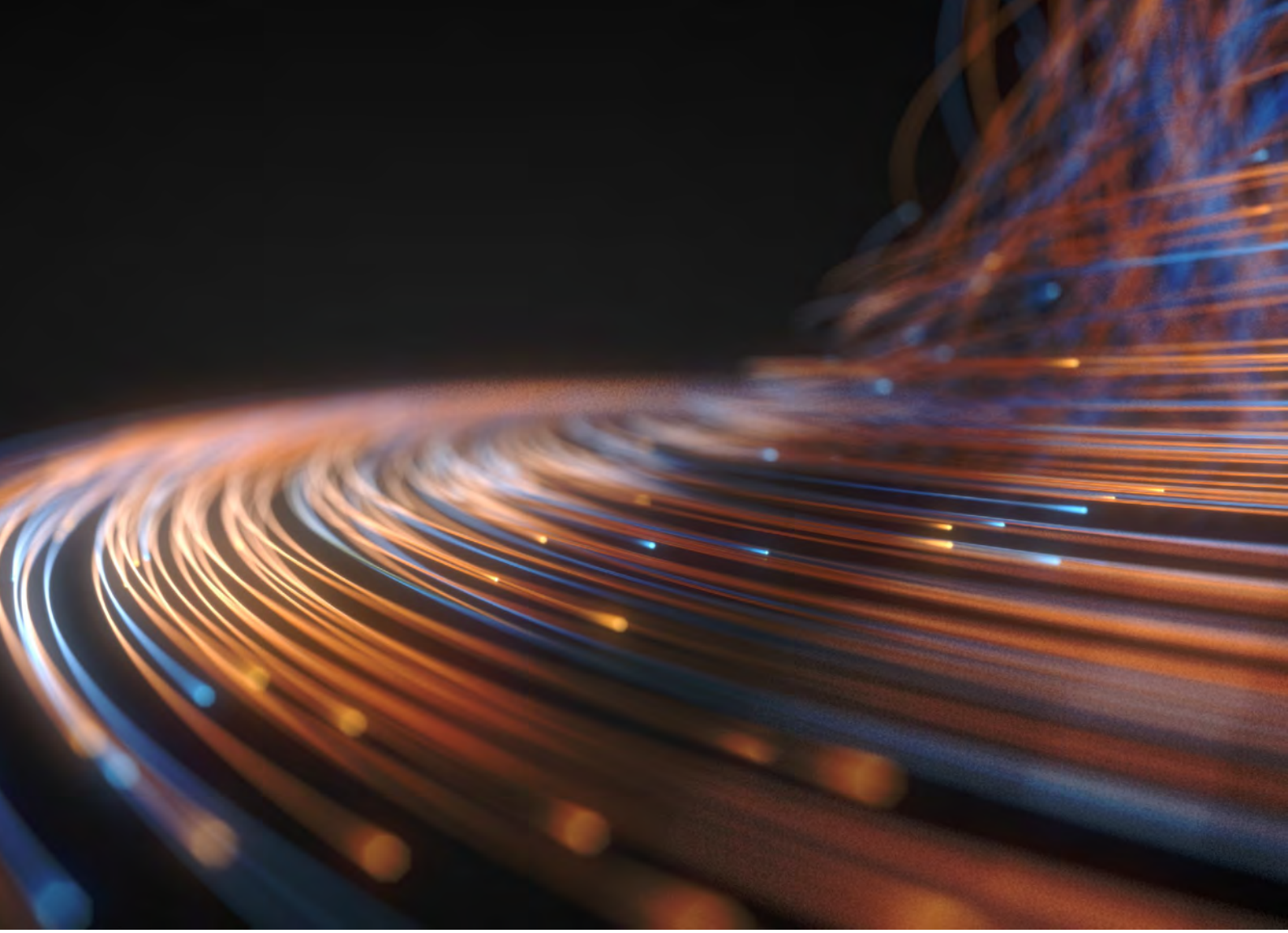
Only a minority of respondents have plans to transfer physical (26%) or digital (8%) information in the next 12 months. The most common challenges for doing regular transfer are: lack of resources for sentencing, lack of resources to prepare transfer and prioritisation by senior management (Figure 22).

Other challenges mentioned in the comments, in addition to those listed in Figure 22, include:

- Complexities of classified information.
- Dealing with hybrid information (i.e. both physical and digital formats).
- Lack of experience, training and skills in preparing digital transfers.
- Local government repositories at capacity.
- The cost of preparing transfers.

Figure 22: Challenges for transferring information





Key findings

The findings suggest that organisations are getting stuck at the preparation stages and have difficulty progressing to doing disposal on a regular, routine basis. Some of the roadblocks originate with us, some are present within organisations, while others concern overcoming common technological or capability challenges.

We acknowledge that there is plenty of work required to improve our instruments, tools, processes and guidance so that they better support disposal. We are initiating a project to address this and some of the common disposal challenges experienced across the public sector.

Disposal authority coverage is far from our *Archives 2057* goal of 100 percent coverage for the core public sector by 2025. Full disposal authority coverage has value beyond enabling regular, routine disposal. It can also provide a public view of the information held across government. This potential will be explored in the project mentioned above.

For recommendations concerning regular, authorised destruction of information, see the *Chief Archivist's Annual Report on the State of Government Recordkeeping 2019/20*.

5.0 IM environment

One of the objectives of our *Monitoring Framework* is to identify and respond to risks, challenges, opportunities and emerging trends that are affecting IM in organisations. The questions in this section are designed to help us be a more responsive regulator and can change from survey-to-survey.

Drivers, challenges and risks

What we asked and why

We asked survey participants what:

- Drivers are important for IM in their organisation (Q.7).
- Challenges affect good IM in their organisation (Q.8).
- Key risks to their organisation's information have been identified (Q.27).

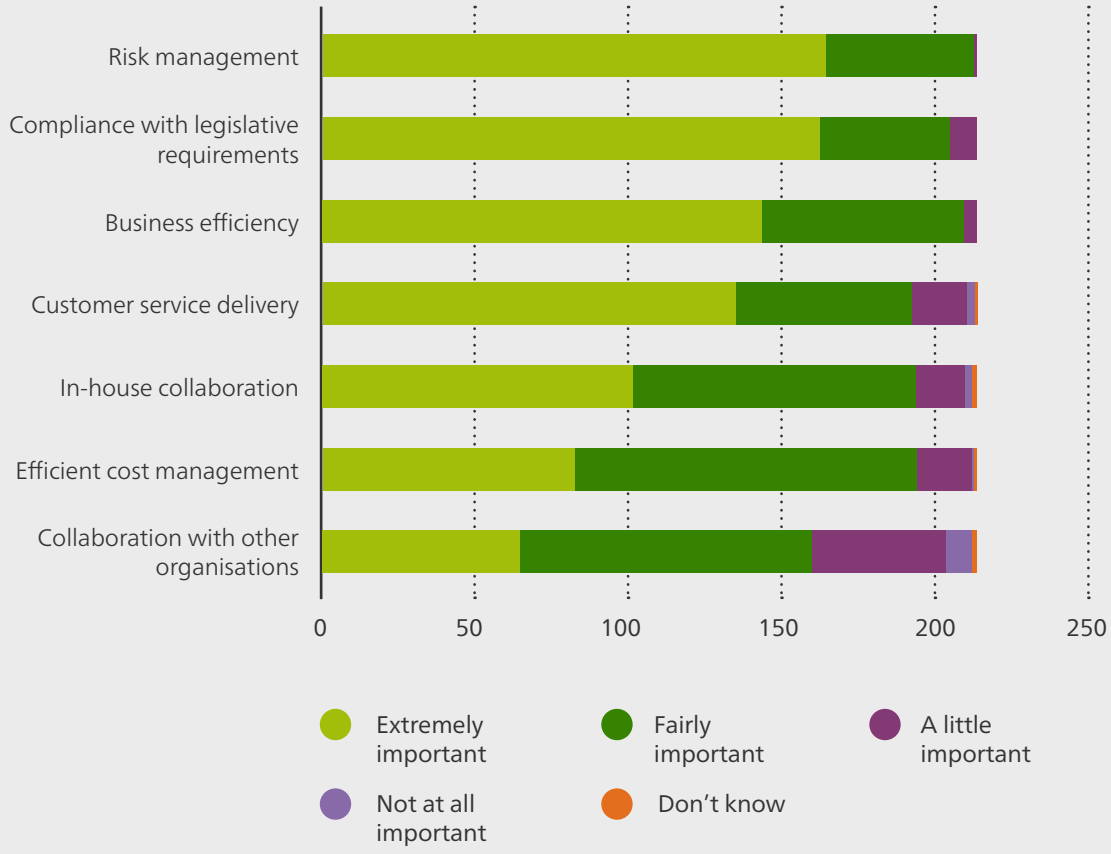
As a regulator, it is helpful for us to maintain an understanding of attitudes towards IM, what motivates public sector organisations to support or avoid IM, and what value organisations see in IM for their business. This informs us about how to better communicate with the organisations we regulate and promote IM in ways that connect our requirements with business goals and priorities. Our experience suggests that it is more effective to encourage good IM based on benefits for the business, rather than compliance for compliance sake.

IM and the related business activities that support or interact with it, such as ICT and security, are a constantly changing landscape. New challenges and risks emerge all the time, while some are constant. Our regulation needs to be responsive and adaptive to change, but we need an evidence-base to guide how we respond and what we respond to.

Findings

Figure 23 shows that the strongest drivers for IM are risk management and compliance with legislative requirements. 77 percent of respondents said that risk management was an 'extremely important' driver, while 76% said that compliance was an 'extremely important' driver. The majority of respondents also rated business efficiency and customer service delivery as 'extremely important'. Other drivers mentioned in the comments, in addition to those listed in Figure 23, included the value of information for supporting strategic goals. This driver was typically mentioned by organisations with a strong research, innovation or data focus.

Figure 23: Drivers for good IM



The majority of respondents rated all but two of the challenges we asked about as either 'reasonably big' or 'huge' (Figure 24). The biggest challenges are lack of understanding of the importance of IM, lack of communication across business groups, and adequately addressing IM during project planning. Other challenges mentioned in the comments, in addition to those listed in Figure 24, include:

- Scale and pace of technological change.
- Number of digital storage environments.
- Upskilling to manage digital information.
- Governance of cloud-based repositories and tools.
- Users' information literacy.
- Resistance to IM being involved with data management.

Figure 25 shows that the most common risks to information are lack of contextual information, unsupported business systems, and inadequate access and use controls. Other risks mentioned in the comments, in addition to those listed in Figure 25, include:

- Recycling user logins.
- Cybersecurity.
- Shadow IT, personal repositories and collaboration tools.
- Proprietary file formats.

Figure 24: Challenges for good IM

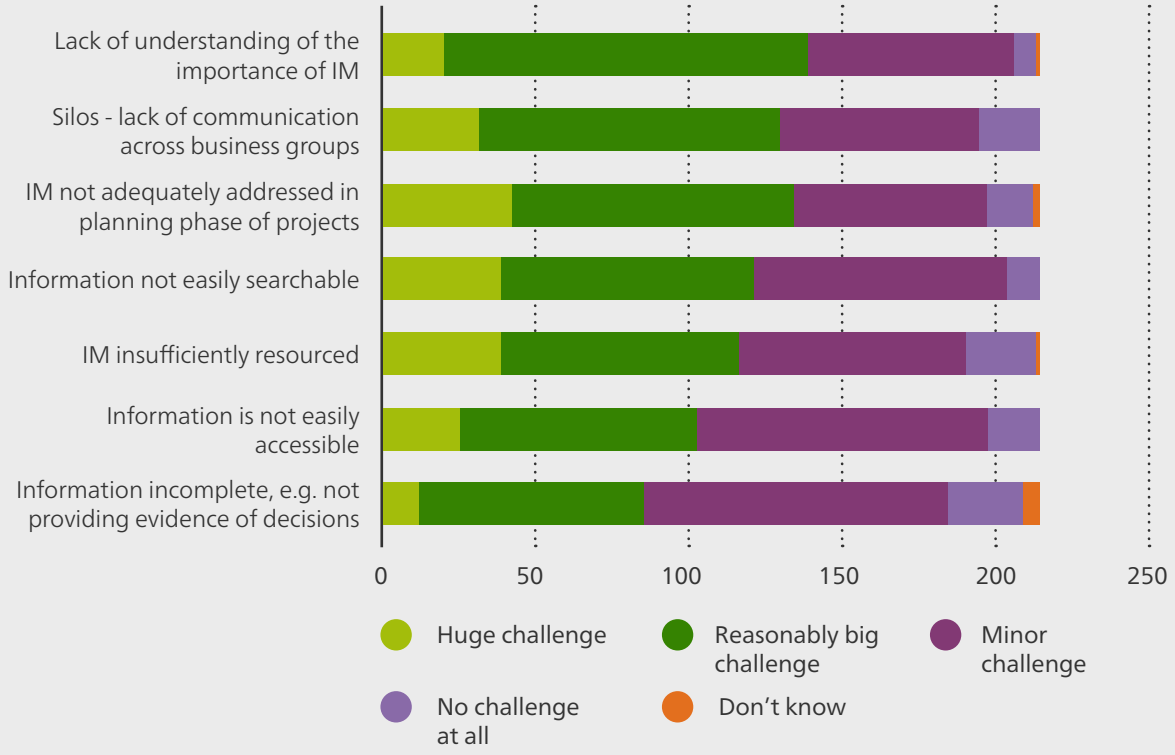
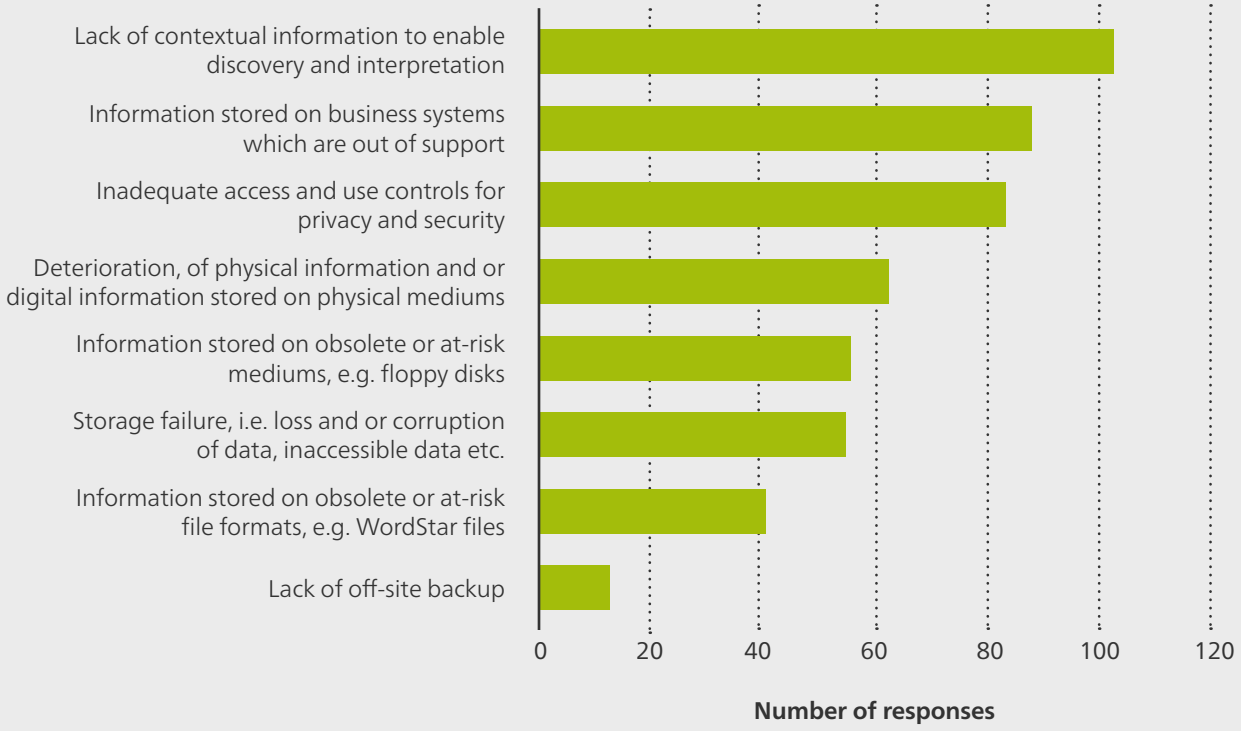


Figure 25: Risks to information



Transition from paper to digital

What we asked and why

We asked survey participants:

- If the organisation's business processes are fully digital (Q.20).
- If the organisation is transitioning from paper-based to digital business processes and what actions it is taking to do so (Q.21 and Q.22).

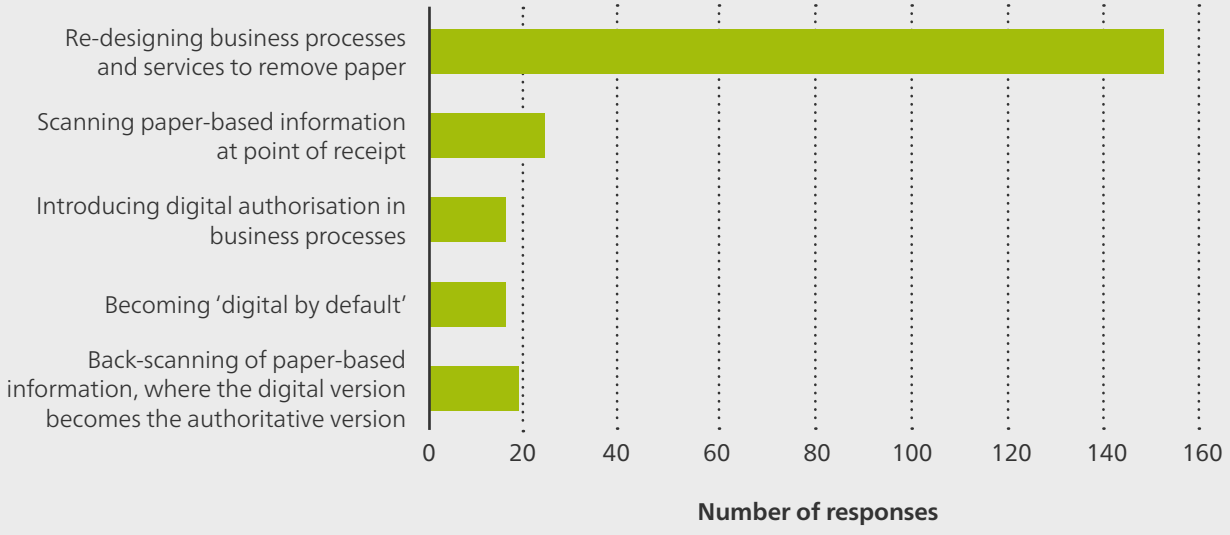
Fully digital public sector information is critical for enabling digital government. Most public sector organisations are already well on the journey to entirely digital work processes. There are two main ways in which digital transition occurs: by redesigning business processes so that there is no paper-based component, or by digitising any paper-based information so that the organisation can manage all transactions digitally.

We are interested in how organisations are doing digital transition because there are often IM challenges associated with this activity. With the right tools and functionality in place it can be much easier to manage digital information, but there is no evidence that digital information is better managed just because it is digital. For example, organisations can put a lot of time and resource into digitising paper-based information, only to find that it has not been done in a way that streamlines business or supports IM requirements.

Findings

12 percent of respondents said that their organisation's business processes are fully digital. Of the respondents that are not yet fully digital, the majority (92%) said that their organisation was transitioning from paper-based to digital business processes. Figure 26 shows the types of actions they are undertaking to transition. The most common action is re-designing business processes and services to remove paper.

Figure 26: Actions to transition from paper-based to digital business processes



Requests for official information

What we asked and why

We asked survey participants:

- About instances in the last 12 months when they have been unable to provide information requested under an official information request (Q.42 and Q.43).
- How often the reason for not being able to provide information is that it does not exist or cannot be found (Q.44 and Q.45).

We are interested in these two reasons for refusing official information requests because they can indicate underlying issues with IM. The Public Records Act 2005 requires organisations to create information about their business activities (also known as 'duty to document'). When the information requested does not exist, this may be a sign that an organisation is deliberately or unintentionally failing to document certain business activities. If information is known to exist but cannot be found, this may signal issues with IM, such as poor metadata.

Findings

Of the 196 respondents that received requests for official information in the last 12 months, 34% (67 organisations) said that there were occasions when they were unable to provide the information requested. Of those, a combined 58% said that the reason for this was 'rarely' or 'never' because the information does not exist. A combined 77% said the reason for this was 'rarely' or 'never' because the information cannot be found.

Magnetic audio-visual information

What we asked and why

We asked survey participants:

- If the organisation holds magnetic audio-visual (AV) information in specified formats (Q.28 and Q.29).
- How much of that information it holds and if it plans to reformat it within the next 2 years (Q.30 and Q.31).

Magnetic tape technology was used for audio and video throughout the 20th century. Many of these tape-based formats are now obsolete. The National Film and Sound Archive of Australia predicts that any tape that is not digitised by 2025 will likely be lost forever.[7] This is due to a combination of lack of playback equipment, inability to maintain playback equipment, and loss of skills in analogue-to-digital transfer. In addition, some tape-based formats have serious preservation issues due to the physical material involved.

We know magnetic media is an at-risk format but we do not know how much of it is held by public sector organisations. We need to forecast what magnetic media might be coming our way so that we can plan for rapidly addressing reformatting issues. We also need to determine what guidance to give organisations that hold magnetic media, regardless of whether it is marked for transfer to our repositories, so that they can meet their legal requirement to maintain information in accessible form.

Findings

27 percent of respondents said that they 'definitely' hold magnetic AV information, while 22% replied 'possibly' and 19% 'don't know' (Figure 27). The most common formats held are VHS and audio cassette. A small number of respondents hold formats that we consider high risk, such as 2" quad, ¼ inch open reel and 16mm magtrack.

44 percent of respondents with magnetic AV information said that they do not know how much of it they hold. While the data seems to indicate that only a small number of respondents hold this type of information in large quantities, the fairly high percentage of 'don't know' responses makes this figure unreliable (Figure 28). Of the 106 respondents with magnetic AV information, 19% are planning to do reformatting within the next 2 years.

7 (2017). National Film and Sound Archives of Australia. *Deadline 2025*.

Figure 27: Organisations that have magnetic audio-visual information

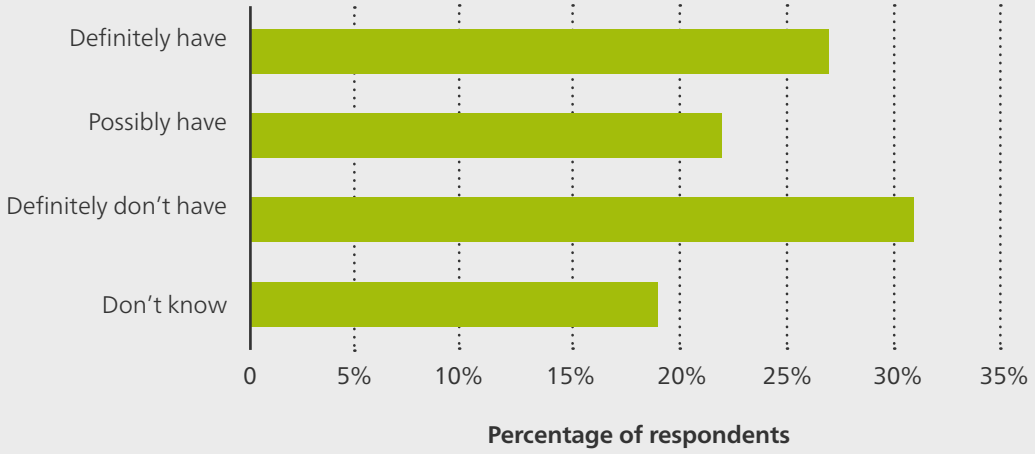
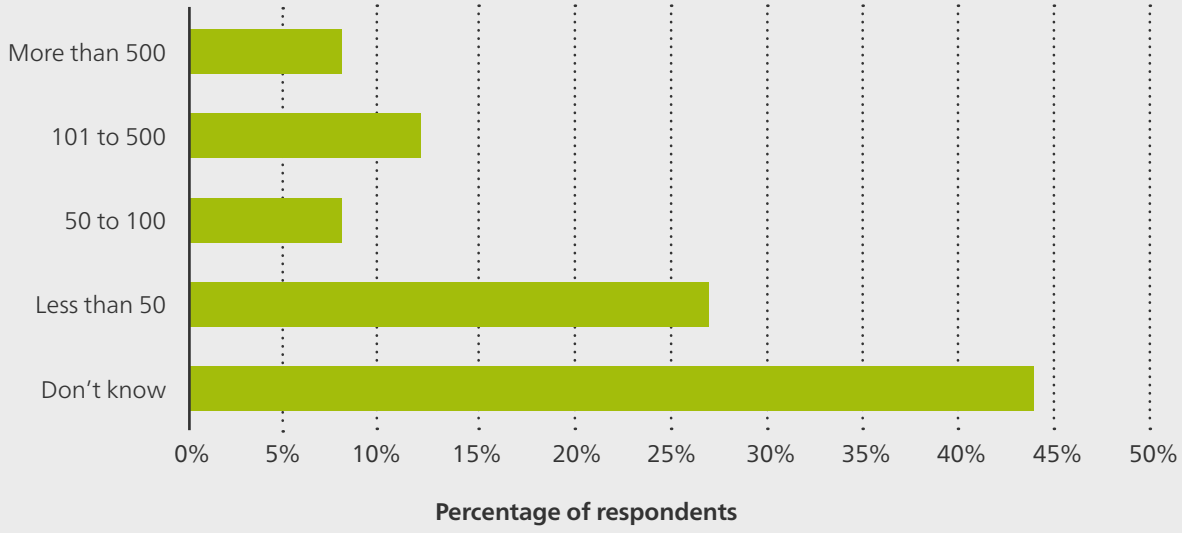


Figure 28: Quantity of magnetic audio-visual information held



Key findings

It is unsurprising that risk management is a key driver for IM in many organisations and this confirms that risk continues to be a strong selling point for how we communicate about IM. We think that we could do more to promote the value of information and good IM for fulfilling organisations' strategic goals. This might assist with building appreciation of the importance of IM among decision-makers.

Some of the challenges that respondents face are outside of our control as a regulator, such as the scale and pace of technological change. However, we are taking steps to improve our capability to provide rapid and useful advice on technical and technological challenges.

For challenges that we can influence more readily, some are likely to require constant, ongoing effort on our part, such as communicating the importance of IM. We are already looking at ways to better reach senior leaders and the ICT community, as we implement some of the recommendations from the *Chief Archivist's Annual Report on the State of Government Recordkeeping 2019/20*.

Upskilling to meet the challenges of digital IM is clearly an issue for both public sector IM staff and us.

As with the challenges, some of the risks to information that respondents highlighted are out of our control, such as the risks associated with out-of-support business systems. For others, we are exploring technologies and architectures, such as an all-of-government ontology, that will assist organisations with addressing information discovery and interpretation issues.

The questions about magnetic AV information were a one-off for the 2019/20 survey to give us a sense of the extent of AV holdings and to inform next steps. Generally, the proportion of 'don't know' responses to these questions suggests a lack of knowledge about whether AV information is held and in what quantities. We may get in touch with individual organisations that have extensive or high-risk holdings to gather further details and discuss how we can support them with managing this information. Organisations that have AV holdings should familiarise themselves with our guidance on *Audiovisual Storage*. They can also contact us for advice on addressing the access and preservation issues associated with magnetic media.

Appendix 1

Survey questionnaire and tables

Note: Except for Q.2 the following tables do not tally comments received through the 'Other (please specify)' response option. Comments are available in the survey data published on data.govt.nz.

Table: Q2 What type of organisation is it?

Response options	Number	Percent
Crown Entity	69	32%
Local Authority	52	24%
Central Government Department	28	13%
Tertiary Education Entity	20	9%
Other, please specify	18	8%
District Health Board	14	7%
State-owned Enterprise	7	3%
Office of Parliament	3	1%
Non-Public Service Department	3	1%
Total	**214**	**100%**

Table: Q3 Which of the following describes this organisation's physical location(s)?

Response options	Number	Percent
Offices located across more than one town city but all in New Zealand	119	56%
One office only	44	21%
More than one office, all of them in the same town city	35	16%
Offices located across more than one country	16	7%
Total	**214**	**100%**

Table: Q4 How many full-time equivalent employees (FTEs) are working for this organisation?

Response options	Number	Percent
Less than 100	60	28%
100 to 299	48	22%
300 to 499	25	12%
500 to 2999	54	25%
3000 to 5999	14	7%
More than 6000	13	6%
Total	**214**	**100%**

Table: Q5 How many full-time equivalent (FTEs) are dedicated IM staff?

Explanatory note: This question is about dedicated information management (IM) staff. Do not include staff whose work is in: geographic information systems (GIS), business intelligence, data management, medical records, or staff whose main role is not in IM, e.g. a business support assistant who oversees IM operations.

Response options	Number	Percent
No IM FTE	44	21%
1 IM FTE or less	73	34%
More than 1 up to 3 IM FTE	44	21%
More than 3 up to 6 IM FTE	25	12%
More than 6 up to 10 IM FTE	20	9%
More than 10 IM FTE	8	4%
Total	**214**	**100%**

Table: Q6 In the last 12 months, which of the following has any dedicated IM staff member(s) done? Tick all that apply (N=214)

Response options	Number	Percent
Attended an IM conference, or similar event	81	38%
Presented at an IM conference, or similar event	19	9%
Attended an IM training course, face-to-face and/or online	101	47%
Studied towards a recognised IM qualification	25	12%
Had an IM relevant secondment	9	4%
None of these	87	41%

Table: Q7 What current drivers for good IM practice and processes are important to your organisation? Please provide an answer for each row (N=214)

Drivers	Not at all important	A little important	Fairly important	Extremely important	Don't know
Business efficiency	0	4	66	144	0
Risk management	0	1	48	165	0
Customer service delivery	2	18	57	136	1
Compliance with legislative requirements	0	9	42	163	0
Efficient cost management	1	18	111	83	1
In-house collaboration	2	16	92	102	2
Collaboration with other organisations	8	44	95	65	2

Table: Q8 Below are some challenges for good IM practices and processes. In this organisation, how big a challenge are these to this organisation's IM? Please provide an answer for each row (N=214)

Challenges	No challenge at all	Minor challenge	Reasonably big challenge	Huge challenge	Don't know
Lack of understanding of the importance of IM	7	67	119	20	1
IM not adequately addressed in planning phase of projects	14	63	92	43	2
IM insufficiently resourced	23	74	77	39	1
Silos - a lack of communication across business groups	19	65	98	32	0
Information incomplete, e.g. not providing evidence of decisions	25	99	73	12	5
Information not easily searchable	10	83	82	39	0
Information is not easily accessible	16	95	77	26	0

Table: Q9 Does your organisation have a formal governance group which:

Explanatory note: This question is about a formal governance group that has been officially set up to provide direction, support and oversight of IM at the executive level.

Response options	Number	Percent
Has IM oversight as part of its mandate?	91	43%
Is dedicated to IM?	20	9%
Neither of the above	103	48%
Total	**214**	**100%**

Table: Q10 Does this organisation's formal governance group meet at least twice a year?

Response options	Number	Percent
Yes	102	92%
No	3	3%
Don't know	6	5%
Total	**111**	**100%**

Table: Q11 Is the Executive Sponsor part of this formal governance group?

Response options	Number	Percent
Yes	96	86%
No	14	13%
Don't know	1	1%
Total	**111**	**100%**

Table: Q12 Has the organisation identified information it holds that is of importance to Māori?

Response options	Number	Percent
Don't hold any	17	8%
Yes	83	39%
No	80	37%
Don't know	34	16%
Total	**214**	**100%**

Table: Q13 Which of the following has this organisation done to improve the usage of information that is of importance to Māori? Tick all that apply

Explanatory note: This question is about usage of information that is of importance to Māori.

Response options	Number	Percent
Documented IM implications from Te Tiriti o Waitangi/Treaty of Waitangi agreements	20	24%
Involved IM staff in negotiating agreements with Māori	11	13%
Improved access	35	42%
Improved discoverability e.g. improved metadata	31	37%
Improved levels of care	18	22%
Worked with Māori to change IM practices	22	27%
No action taken	15	18%
		N=83

Table: Q14 In the last 12 months, has this organisation done any self-monitoring of its compliance with: Tick all that apply

Response options	Number	Percent
Archives New Zealand's requirements?	109	51%
This organisation's own IM policy?	112	52%
Neither of these	65	30%
		N=214

Table: Q15 What method(s) were used for self-monitoring? Tick all that apply

Response options	Number	Percent
Bench marking exercise	21	14%
Assessment by a third party	26	17%
Internal audit	57	38%
Review of processes	111	74%
Risk assessment	62	42%
		N=149

Table: Q16 As a result of self-monitoring, what action is this organisation taking? Tick all that apply

Response options	Number	Percent
Developing an action plan	67	45%
Developed an action plan	35	23%
Implementing an action plan	46	31%
Implemented an action plan	12	8%
Deferring action	6	4%
None of these	17	11%
		N=149

Table: Q17 Does this organisation have a documented IM policy?

Response options	Number	Percent
Yes	175	82%
No	35	16%
Don't know	4	2%
Total	**214**	**100%**

Table: Q18 Which of the groups below does this organisation inform about their IM responsibilities? Tick all that apply

Response options	Number	Percent
Staff at all levels	201	94%
Contractors	115	54%
Consultants	88	41%
None of these	11	5%
		N=214

Table: Q19 In which way(s) does this organisation inform the groups that you ticked in the previous question about their IM responsibilities? Tick all that apply

Response options	Number	Percent
Contracts	97	48%
Code of conduct	98	48%
Job descriptions	76	37%
Induction training, face-to-face and/or online	163	80%
Refresher training, face-to-face and/or online	103	51%
Performance development plans/agreements	30	15%
None of the above	2	1%
Don't know	1	0%
		N=203

Table: Q20 Are all of this organisation's business processes fully digital?

Response options	Number	Percent
Yes	25	12%
No	187	87%
Don't know	2	1%
Total	**214**	**100%**

Table: Q21 Is this organisation taking action to transition from paper-based to digital business processes?

Response options	Number	Percent
Yes	173	92%
No	16	8%
Total	**189**	**100%**

Table: Q22 What action(s) is this organisation taking to transition from paper-based to digital business processes? Tick all that apply

Response options	Number	Percent
Becoming 'digital by default'	108	62%
Re-designing business processes and services to remove paper	151	87%
Introducing digital authorisation in business processes	124	72%
Scanning paper-based information at point of receipt	130	75%
Back-scanning of paper-based information, where the digital version becomes the authoritative version	96	55%
		N=173

Table: Q23 Does this organisation have an information asset register (or similar way of recording information assets)?

Response options	Number	Percent
No	82	38%
In development	56	26%
Yes	47	22%
Work started but deferred	29	14%
Total	**214**	**100%**

Table: Q24 Is that register:

Response options	Number	Percent
Up-to-date?	29	62%
Being used?	34	72%
Neither of these	5	11%
		N=47

Table: Q25 Is this organisation planning to have such an information asset register or similar?

Response options	Number	Percent
Yes	29	35%
No	22	27%
Don't know	31	38%
Total	**82**	**100%**

Table: Q26 Has this organisation identified any key risks to its information?

Response options	Number	Percent
Yes	177	83%
No	28	13%
Don't know	9	4%
Total	**214**	**100%**

Table: Q27 What key risks to this organisation's information have been identified? Tick all that apply

Response options	Number	Percent
Lack of off-site backup	13	7%
Information stored on obsolete or at-risk mediums, e.g. floppy disks	56	32%
Information stored on obsolete or at-risk file formats, e.g. WordStar files	41	23%
Lack of contextual information to enable discovery and interpretation	103	58%
Information stored on business systems which are out of support	88	50%
Inadequate access and use controls for privacy and security	84	47%
Deterioration, of physical information and or digital information stored on physical mediums	63	36%
Storage failure, i.e. loss and/or corruption of data, inaccessible data	55	31%
		N=177

Table: Q28 Does your organisation have magnetic audio-visual records on any of the following formats:

VHS, U-matic, 2" Quad, Video8, audio cassette, micro cassette, ¼ inch open reel, 16mm magtrack, Betacam, Beta SP, Betamax?

Response options	Number	Percent
Definitely have	58	27%
Possibly have	48	22%
Definitely don't have	67	31%
Don't know	41	19%
Total	**214**	**100%**

Table: Q29 Which of these does this organisation have? Tick all that apply

Response options	Number	Percent
Formats not known	34	32%
VHS	74	70%
U-matic	4	4%
2" Quad	3	3%
Video8	6	6%
Audio cassette	49	46%
Micro cassette	21	20%
¼ inch open reel	6	6%
16mm magtrack	5	5%
Betacam	3	3%
Beta SP	4	4%
Betamax	3	3%
Digital audio tape (DAT)	13	12%
		N=106

Table: Q30 Approximately how many magnetic audio-visual records does this organisation hold?

Response options	Number	Percent
Less than 50	29	27%
50 to 100	9	8%
101 to 500	13	12%
More than 500	8	8%
Don't know	47	44%
Total	**106**	**100%**

Table: Q31 Does this organisation plan to reformat its magnetic audio-visual records within the next 2 years?

Response options	Number	Percent
Yes	20	19%
No	45	42%
Don't know	41	39%
Total	**106**	**100%**

Table: Q32 Has this organisation identified its most important high-value/high-risk information?

Explanatory note: For more information about this please see Factsheet 16/F2.

Response options	Number	Percent
Yes	78	36%
In progress	91	43%
No	39	18%
Don't know	6	3%
Total	**214**	**100%**

Table: Q33 In the last 12 months, in order to actively manage its high-value/high-risk information, what action(s) has this organisation taken? Tick all that apply

Explanatory note: 'Business information systems' in the list below include human resources information systems (HRIS), financial systems, specialised databases etc.

Response options	Number	Percent
Tested its Business Continuity Plan	126	59%
Implemented a new business information system to mitigate risks to information	74	35%
Redeveloped systems to improve long-term accessibility of information	82	38%
Don't know	21	10%
		N=214

Table: Q34 In the last 12 months, has this organisation implemented any new business information system(s)?

Explanatory note: 'Business information systems' in the list below include human resources information systems (HRIS), financial systems, specialised databases etc.

Response options	Number	Percent
Yes	146	68%
No	65	30%
Don't know	3	1%
Total	**214**	**100%**

Table: Q35 Is a process for managing information through its life-cycle built into this organisation's new business information system(s)?

Response options	Number	Percent
Yes	73	50%
No	48	33%
Don't know	25	17%
Total	**146**	**100%**

Table: Q36 Which challenge(s) affect this organisation's ability to integrate IM requirements into new or upgraded business information systems? Tick all that apply

Response options	Number	Percent
The number of systems in use	119	56%
IM requirements are not specified in the procurement process	99	46%
Internal staff are not fully aware of the requirements	131	61%
IM staff are not consulted enough	112	52%
Not enough management support	52	24%
None	26	12%
Don't know	5	2%
		N=214

Table: Q37 Do this organisation's current systems for managing documents and records meet the requirements set in Archives New Zealand's minimum requirements for metadata?

Response options	Number	Percent
All systems do	34	16%
Some systems do	153	71%
No systems do	6	3%
Don't know	21	10%
Total	**214**	**100%**

Table: Q38 Does this organisation have any digital information of long-term value (i.e. required for more than 10 years)?

Response options	Number	Percent
Yes	178	83%
No	21	10%
Don't know	15	7%
Total	**214**	**100%**

Table: Q39 This question is about ensuring that information of long-term value remains usable for as long as required. In the last 12 months, what action(s) has this organisation taken for that purpose? Tick all that apply

Response options	Number	Percent
Identified information needing long-term retention	114	64%
Implemented a digital storage management plan	29	16%
Migrated information to new file formats	49	28%
Migrated information to a long-term digital storage environment	52	29%
Used checksums to monitor integrity of information	12	7%
Ensured metadata is persistently linked to information	62	35%
None of these	22	12%
Don't know	9	5%
		N=178

Table: Q40 Does this organisation have any digital information that is inaccessible (i.e. cannot be located and/or cannot be retrieved and/or cannot be used?

Response options	Number	Percent
Definitely have	32	15%
Possibly have	82	38%
Definitely don't have	61	29%
Don't know	39	18%
Total	**214**	**100%**

Table: Q41 What are the reasons this organisation is unable to access that digital information? Tick all that apply

Response options	Number	Percent
Not enough metadata to easily locate information	66	58%
Information stored in obsolete file formats	65	57%
Information stored in personal systems, e.g. OneDrive	77	68%
Software needed to access information no longer available	39	34%
Physical deterioration of the medium, e.g. CD ROMs	32	28%
Storage failure	17	15%
		N=114

Table: Q42 In the last 12 months, has this organisation had any requests for official information under the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987?

Response options	Number	Percent
Yes	196	92%
No	11	5%
Don't know	7	3%
Total	**214**	**100%**

Table: Q43 In the last 12 months, has this organisation ever been unable to provide the official information asked for?

Response options	Number	Percent
Yes	67	34%
No	101	52%
Don't know	28	14%
Total	**196**	**100%**

Table: Q44 In the last 12 months, how often has the reason for being unable to provide the official information been that the information does not exist (i.e. the record has not been created)?

Response options	Number	Percent
Never	8	12%
Rarely	31	46%
Occasionally	23	34%
Often	1	1%
Don't know	4	6%
Total	**67**	**100%**

Table: Q45 In the last 12 months, how often has the reason for being unable to provide the official information been that the information does exist but could not be found?

Response options	Number	Percent
Never	23	34%
Rarely	29	43%
Occasionally	12	18%
Often	0	0%
Don't know	3	4%
Total	**67**	**100%**

Table: Q46 This question is about business changes that have implications for IM. In the last 12 months, which of these changes has occurred? Tick all that apply

Response options	Number	Percent
Established new functions	81	38%
Established new activity activities within a function	124	58%
As part of an administrative change, received information from another organisation	39	18%
As part of an administrative change, transferred information to another organisation	35	16%
Decommissioned business information systems	69	32%
Decommissioned website	38	18%
Implemented new service offerings	83	39%
Migrated information to a new storage environment	114	53%
Migrated information between systems	119	56%
None of these	23	11%
		N=214

Table: Q47 When business changes occur, they can have an impact on the organisation's information. When the changes that you ticked in the previous question happened, did this organisation take action to guarantee the integrity of the information involved?

Response options	Number	Percent
In every case	110	58%
In some cases	65	34%
Never	4	2%
Don't know	12	6%
Total	**191**	**100%**

Table: Q48 This question is about physical information. Which security risk(s) does this organisation take measures to protect against? Tick all that apply

Response options	Number	Percent
Unauthorised access	205	96%
Unauthorised alteration	136	64%
Unauthorised destruction	169	79%
Loss	137	64%
None of these	7	3%
		N=214

Table: Q49 This question is about storage of digital information. Which security risk(s) does this organisation take measures to protect against? Tick all that apply

Response options	Number	Percent
Unauthorised access	212	99%
Unauthorised alteration	180	84%
Unauthorised destruction	183	86%
Loss	166	78%
None of these	1	0%
		N=214

Table: Q50 Does this organisation hold any information that is more than 25 years old?

Response options	Number	Percent
Yes	163	76%
No	36	17%
Don't know	15	7%
Total	**214**	**100%**

Table: Q51 How much of that information that is more than 25 years old has been classified as either open or restricted access?

Response options	Number	Percent
None or hardly any	48	29%
About a quarter of it	8	5%
About half of it	9	6%
About three quarters of it	13	8%
All or almost all	45	28%
Don't know	40	25%
Total	**163**	**100%**

Table: Q52 How much of the information held by this organisation is covered by authorised disposal authorities?

Explanatory note: This question is about authorised disposal authorities, including: current organisation-specific disposal authorities, general disposal authorities (GDA 6 and 7), and current local authority retention and disposal schedules.

Response options	Number	Percent
None or hardly any	15	7%
About a quarter of it	12	6%
About half of it	12	6%
About three quarters of it	19	9%
All or almost all	121	57%
Don't know	35	16%
Total	**214**	**100%**

Table: Q53 This question is about the information not covered by disposal authorities. When does this organisation plan to start improving coverage?

Response options	Number	Percent
We are currently appraising this organisation's information	29	14%
In less than 12 months	18	8%
In the next 1-3 years	26	12%
In the next 4-5 years	2	1%
Don't know	22	10%
Not specified	117	55%
Total	**214**	**100%**

Table: Q54 This question is about both physical and digital information. In the last 12 months, which action(s) has this organisation carried out in preparation for disposal? Tick all that apply

Explanatory note: 'Sentenced' in the list below means the process of applying a disposal authority and its disposal actions across an organisation's information (see Guide 16/G10). 'Unstructured information' means information that either does not have a pre-defined data model or is not organised in a pre-defined manner.

Response options	Number	Percent
Developed a disposal implementation plan	52	24%
Sentenced information in offsite storage	90	42%
Sentenced unstructured information in business information systems	32	15%
Sentenced unstructured information in shared drives	32	15%
Set up automated disposal in Enterprise Content Management system, or similar	27	13%
Used automated tools to analyse digital files in preparation for transfer, e.g. DROID	7	3%
Obtained approval to dispose of information from business owners	104	49%
None of the above	52	24%
Don't know	15	7%
		N=214

Table: Q55 In the last 12 months, has your organisation carried out authorised destruction of physical information?

Response options	Number	Percent
Yes	111	52%
No	87	41%
Don't know	16	7%
Total	**214**	**100%**

Table: Q56 In the last 12 months, has this organisation carried out authorised destruction of digital information?

Response options	Number	Percent
Yes	55	26%
No	137	64%
Don't know	22	10%
Total	**214**	**100%**

Table: Q57 This question is about both physical and digital information. Which challenge(s) affect this organisation's ability to undertake regular authorised destruction of information? Tick all that apply

Response options	Number	Percent
Not enough resources put towards sentencing activity	127	59%
A lack of confidence that sentencing has been done accurately	41	19%
The cost of secure destruction/deletion through the storage provider	33	15%
The difficulty of obtaining approvals	34	16%
Destruction not seen as a priority for staff	111	52%
Systems not set up to automate regular authorised deletion	148	69%
None of the above	10	5%
Don't know	8	4%
		N=214

Table: Q58 This question is about transferring physical information. In the next 12 months, is this organisation planning to transfer any physical information?

Explanatory note: Public offices can transfer to an Archives New Zealand repository (except to the Wellington repository, which is currently closed for transfers) or to an approved repository. Local authorities can transfer to a local authority archive.

Response options	Number	Percent
Yes	56	26%
No	130	61%
Don't know	28	13%
Total	**214**	**100%**

Table: Q59 Where are you planning to transfer physical information to?

Response options	Number	Percent
An Archives New Zealand repository (Auckland, Christchurch, Dunedin)	28	50%
An Approved Repository	15	27%
A Local Authority archive	9	16%
Don't know	4	7%
Total	**56**	**100%**

Table: Q60 Why is there no plan for transferring physical information in the next 12 months?

Response options	Number	Percent
Wellington repository is closed	37	23%
There is no Local Authority archive to transfer to	12	8%
Have no information over 25 years old	29	18%
Other, please specify	80	51%
Total	**158**	**100%**

Table: Q61 In the next 12 months, is this organisation planning to transfer any digital information to:

Response options	Number	Percent
Archives New Zealand	16	7%
A Local Authority archive	1	0%
Neither of these	157	73%
Don't know	40	19%
Total	**214**	**100%**

Table: Q62 This question is about both physical and digital information. What challenge(s) affect this organisation's ability to undertake regular transfer of information? Tick all that apply

Response options	Number	Percent
Not enough resources put towards sentencing activity	126	59%
Lack of confidence that sentencing has been done accurately	30	14%
Not a priority for senior management	64	30%
Lack of resources to prepare transfer	101	47%
Lack of skills in doing physical transfers	40	19%
Difficulty obtaining approval from senior management	16	7%
Difficulty understanding Archives New Zealand's processes and requirements	37	17%
Archives New Zealand's Wellington repository is not taking transfer of physical information	62	29%
No Local Authority archive to transfer to	15	7%
Current system is unable to export records and descriptive metadata for digital transfer	30	14%
Lack of system support to export records and descriptive metadata for digital transfer	37	17%
Don't know	18	8%
		N=214

Appendix 2

Monitoring criteria

Categories	Criteria	
Governance	1	There is a current organisation-wide strategy for information and records management that is approved by senior management and that has a senior management owner. The strategy is operationalised, reviewed and monitored regularly.
	2	There is a current organisation-wide policy, approved by senior management, which delineates roles and responsibilities for information and records management for Executive Sponsors, Managers, IM staff and all staff including contractors. The policy is implemented, reviewed and monitored regularly.
	3	The organisation has governance arrangements for information and records management into which the Executive Sponsor role is integrated.
	4	Business owners and business units are responsible for ensuring that information management is integrated into business processes and activities.
	5	Outsourced functions, shared services and collaborative work with other public offices, local authorities and /or third parties, specify information and records management obligations, and these are monitored and enforced by the organisation.
	6	The organisation can demonstrate that it understands what information it holds that is important to Māori, and the IM implications of ToW agreements it is party to and manages its information and records appropriately.
Self-monitoring	7	The organisation regularly monitors its level of compliance with information management policies and their alignment with the Public Records Act 2005, any mandatory standards, and with other legislation with IM requirements. It identifies potential improvements and, where appropriate, takes corrective actions.

Capability	8	The organisation identifies the IM skills required to meet its business needs. Internal IRM staff are supported in their professional development, or external skills are accessed as appropriate.
	9	Information and records management roles and responsibilities are assigned, documented and communicated to all levels of the organisation. Staff and contractors are aware of their responsibilities and the organisation's expectations and receive training.
Creation	10	The organisation routinely identifies and creates reliable, usable and accessible information and records to meet legislative, business and user needs.
	11	Information and records needed to support high-value / high-risk business functions are identified, documented and regularly reviewed
Management	12	Requirements for creation, management, metadata, storage and disposal are built into all systems that hold information and records.
	13	Information and records are managed to ensure that they are reliable, usable and complete.
	14	Information and records are managed during system, service and other business changes to ensure preservation and ongoing accessibility.
	15	The organisation has current business continuity and recovery plans to provide for ongoing access to and usability of its information and records for core business functions following a business disruption event. Plans are regularly tested and updated.
Storage	16	Organisation repositories have security and protection mechanisms in place for all information and records, wherever they are held including whether in transit or outside the workplace.
	17	Local authorities store protected information and records in a securely controlled environment suitable for maintaining and preserving archival information and records. **Local authorities only.**
Access	18	The organisation has processes in place to manage access to, the use of, and sharing of information and records, in line with legislative requirements.
	19	All local authority archives are classified as either open or restricted access. **Local authorities only.**

Disposal	20	The organisation has a current, approved disposal authority (or authorities) that covers all formats of its information holdings and all business functions. Disposal authorities are regularly reviewed for relevance.
	21	All information and records are retained for as long as required for business use and their disposal is approved and implemented in accordance with applicable disposal authorities. Disposal is documented.
	22	Public information and records over 25 years that have archival value are transferred to Archives New Zealand, and/or have current deferral of transfer(s) in place. Public offices determine all information and records over 25 years old as having either open or restricted access status.

Appendix 3

List of respondents and non-respondents (A-Z)

Organisation name	Response
Accident Compensation Corporation	Complete
Accreditation Council	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 (Creative NZ)	Complete
Ashburton District Council	Complete
AsureQuality Limited	Complete
Auckland Council	Complete
Auckland DHB	Complete
Auckland Transport	Complete
Auckland University of Technology	Complete
Bay of Plenty DHB	No response
Bay of Plenty Regional Council	No response
Broadcasting Commission	Complete
Broadcasting Standards Authority	Complete
Buller District Council	Complete
Callaghan Innovation (and Callaghan Innovation Research Limited)	No response
Canterbury DHB / West Coast DHB	Complete

Capital and Coast DHB	Complete
Carterton District Council	No response
Central Hawke's Bay District Council	Complete
Central Otago District Council	Complete
Central Region Technical Advisory Services Limited	Complete
Chatham Islands Council	Complete
Children's Commissioner	Complete
Christchurch City Council	Complete
Civil Aviation Authority of New Zealand	Complete
Climate Change Commission	Complete
Clutha District Council	Complete
Commerce Commission	Complete
Commercial Fisheries Services (FishServe)	Complete
Counties Manukau DHB	Complete
Courts of New Zealand Ngā Kotī o Aotearoa	Complete
Crown Irrigation Investments Limited	Complete
Crown Law Office	Complete
Department of Conservation	Complete
Department of Corrections	Complete
Department of Internal Affairs	Complete
Department of Prime Minister and Cabinet	Complete
Drug free Sport New Zealand	Complete
Dunedin City Council	No response
Earthquake Commission	Complete
Eastern Institute of Technology	Complete
Education New Zealand	Complete
Education Review Office	Complete

Electoral Commission	No response
Electricity Authority Te Mana Hiko	Complete
Enable New Zealand Limited	No response
Energy Efficiency and Conservation Authority	Complete
Environment Canterbury (Canterbury Regional Council)	Complete
Environmental Protection Authority	Complete
External Reporting Board (XRB)	Complete
Far North District Council	Complete
Financial Markets Authority	Complete
Fire and Emergency New Zealand	Complete
Game Animal Council	Complete
Gisborne District Council	No response
Gore District Council	Complete
Government Communications Security Bureau	Complete
Government Superannuation Fund Authority	Complete
Greater Wellington Regional Council (Wellington Regional Council)	No response
Grey District Council	Complete
Guardians of New Zealand Superannuation (New Zealand Superfund)	Complete
Hamilton City Council	Complete
Hastings District Council	No response
Hauraki District Council	Complete
Hawke's Bay DHB	Incomplete
Hawke's Bay Regional Council	Complete
Health and Disability Commissioner	Complete
Health Promotion Agency	Complete
Health Quality and Safety Commission	Complete
Health Research Council of New Zealand	Complete

HealthAlliance NZ Ltd	Complete
HealthShare Limited	Complete
HealthSource Ltd	No response
Heritage New Zealand Pouhere Taonga	Complete
High Performance Sport New Zealand Limited	Complete
Horizons Regional Council (Manawatu-Wanganui Regional Council)	Complete
Horowhenua District council	No response
Human Rights Commission	Complete
Hurunui District Council	Complete
Hutt City Council	Complete
Hutt DHB (Hutt Valley DHB)	No response
Independent Police Conduct Authority	Complete
Inland Revenue Department	Complete
Institute of Environmental Science and Research Limited (ESR)	Late response
Institute of Geological and Nuclear Sciences Limited (GNS Science)	Complete
Invercargill City Council	No response
Judicial Conduct Commissioner	No response
Kaikoura District Council	No response
Kāinga Ora - Homes and Communities	Complete
Kaipara District Council	Complete
Kapiti Coast District Council	Complete
Kawerau District Council	No response
KiwiRail Holdings Limited	Complete
Kordia Group Limited	No response
Lakes DHB	Complete
Land Information New Zealand	Complete
Landcare Research New Zealand Limited	Complete

Landcorp Farming Limited	No response
Law Commission	Complete
Lincoln University	Complete
Mackenzie District Council	Complete
Manawatu District Council	Complete
Manukau Institute of Technology	Complete
Maritime New Zealand	Complete
Marlborough District Council	No response
Massey University Te Kunenga Ki Pūrehuroa	Complete
Masterton District Council	Complete
Matamata-Piako District Council	Complete
Meteorological Service of New Zealand Limited	Complete
MidCentral DHB	Complete
Ministry for Culture and Heritage Manatū Taonga	Complete
Ministry for Pacific Peoples	Complete
Ministry for Primary Industries Manatū Ahu Matua	Complete
Ministry for the Environment	Complete
Ministry for Women	Complete
Ministry of Business, Innovation and Employment	Complete
Ministry of Defence	Complete
Ministry of Education Te Tāhuhu o te Mātauranga	Complete
Ministry of Foreign Affairs and Trade	Complete
Ministry of Health	Complete
Ministry of Housing and Urban Development	Incomplete
Ministry of Justice Tāhū o te Ture	Complete
Ministry of Māori Development Te Puni kokiri	Complete
Ministry of Social Development	Complete

Ministry of Transport	Complete
Museum of New Zealand Te Papa Tongarewa Board	Complete
Napier City Council	Complete
National Institute of Water and Atmospheric Research Limited (NIWA)	Complete
National Pacific Radio Trust	No response
Nelson City Council	Complete
Nelson Marlborough District Health Board	Complete
Nelson Marlborough Institute of Technology (NMIT)	Complete
NetSafe Incorporated	Complete
New Plymouth District Council	No response
New Zealand Antarctic Institute (Antarctica New Zealand)	Complete
New Zealand Artificial Limb Service	Complete
New Zealand Blood Service	Complete
New Zealand Customs Service	Complete
New Zealand Defence Force	Complete
New Zealand Film Commission	Complete
New Zealand Fish and Game Council	Incomplete
New Zealand Forest Research Institute Limited (Scion)	Complete
New Zealand Green Investment Finance Ltd	Complete
New Zealand Health Partnerships Limited	No response
New Zealand Infrastructure Commission Te Waihanga	Complete
New Zealand Institute of Skills and Technology	No response
New Zealand Lotteries Commission	Complete
New Zealand Parole Board	Complete
New Zealand Police	Complete
New Zealand Post Limited	No response
New Zealand Productivity Commission	Complete

New Zealand Qualifications Authority	Complete
New Zealand Railways Corporation (NZRC)	No response
New Zealand Security Intelligence Service	Complete
New Zealand Symphony Orchestra	No response
New Zealand Tourism Board (Tourism New Zealand)	Complete
New Zealand Trade and Enterprise	Complete
New Zealand Transport Agency Waka Kotahi	Complete
New Zealand Venture Investment Fund Limited	No response
New Zealand Walking Access Commission	Complete
Northern Regional Alliance Limited	Complete
Northland DHB	Complete
Northland Polytechnic (NorthTec)	Incomplete
Northland Regional Council	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
Opotiki District Council	Complete
Oranga Tamariki - Ministry for Children	Complete
Otago Polytechnic Limited	Complete
Otago Regional Council	No response
Otorohanga District Council	Complete
Palmerston North City Council	Complete
Parliamentary Commissioner for the Environment	Complete
Parliamentary Counsel Office	Complete
Parliamentary Service	Complete
Pharmaceutical Management Agency (PHARMAC)	Complete

Plant and Food Research	Complete
Porirua City Council	No response
Privacy Commissioner	Complete
Public Service Commission Te Kawa Mataaho	Complete
Public Trust	Complete
Queenstown-Lakes District Council	No response
Quotable Value Limited	Complete
Radio New Zealand Limited	Late response
Rangitikei District Council	No response
Real Estate Agents Authority	Complete
Reserve Bank of New Zealand	Complete
Retirement Commissioner	Complete
Rotorua Lakes Council	No response
Royal Commission of Inquiry into Historical Abuse in State Care and in the Care of Faith-based Institutions	Complete
Ruapehu District Council	No response
Selwyn District Council	Complete
Serious Fraud Office	Complete
Social Workers Registration Board	Complete
South Canterbury DHB	Complete
South Taranaki District Council	Incomplete
South Waikato District Council	No response
South Wairarapa District Council	Complete
Southern District Health Board	Complete
Southern Institute of Technology Limited	Complete
Southland District Council	Complete
Southland Regional Council (Environment Southland)	Complete
Sport and Recreation New Zealand (Sport New Zealand)	Complete

Statistics New Zealand	Complete
Stratford District Council	Complete
STRMix Limited	No response
Tai Poutini Polytechnic Limited	Complete
Tairawhiti DHB	Complete
Takeovers Panel	Complete
Taranaki DHB	Complete
Taranaki Regional Council	No response
Tararua District Council	No response
Tasman District Council	Complete
Taupō District Council	Complete
Tauranga City Council	Complete
Te Kāhui Whakamana Rua Tekau mā Iwa Pike River Recovery Agency	Complete
Te Reo Whakapuaki Irirangi (Te Māngai Pāho) 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	No response
Te Whare Wānanga o Awanuiārangi	No response
Television New Zealand Limited	Complete
Tertiary Education Commission	Complete
Thames-Coromandel District Council	Complete
The Māori Trustee (Te Tumu Paeroa)	Complete
The Office for Māori Crown Relations - Te Arawhiti	Complete
The Open Polytechnic of New Zealand Limited	Complete
The Treasury Te Tai Ōhunga	Complete
Timaru District Council	Complete
Toi-Ohomai Institute of Technology Limited	Complete

Transport Accident Investigation Commission	Complete
Transpower New Zealand Limited	Complete
Unitec Institute of Technology Limited	Complete
Universal College of Learning Limited (UCOL)	Complete
University of Auckland	Complete
University of Canterbury	Complete
University of Otago	Complete
University of Waikato	Complete
Upper Hutt City Council	Complete
Victoria University of Wellington	Complete
Waikato DHB	Complete
Waikato District Council	Complete
Waikato Institute of Technology Limited (Wintec)	Complete
Waikato Regional Council	Complete
Waimakariri District Council	Complete
Waimate District Council	Complete
Waipa District Council	Complete
Wairarapa DHB	Complete
Wairoa District Council	Complete
Waitaki District Council	Complete
Waitemata DHB	Complete
Waitomo District Council	Complete
Wellington City Council	Complete
Wellington Institute of Technology	No response
West Coast Regional Council	No response
Western Bay of Plenty District Council	Complete
Western Institute of Technology at Taranaki	No response

Westland District Council	Complete
Whakatāne District Council	No response
Whanganui DHB	Complete
Whanganui District Council	No response
Whangarei District Council	No response
Whitireia Community Polytechnic / Weltec	No response
WorkSafe New Zealand Mahi Haumaru Aotearoa	Complete

Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

New Zealand Government