Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

FINDINGS REPORT

Survey of public sector information management 2020/21

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

Minister's foreword

Tēnā koutou

Te Rua Mahara o Te Kāwanatanga, Archives New Zealand (Archives), is committed to transparency of public sector performance against the requirements of the Public Records Act 2005. The survey of public sector information management is critical to maintaining public confidence in information quality and stewardship, and to enabling public sector organisations to lift their performance.

This is the third year of the Archives' annual survey, a core tool used to collect information for monitoring purposes. The report confirmed no significant information management improvement and there is clearly much more effort required to increase and sustain information management performance across the sector. Clear patterns are emerging that Archives, as a regulator, needs to work with the sector to improve.

To achieve this outcome, I encourage all public offices and local authorities to participate in the annual survey to ensure that the current state of information management continues to be accurately reflected in these findings. I also encourage the leadership of those organisation to reflect on the findings and identify where they could focus their efforts to improve performance, and address risk.

Nō reira

Hon Jan Tinetti
Minister for Internal Affairs

Executive summary

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

Te Rua Mahara o te Kāwanatanga Archives New Zealand (Archives) uses its annual survey as a core mechanism to gather information for monitoring purposes. It provides the data for tracking organisational improvement over time and informing how public sector organisations information management (IM) practice is performing against the requirements of the Public Records Act 2005 (PRA) and the mandatory standard.

The Survey of public sector information management 2020/21 (the survey) is the third annual survey delivered in the current series. It surveyed 258 public sector organisations: 180 public offices were required to respond by 'direction to report' (section 31 of the PRA), and 78 local authorities were invited to respond. The survey response rate was 84%, slightly up on last year's 80%.

A third year of the survey has provided added assurance to the consistency of information and data gathered in the series. The report confirmed no significant IM improvement across the public sector and supports what the 2010 Government Recordkeeping Survey told us. While the comparisons with the 2010 survey are indirect, they clearly indicate that collective IM maturity has not uplifted significantly and that much more effort is required to increase and sustain IM performance across the sector.

Reporting on the five key indicators (fundamental building blocks for effective IM) provides a high-level perspective on whether IM practice is improving, declining or remaining stable. Recommendations against the key indicators from our 2019/20 Report on the State of Government Recordkeeping talked about what action we could take to encourage the progress and improvements we want to see. These recommendations have been updated in this survey findings report and shared through 'Developments and next steps' for each indicator.

The number of organisations implementing governance groups for IM is up from 52% to 60%. While there is improvement in this area Archives acknowledges that there will need to be a concerted effort from the remaining 40% to raise the number of governance groups across the sector.

Archives considers that an active governance group is the foundation for lifting the importance of IM in organisations and integrating it into business operations. Previous surveys have found a statistically significant relationship between the existence of a formal governance group for IM and a positive result against indicator 4. This remains the case in the 2020/21 survey and supports the conclusion that when a formal governance group is present there is a greater likelihood that the organisation will build IM requirements into new business systems.

However, it is unacceptable to see only a marginal increase overall in IM requirements being built into business systems implemented in the last 12 months, the percentage increase being from 50% to 52%. Given that IM requirements have been mandatory for over a decade now it

is alarming to see the low number of organisations that have built IM requirements into new business systems.

For the first time this year we see an overall increase in the number of IM staff employed by public sector organisations, an increase of 68 IM FTEs across the public sector organisations. Proportionally, the percentage of organisations with 'some' IM staff versus none remains static at 79% for the third year running. The proportion of local authorities with 'some' IM staff is much higher compared to public offices. Almost all local authorities have some IM FTE. For organisations with fewer than 100 total FTE it is common to have no IM staff at all.

Identifying high-value/high-risk information is a foundation for IM activities and is a critical first step towards mitigating associated risks and extracting maximum value from information assets. If mismanaged, it could expose the organisation to major financial risk, material loss, breach of statutory obligations or loss of reputation. Organisations identifying their high-value/high-risk information shows a slight decline and is almost static at 35% compared with 36% in 2019/20. Percentage in progress is 49% compared to 43% in 2020.

Collaboration with iwi and Māori entities remains central to developing Mātauranga Māori strategies and policies for IM. Some progress has been made, improving access and discoverability, and this remains the most common activity for organisations. Public sector organisations are encouraged to improve Māori metadata in consultation and collaboration with iwi/Māori. Consider adding new fields, or more tagging capability and/or metadata for iwi/Māori concepts.

General disposal authorities (GDAs) (GDA 6 and GDA 7) 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. GDAs are designed to make it easy to destroy information that has no long-term value. Destruction, as one of the approved methods of disposal, is an activity that all public sector organisations can do, and is an important component of effective IM. Through the destruction of low-value information accessibility to high-value information is improved and the cost of management and storage is reduced. Organisations actively doing authorised destruction in the past 12 months has gone down slightly to 56% from 58%. There has been a small decrease in destruction for two years running, with authorised destruction of digital information being much lower than physical information.

Digital instability is identified as the most common risk, whether it is the use of shadow IT, or outdated digital storage which compromises the integrity of the information stored. External cyber-attacks have been identified as a significant concern for organisations. The need to upskill IM staff is identified and presents as a challenging issue for public sector organisations.

Key findings from the survey have shown some areas of improvement however this is not a significant enough step forward to demonstrate any meaningful change. It is not surprising that risk management remains a key driver for IM in many organisations and confirms that risk should underpin how we communicate about IM. COVID-19 remains the largest impact on organisations and their IM practices this year. The ability to access information remotely and digitally is more important than ever for operations.

It is vital that we understand what motivates public sector organisations in IM. Archives annual survey on public sector information management is one way of improving that knowledge.

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

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 from our Monitoring Framework (Appendix 2). 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

The annual survey covers central government organisations, referred to by the Public Records Act 2005 (PRA) as 'public offices', and local authorities (i.e. councils) but excludes:

- school boards;
- Crown entity subsidiaries;
- reserve boards as defined in section 2 of the Reserves Act 1977;
- regional fish and game councils;
- Ministers of the Crown; and
- council-controlled organisations.

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

The Standard/Information and records management standard - Under section 27 of the Public Records Act 2005 Archives New Zealand issued the Information and records management standard. The standard supports the systematic and efficient management of government information and records, outlining the obligations of regulated organisations under the Public Records Act.

Key findings from the 2020/21 Survey of public sector information management

Introduction

In 2020/21 Archives New Zealand conducted its third annual survey of information management (IM) practices in public offices and local authorities. The objectives of the survey are to:

Establish and track how well public sector organisations are performing against the requirements of the PRA, the Information and records management standard, and good IM practice

Allow tracking of improvements to organisations' performance over time

Identify the risks, challenges, opportunities, and emerging trends affecting IM in organisations, so we can feed this intelligence into responsive regulation

Provide public visibility of organisations' performance

This section of the report examines performance over time against five key indicators. When we reinstated the survey in 2019, we selected a handful of indicators to measure the overall state of public sector IM. The indicators provide a high-level perspective on whether IM is improving, declining or remaining stable. They focus on:

1. Implementing governance groups for information management
2. Overall number of IM staff employed by public sector organisations
3. Identifying high-value and/or high-risk information
4. Building IM requirements into new business systems
5. Active, authorised destruction of information

The key indicators are not the sole measure of the state of public sector IM, but we consider them to be fundamental building blocks for effective IM. The full survey results provide more comprehensive data on the performance of public sector organisations. These results will be reported on **data.govt.nz**.

Who was surveyed?

The annual survey covers central government organisations, referred to by the Public Records Act 2005 (PRA) as 'public offices', and local authorities (i.e. councils) but excludes:

- school boards;
- Crown entity subsidiaries;
- reserve boards as defined in section 2 of the Reserves Act 1977;
- regional fish and game councils;
- Ministers of the Crown; and
- council-controlled organisations.

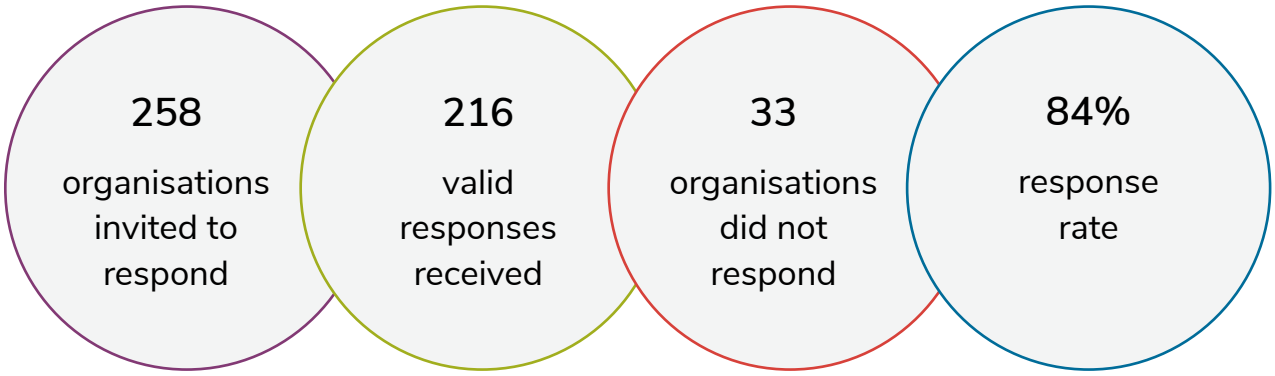
The survey was sent to 258 public sector organisations, including:

- 180 public offices, which were required to respond by direction to report (section 31 of the PRA)
- 78 local authorities, which were invited to respond

The questionnaire was delivered via the online survey tool SurveyMonkey and was open from 8-25 June 2021. Executive Sponsors from organisations in scope were invited to participate and were asked to coordinate their organisation's response.

Response rates

The survey recorded an 84% response rate, slightly up on last year's figure of 80%. We received five late responses and four partial responses, all of which were excluded from analysis. A total of 33 organisations did not respond, comprising 15 public offices and 18 local authorities. The responses from the Government Communications Security Bureau and New Zealand Security Intelligence Service are excluded from the analysis. Some organisations were permitted to submit combined responses, in cases where they shared both an Executive Sponsor and IM. For the purposes of calculating response rates, these responses were counted as a single public office or local authority.



Responding to the 2020 survey findings

In the 2019/20 Report on the State of Government Recordkeeping, we made recommendations against each of the key indicators. The recommendations focused on actions we could take to encourage the progress and improvements we want to see. This year we are including an update on the work we have done to address those recommendations. To learn more, refer to the 'Developments and next steps' section for each indicator.

INDICATOR 1

An increasing number of organisations have implemented governance groups for information management

What we asked and why it is important

We asked survey participants if they have a formal governance group in place which is either dedicated to IM or has IM oversight as part of its mandate (Q.5).

The Standard requires that: Information and records management must be the responsibility of senior management. Senior management must provide direction and support to meet business requirements as well as relevant laws and regulations (1.2).

The role of an active governance group is to ensure, 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.

What we found and how it compares to previous surveys

This year, the percentage of respondents with a formal governance group in place increased to 60% compared to 52% in 2019/20 (Figures 2 and 3). We are pleased to see this upward trend but will continue our efforts to influence change in the 40% of organisations that do not have a formal governance group.

In Figure 1, the change between 2018/19 and 2019/20 is represented as a dotted line to show that the increase is influenced by modifications to the question. The 2018/19 survey offered an 'in development' response option, which was selected by 24% of responding organisations. Subsequent surveys did not offer this option.

Figure 1: Change over time for Indicator 1

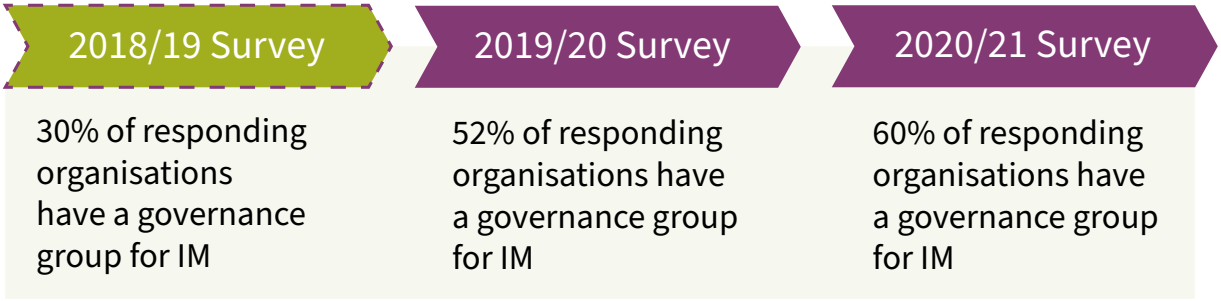
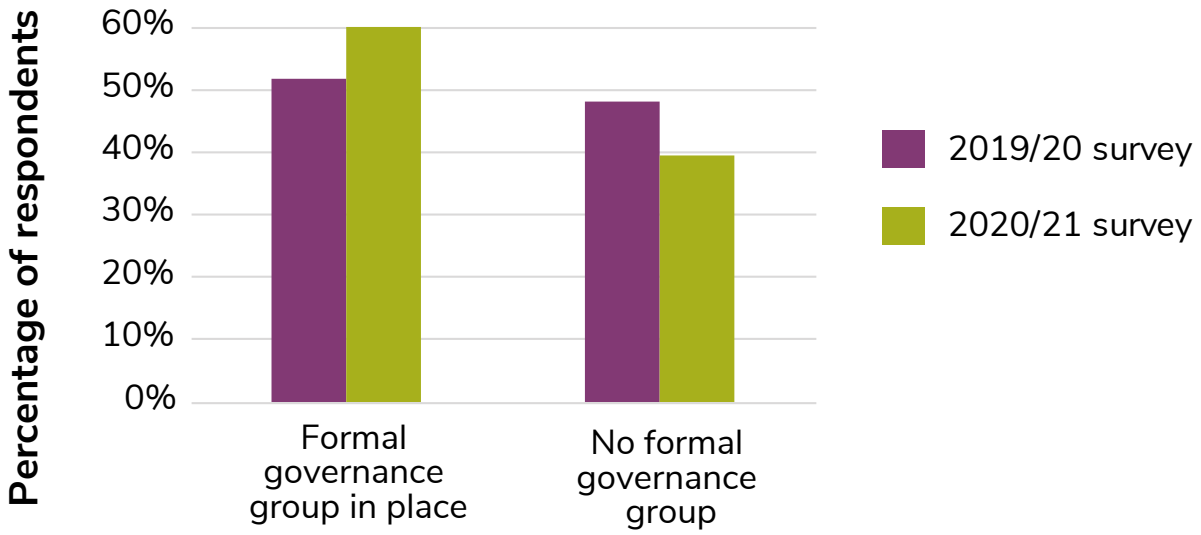


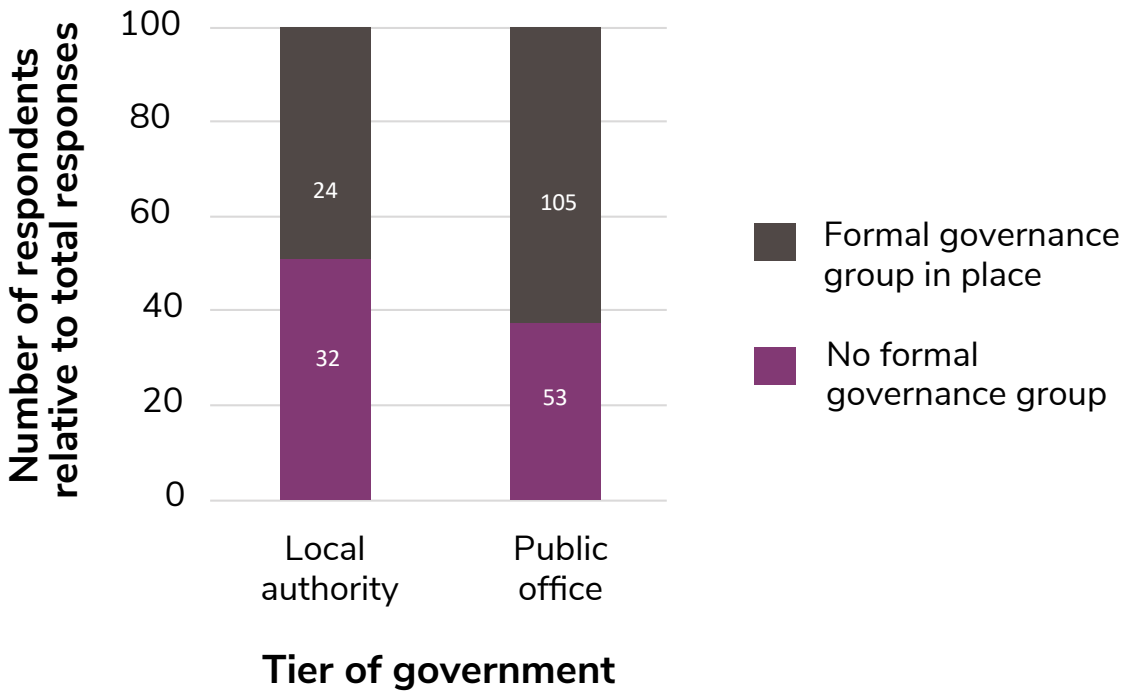
Figure 2: 2019/20 and 2020/21 results for Indicator 1[1]



Looking at the response split by tier of government, local authority respondents are less likely to have a formal governance group in place than public offices (see Figure 3).

1 Data from the 2018/19 survey is not plotted in Figure 2. The question was asked differently, with an 'in development' option provided.

Figure 3: Formal governance groups compared to tier of government



Developments and next steps

In 2019/20 we identified the following potential actions for influencing change in organisations that do not have a formal governance group:

- Make our expectations more explicit in our guidance, communications and interactions with Executive Sponsors.
- Engage with selected organisations that hold high-value and/or high-risk information, on the basis that an absence of formal IM governance heightens the risk of IM failure and consequent public harm.
- Engage with individual organisations that lack formal IM governance as a component of follow-up on their audit findings.

Since then, we have started revising our guidance and planning for a series of recurring engagement sessions for Executive Sponsors, where governance arrangements will be addressed. At the time of writing, 6 out of the 31 organisations audited in the previous year have been asked to include establishment of an IM governance group in their post-audit action plans.

In addition to the above work, the data suggests that an extra focus on encouraging IM governance groups in local authorities may be needed. This could include communicating our expectations in local government-specific forums.

INDICATOR 2

An overall increasing number of IM staff employed by public sector organisations

What we asked and why it is important

We asked how many dedicated, full-time equivalent (FTE) IM staff organisations employed (Q.15). The question asked respondents to exclude staff in geospatial information systems, business intelligence, data management, medical records or staff whose main role is not IM.

The Standard requires that: Organisations must have information and records management staff, or access to appropriate skills (1.4).

IM impacts all areas of business, and IM specialists should be involved and included in a wide variety of business activities. These include system and process design, information and records sharing, risk management, and managing information, data and records for accountability and value.

As new technologies proliferate at speed, the opportunities and challenges for meeting IM requirements also multiply. IM specialists remain essential for the proper functioning of digital government, through their IM leadership and advocacy, and by harnessing the abilities of technology to make IM easier for their organisations.

What we found and how it compares to previous surveys

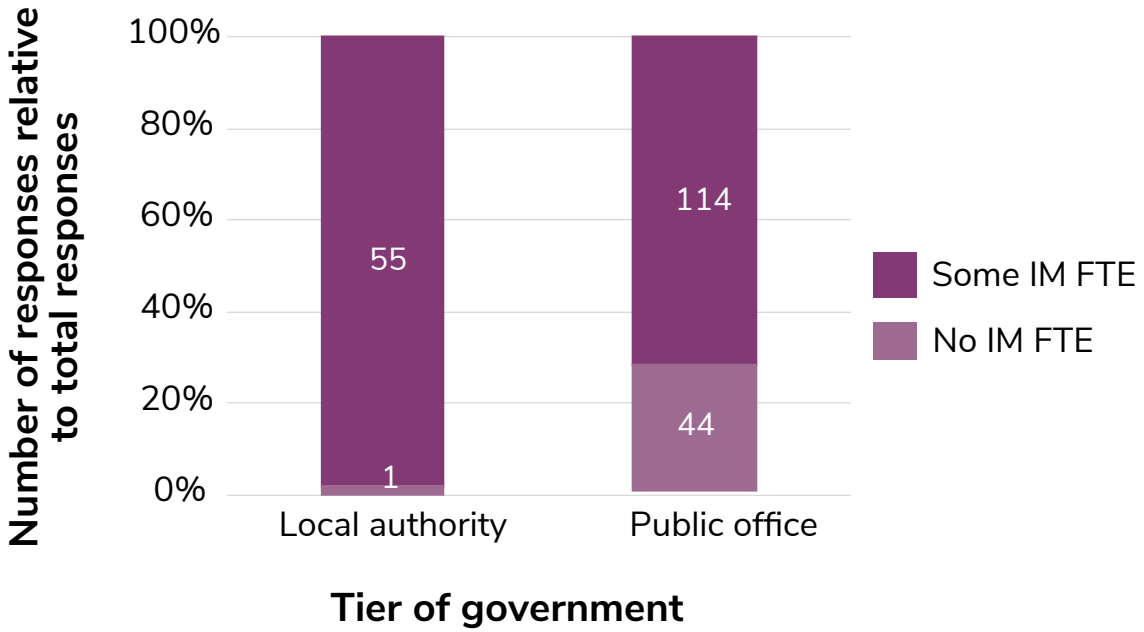
For the last two surveys we have asked respondents to tell us the exact number of IM staff employed by their organisation. This year, we can see the overall figure for the first time and how it has changed since the previous survey (Figure 4). Since the 2019/20 survey there has been an increase of 68 IM FTEs across public sector organisations. Proportionally, the percentage of organisations with 'some' IM staff versus none remains static at 79% for the third year running.

Figure 4: Change over time for Indicator 2[2]

2019/20 Survey	2020/21 Survey
579 IM FTEs employed by public sector organisations	646.9 IM FTEs employed by public sector organisations

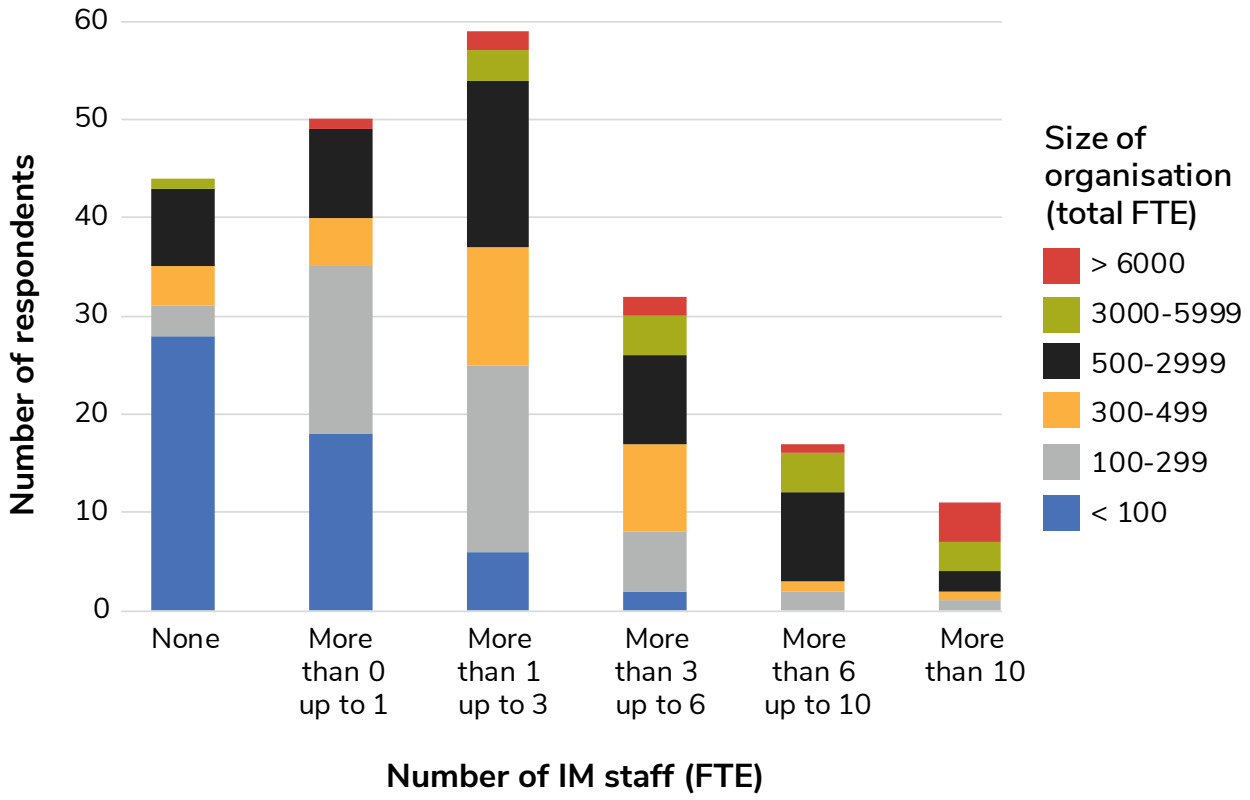
We also looked at levels of IM staffing compared to tier of government and total FTE employed. The proportion of local authorities with 'some' IM staff is much higher compared to public offices (Figure 5). Almost all local authorities have some IM FTE. For organisations with fewer than 100 total FTEs (shaded blue in Figure 6) it is common to have no IM staff.

Figure 5: IM FTE compared to tier of government



2 Data from 2018/19 is not plotted in Figure 4. The question was asked differently, with responding organisations selecting from a range rather than providing an exact number of FTEs.

Figure 6: IM FTE compared to total FTE



Developments and next steps

In 2019/20 we identified the following potential actions for influencing IM staffing levels:

- Engage with selected organisations that have no dedicated IM staff as a component of follow-up on their audit findings.
- Establish recommended staff metrics, which can assist Executive Sponsors with assessing appropriate staffing levels.

At the time of writing, 3 out of the 31 organisations audited in the previous year have been asked to address lack of IM staff in their post-audit action plans. Establishing recommendations for the appropriate number of IM staff and types or levels of IM capability and capacity is a medium-term goal and relies on growing and comparing our evidence base from both the annual survey and audits.

INDICATOR 3

An overall increase in organisations that have identified their high-value and/or high-risk information

What we asked and why it is important

We asked survey participants if they have identified their high-value and/or high-risk information (Q.19).

The Standard requires that: High-value and/or high-risk information areas of business, and the information and records needed to support them, must be identified and regularly reviewed (2.2).

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 operational failure, financial or material loss, breach of statutory obligations, or loss of public or Ministerial confidence.

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 the lives of New Zealanders. Those impacts can include physical, emotional and psychological harm. We have seen this through the work of the Abuse in Care Inquiry.

Identifying high-value/high-risk information is a foundation for other IM activities. It is a critical first step towards mitigating associated risks and extracting maximum value from information assets.

What we found and how it compares to previous surveys

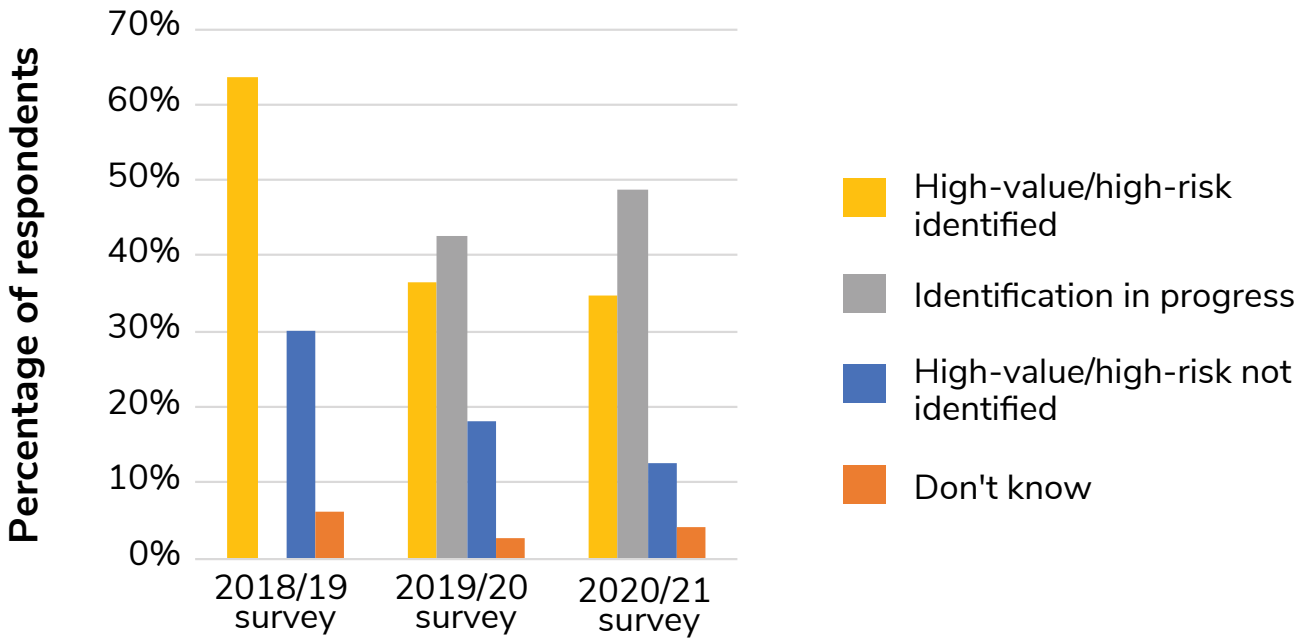
This year, the percentage of organisations that have identified their high-value and/or high-risk information is almost static at 35% compared with 36% in 2019/20 (Figures 7 and 8). The percentage that are 'in progress' is 49% compared to 43% in 2020. This means that most responding organisations either have done or are doing something.

In Figure 7, the change between 2018/19 and 2019/20 is represented as a dotted line to show that the decrease is influenced by modifications to the question. The 2018/19 survey did not offer an 'in progress' response option, while subsequent surveys did. This partly explains the large decrease in 'yes' responses between the first and second surveys.

Figure 7: Percentage change over time for Indicator 3

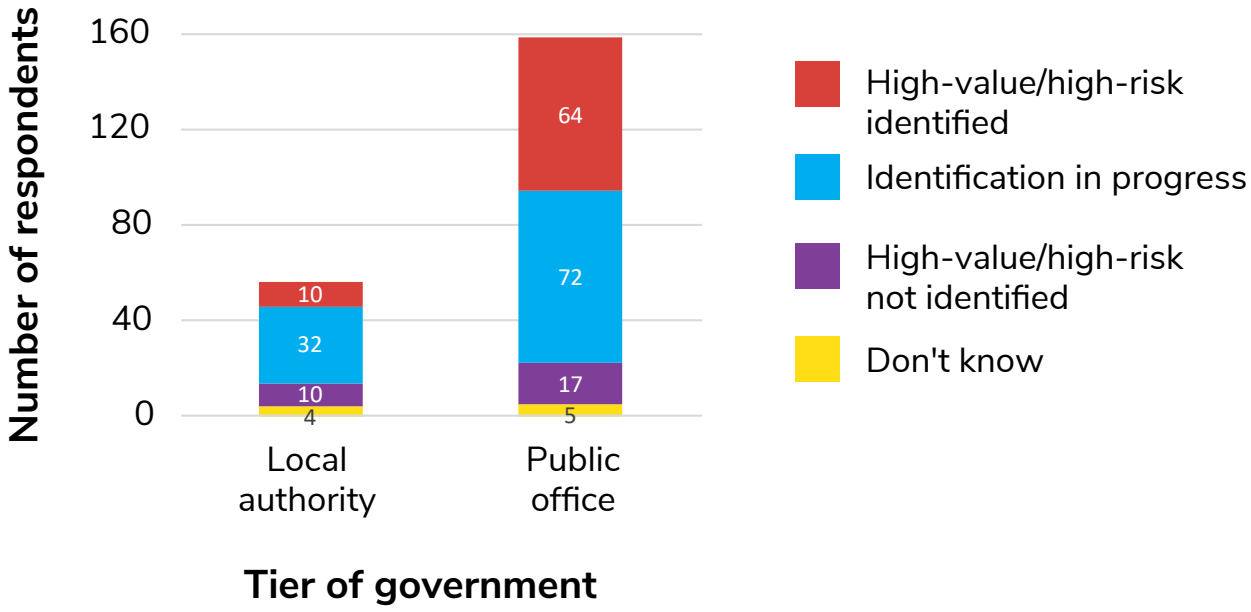
2018/19 Survey	2019/20 Survey	2020/21 Survey
64% of responding organisations have identified their high-value/high-risk information	36% of responding organisations have identified their high-value/high-risk information	35% of responding organisations have identified their high-value/high-risk information

Figure 8: 2018/19 to 2020/21 results for Indicator 3



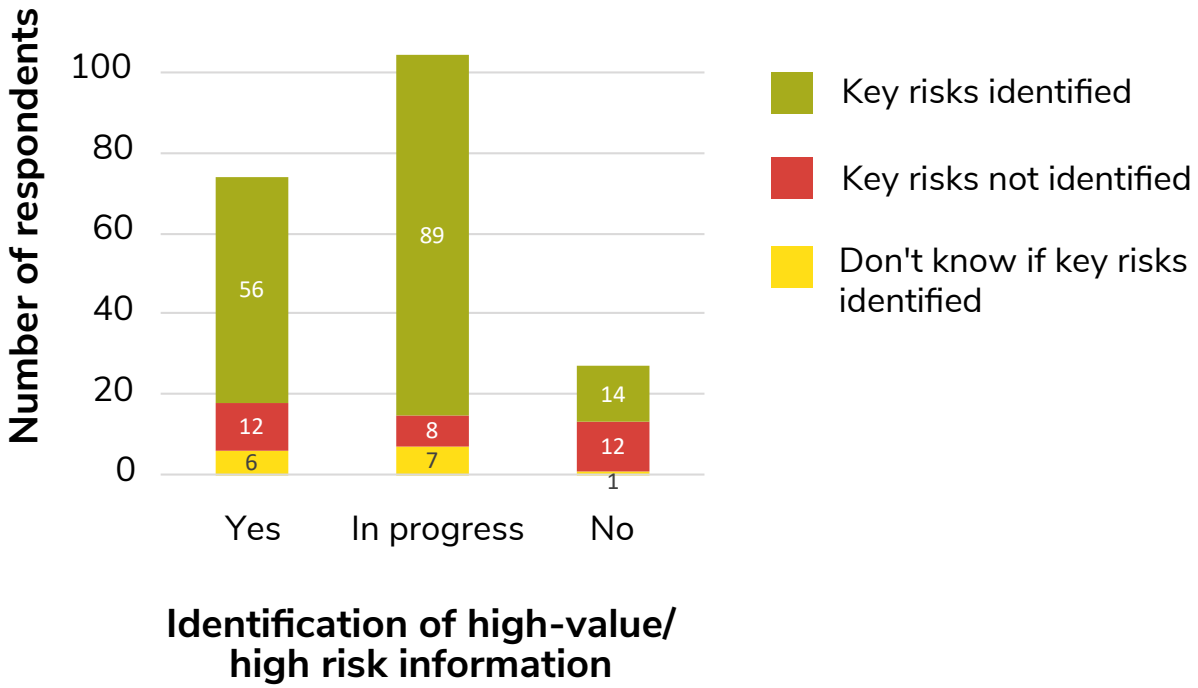
We looked at the data by tier of government and found that a higher proportion of public offices have identified, or are in the process of identifying, their high-value/high-risk information compared to local authorities (shaded blue in Figure 9).

Figure 9: Identification of high-value/high-risk information compared to tier of government



We also found that there was a statistically significant relationship between organisations identifying their high-value/high-risk information and identifying key risks associated with their information (Figure 10).

Figure 10: Identification of high-value/high-risk information compared to identification of key risks to information (Q.51)



Developments and next steps

In 2019/20 we identified the following potential actions for influencing change in organisations that have not identified their high-value and/or high-risk information:

- Engage with individual organisations that have not identified their high-value and/or high-risk information as a component of follow-up on their audit findings.

At the time of writing, 7 out of the 31 organisations audited in the previous year have been asked to include identification of high-value/high-risk information in their post-audit action plans.

INDICATOR 4

An overall increase in the number of organisations building IM requirements into new business systems

What we asked and why it is important

We asked survey participants whether they have built a process for managing information through its lifecycle into new business information systems (i.e. systems implemented in the last 12 months) (Q.25).

The Standard requires that: Information and records management must be design components of all systems and service environments where high risk/high value business is undertaken (2.3).

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.

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. For new systems, we expect these requirements to be built in from the start.

Business information systems are not limited to electronic documents and records management systems or enterprise content management systems. Information that has to be managed in accordance with our requirements is created and stored across a wide variety of business systems, including:

- finance and human resources
- line-of-business systems that support the organisation's unique functions
- systems that support collaboration between government organisations and/or external parties
- email and email archiving systems
- network drives.

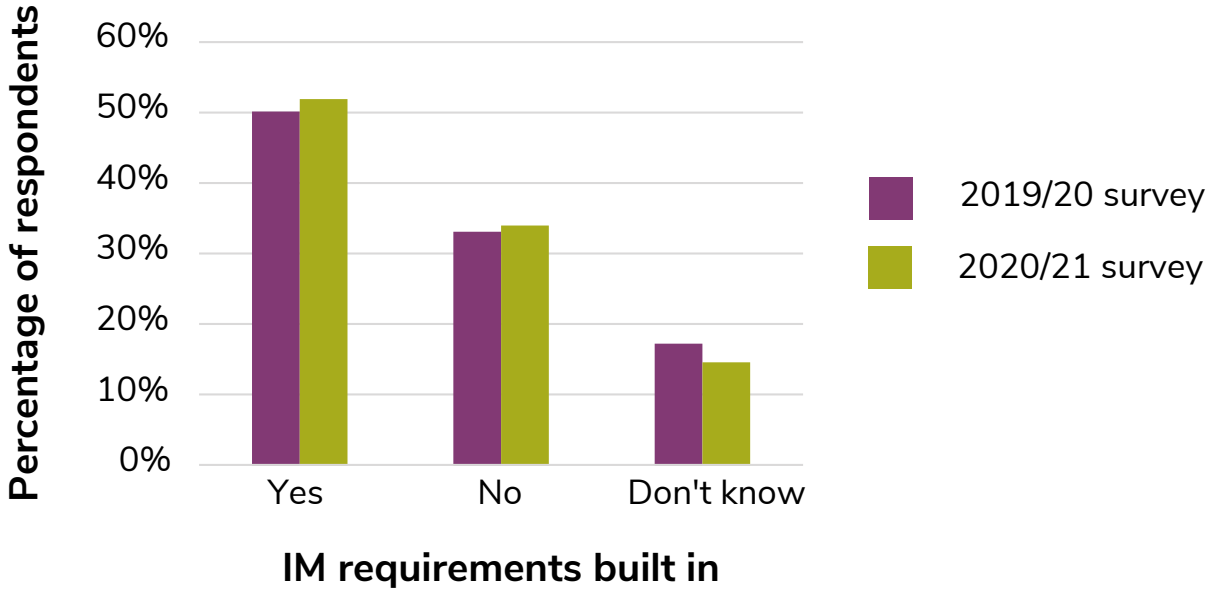
What we found and how it compares to previous surveys

This year, the percentage of organisations that have built IM requirements into business systems implemented in the last 12 months has gone up marginally to 52% from 50% in 2019/20 (Figures 11 and 12). Although the indicator has technically been met this year, we consider the proportion of 'yes' responses is still alarmingly low given that building in IM requirements has been mandatory for over a decade.

In Figure 11, the change between 2018/19 and 2019/20 is represented as a dotted line to show that the decrease is influenced by modifications to the question. The 2018/19 survey offered a 'partially' response option, which was selected by 62% of responding organisations. Subsequent surveys did not offer this option.

Figure 11: Percentage change over time for Indicator 4

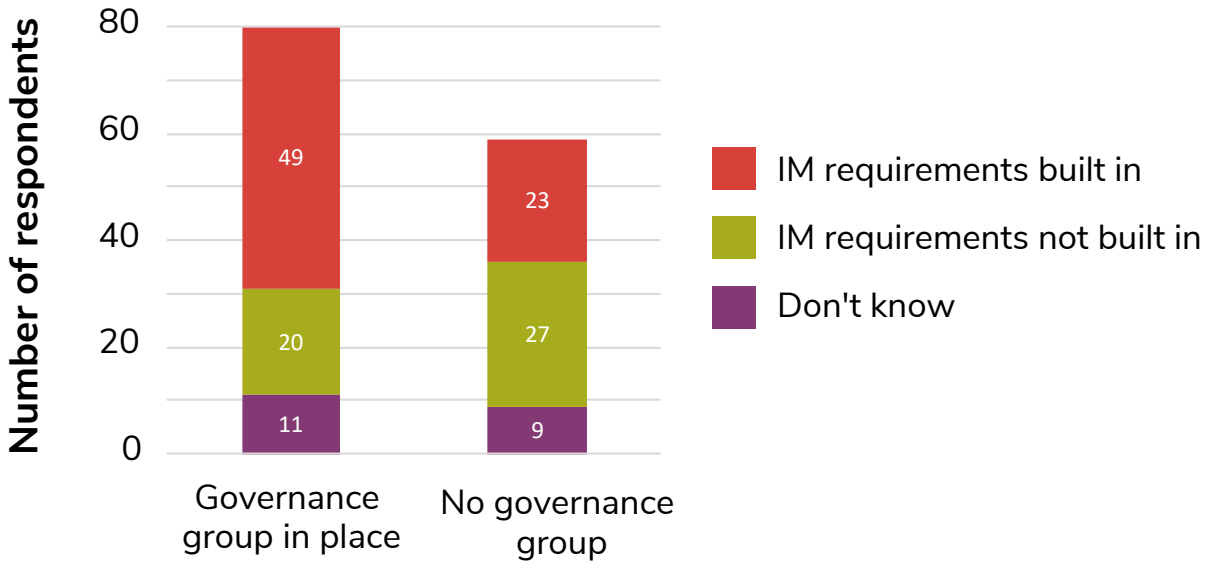
Figure 12: 2019/20 and 2020/21 results for Indicator 4[3]



For the second year running, we compared the Indicator 4 data against the presence of a formal governance group for IM and found a statistically significant relationship between the two (shaded red in Figure 13). This strengthens our finding that when a formal governance group is present there is a greater likelihood that the organisation will build IM requirements into new business systems. One of the purposes of a formal governance group is to ensure, at a strategic level, that IM requirements are considered when developing business systems.

3 Data from 2018/19 is not plotted in Figure 12. The question was asked differently, with a 'partially' option provided.

Figure 13: IM requirements built in compared to presence of formal governance group for IM



The top three challenges affecting organisations' ability to build in IM requirements have shifted slightly this year:

- Lack of awareness amongst internal staff (no change)
- Number of systems in use (no change)
- Age of business systems (new)

Developments and next steps

In 2019/20 we identified the following potential actions for helping organisations to overcome the challenges associated with building IM requirements into new business systems:

- Use our guidance, communications and interactions with Executive Sponsors to emphasise the importance of involving IM staff in new business system projects and of raising awareness amongst staff responsible for the system build.
- Engaging with the ICT community and industry on involving IM in new business system projects.

Since then, we have started planning for a series of recurring engagement sessions for Executive Sponsors, where building in IM requirements will be addressed. We have also presented to the Public Sector CIO Forum on the importance of IM by-design, with building in IM requirements at the forefront. We will continue to take up opportunities to reach the ICT community and industry in 2021.

INDICATOR 5

An overall increase in the number of organisations actively doing authorised destruction of information

What we asked and why it is important

We asked survey participants if they have carried out any authorised destruction of information in the past 12 months (Q.39 on physical information and Q.40 on digital information).

The Standard requires that: Information and records must be systematically disposed of when authorised and legally appropriate to do so (3.7).

Our general disposal authorities (GDAs) (GDA 6 and GDA 7) 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. GDAs are designed to make it easy to destroy information that has no long-term value.

This indicator focuses on destruction as one of the approved methods of disposal because it is an activity that all public sector organisations can be doing. Even if they do not have an organisation-specific disposal authority in place, organisations can still apply and action the GDAs.

Although destroying information may seem daunting or risky, it is an important component of effective IM. Typically, a large proportion of the information an organisation creates does not have long-term value for the organisation or New Zealanders, and a time will come when it is no longer required and can be safely destroyed.

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. 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.

On 28 March 2019, a moratorium was put in place on the disposal of any records relevant to the Royal Commission of Inquiry into Historical Abuse in State Care and in Faith-Based Institutions. This is likely to have had an impact on authorised destruction by some public offices during the timeframes of the survey. However, the impact on destruction practices was not measured as an explicit component of the survey.

What we found and how it compares to previous surveys

This year, the percentage of organisations that have reported doing destruction in the past 12 months has gone down slightly to 56% from 58% in 2019/20 (Figures 14 and 15). This means that we have seen a small decrease in destruction for two years running. Authorised destruction of digital information is much lower than physical information (Figure 16) which is consistent with our previous survey findings.

Figure 14: Percentage change over time for Indicator 5

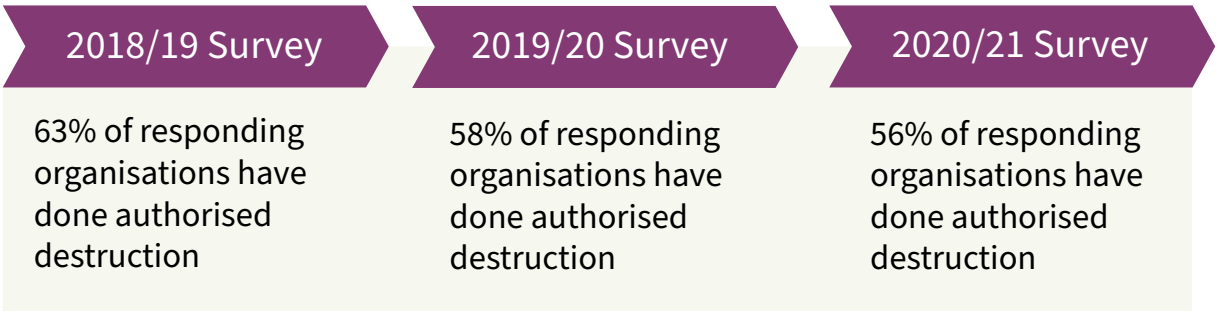


Figure 15: 2018/19 to 2020/21 results for Indicator 5

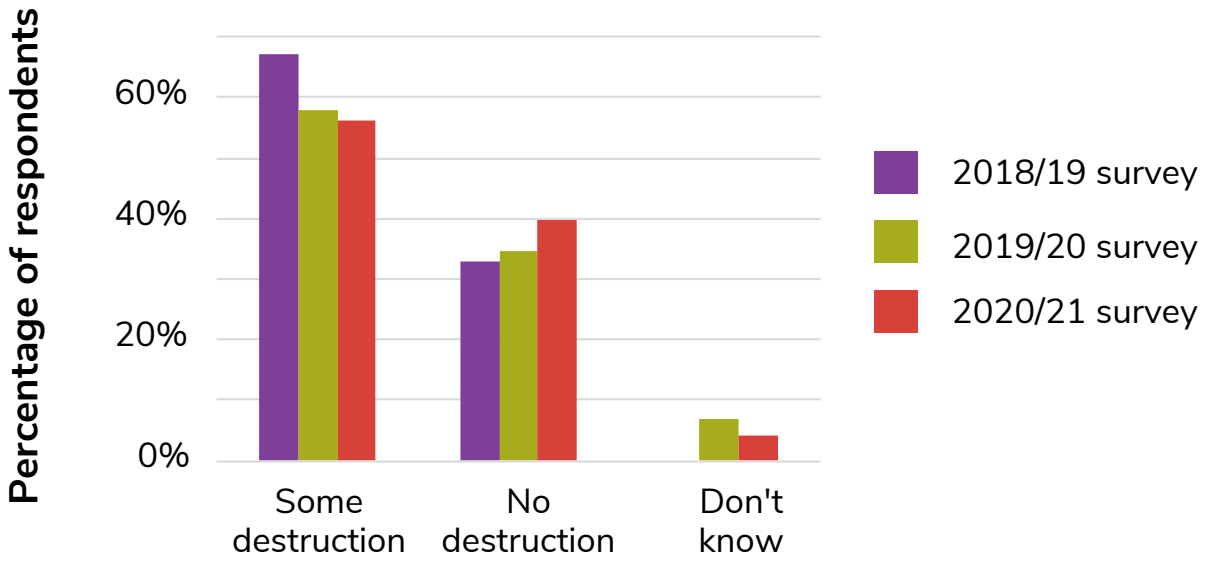
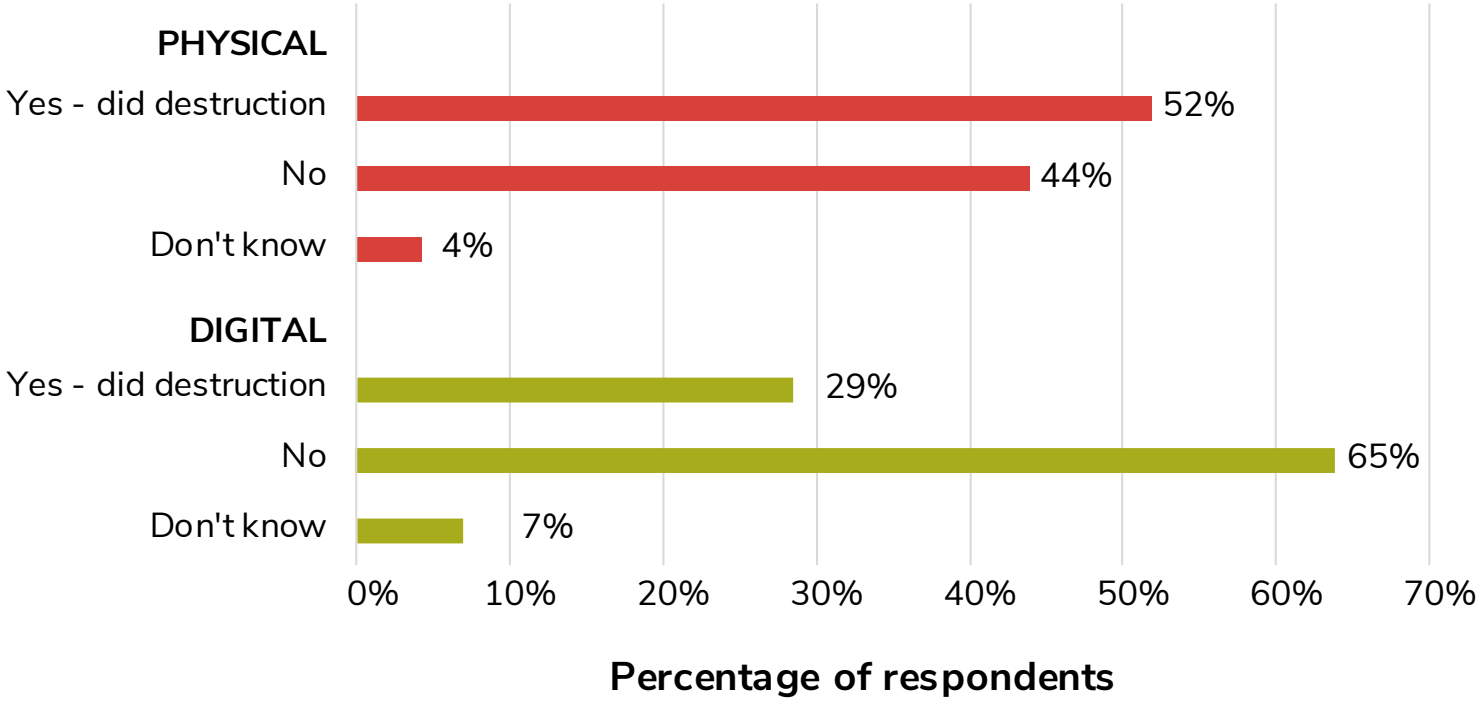


Figure 16: Authorised destruction by format in 2020/21



We looked at the data by tier of government and found that a higher proportion of public offices did authorised destruction compared to local authorities (Figure 17). We also looked at the data by IM FTE, which showed that proportionally the more IM FTE in place the greater the likelihood that destruction is happening (Figure 18).

Figure 17: Authorised destruction compared to tier of government

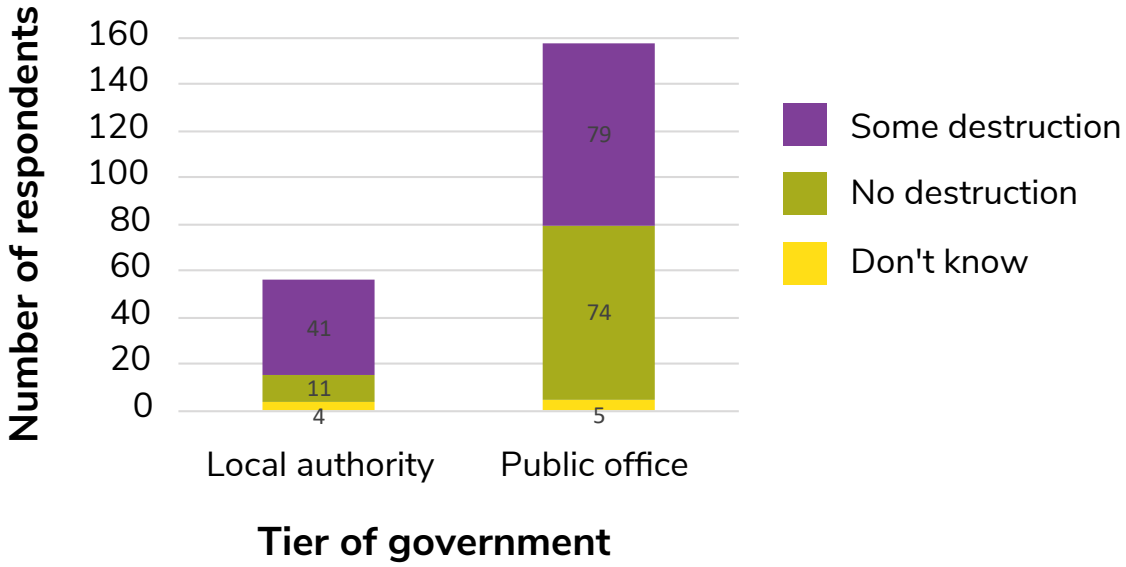
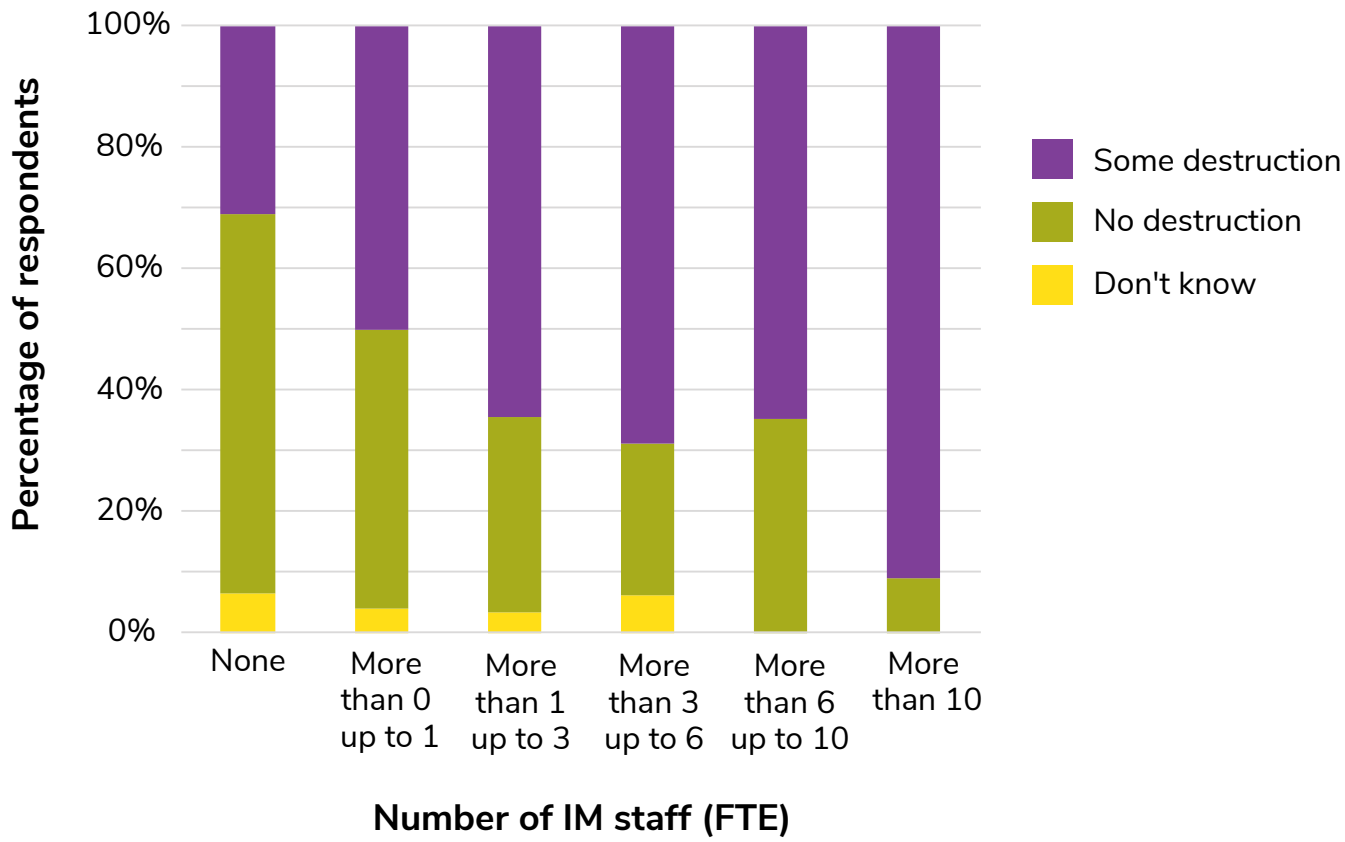


Figure 18: Authorised destruction compared to IM FTE



The top three challenges affecting organisations' ability to undertake regular, authorised destruction remain the same as the previous two surveys:

- Systems not set-up to automate regular, authorised deletion
- Not enough resources put towards sentencing activity
- Destruction not seen as a priority for staff

Developments and next steps

In 2019/20 we identified the following potential actions for helping organisations to overcome the challenges associated with implementing disposal:

- Make the importance of regular, authorised destruction more explicit in our guidance, communications and interactions with Executive Sponsors. This could include addressing those challenges that a formal governance group has influence over, such as resourcing, prioritisation, and design of new business systems.
- Engage with the ICT community on system functionality that supports disposal.
- Engage with organisations that are subject to the disposal moratorium and reported undertaking authorised destruction in the past 12 months. Seek confirmation that the information destroyed is outside the scope of the moratorium.

Since then, we have started revising our guidance and planning for a series of recurring engagement sessions for Executive Sponsors, where regular, authorised destruction will be addressed. We are also scoping a large programme of work to address more effective regulation and implementation of disposal. In May 2021, we issued a moratorium reminder notice to all Executive Sponsors and have had ad-hoc engagements with organisations on safely disposing of information while the Royal Commission of Inquiry into Abuse in State Care runs its course.

Reflections on the 2010 Government Recordkeeping Survey

From 2005 to 2010, we conducted annual surveys of public offices and local authorities, with survey questions centred on the requirements in the PRA. For the most part the results are not directly comparable to our more recent surveys, but there are a few insights that are relevant to look back on.

In 2010, we found that 68% of public offices and 75% of local authorities had specialised staff responsible for records management. In comparison, in the 2020/21 survey we found that 72% of responding public offices and 98% of responding local authorities have 'some' IM staff.

Another area available for comparison is disposal, although in 2010 our survey questions did not distinguish between different types of disposal action (i.e. destruction or transfer). In 2010, we found that 47% of public offices and 60% of local authorities had disposed of records in the last 12 months. In comparison, in the 2020/21 survey we found that 50% of public offices and 73% of local authorities have done some destruction.

While the comparisons with the 2010 survey are indirect, they suggest that collective IM maturity has not uplifted significantly. There have been many challenges over the past decade for both public sector organisations and Archives New Zealand. These include rapid advances in technology, the constant need to advocate for investment in IM, structural changes and earthquake recovery. Some challenges will be addressed by new archival storage capacity and management systems (for Archives) and technological solutions that automate IM at scale (for the sector). However, there is clearly much more effort required to increase and sustain IM performance.

Governance, capability and self-monitoring

This section covers the people component of IM:

- The people within an organisation who set the direction for IM or have IM responsibilities.
- The rights of people outside the organisations, 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.

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

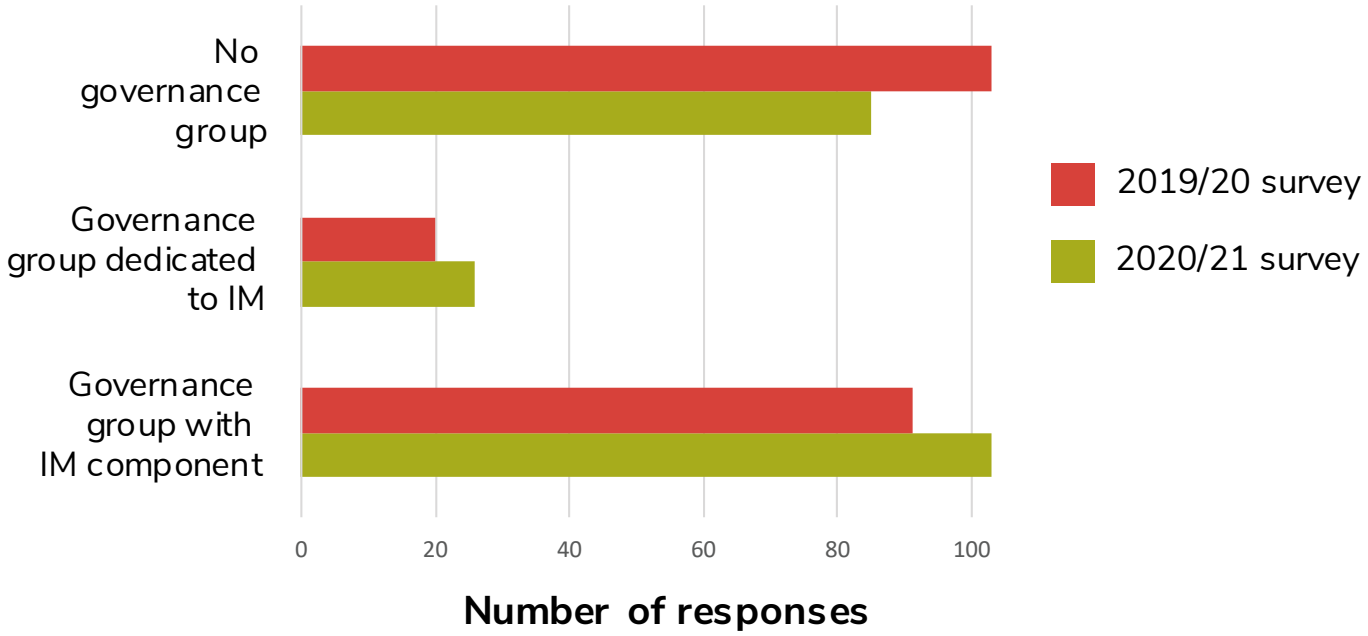
We asked survey participants if:

- They have a formal governance group which is either dedicated to IM or has IM oversight as part of its mandate (Q.5).
- That group meets at least twice a year (Q.6).
- The Executive Sponsor is part of that group (Q.7).

Findings

Figure 1 shows the frequency and type of governance groups in place. 60 percent of respondents have a formal governance group in place, compared to 52% in 2019/20. Most of the respondents who do have a formal governance group in place said that the group meets at least twice a year (93%) and that their Executive Sponsor is part of the group (91%).

Figure 19: Frequency and type of IM governance groups



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.9).
- Whether the organisation has criteria or methodologies for assessing this (Q.10).
- What the organisation has done to improve use of the information identified (Q.11).

Findings

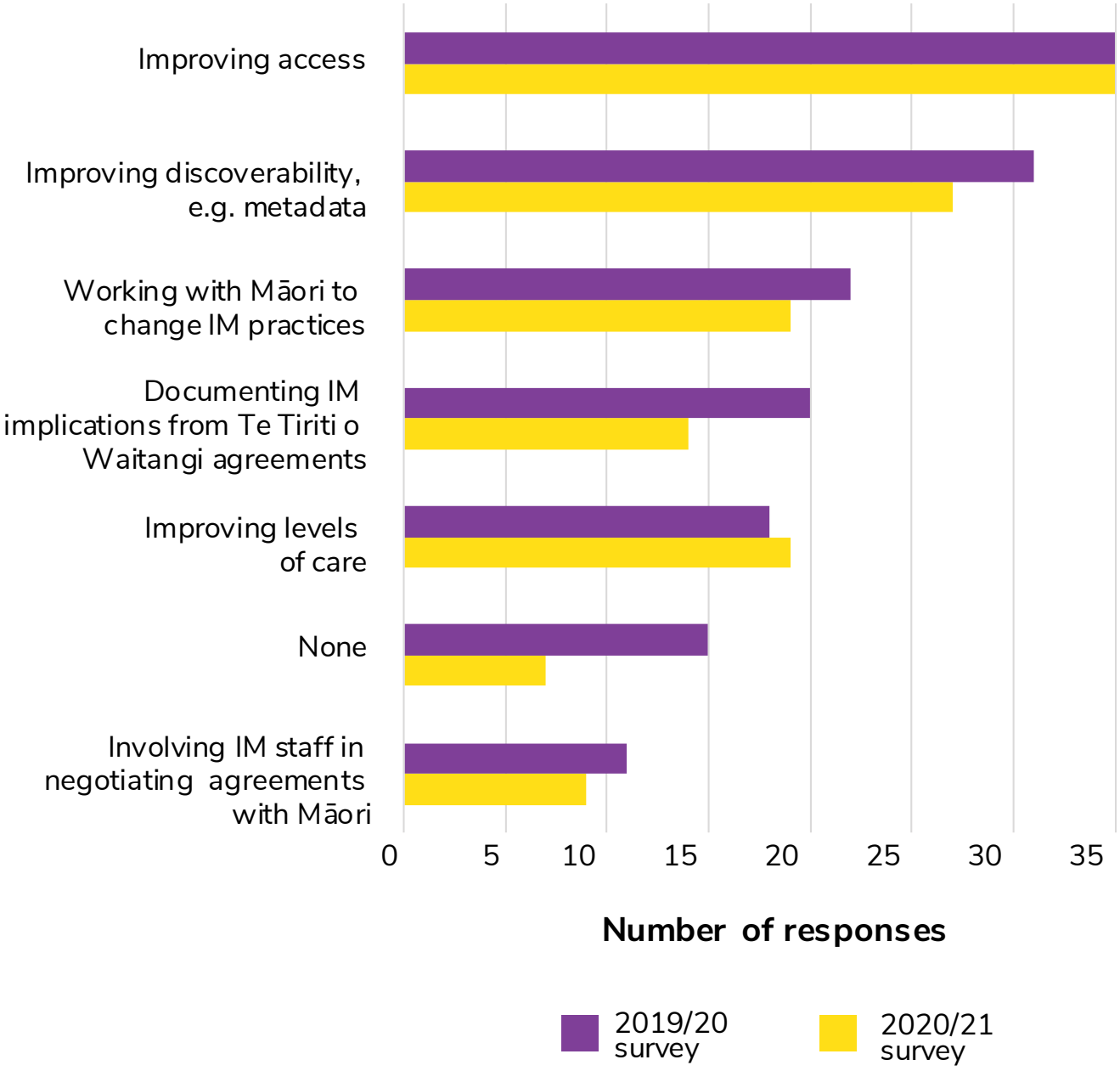
Thirty-five percent of respondents said that they have identified information that is of importance to Māori, compare to 39% in 2019/20. Of those, 30 respondents (41%) said that they had criteria or methodologies for assessing this. These included:

- Reviewing, classifying and recording relevant information, including use of Information Asset Registers.
- Identifying key external stakeholders and establishing relationships and operational agreements (e.g. MoUs) with these groups to assist with this task.
- Dedicated staff/teams or internal Advisory Groups to help identify and manage this information.

Respondents who have identified information of importance to Māori told us more about what activities they are doing to improve usage (Figure 20). 'Improving access' is once again the most common activity. Other activities mentioned in the comments in addition to those listed in Figure 2, include:

- Establishing/improving Māori data governance frameworks.
- Upskilling staff (e.g. in mātauranga Māori) through recruitment and/or training.
- Having entities in partnership with Māori and local iwi.
- Having specialised staff, teams and/or internal Advisory Groups.

Figure 20: 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.12 and Q.13).
- What actions were taken as a result of self-monitoring (Q.14).

Findings

Seventy-six percent of respondents said that they have done self-monitoring in the last 12 months, compared to 70% in 2019/20. 59 percent have monitored against our requirements, while 54% have monitored against their own IM policy. A review of processes is once again the most common activity (Figure 21). This year we added a new response option for self-monitoring methods ('maturity assessment') based on our analysis of qualitative responses in 2019/20. 38 percent of respondents who have done self-monitoring said that they did a maturity assessment. Other activities mentioned in the comments in addition to those listed in Figure 21, include:

- Regular monitoring and reporting to leadership or governance groups.
- Establishment, review and/or update of policy and strategies around self-monitoring.
- Annual compliance surveys.

The majority of the 162 respondents who have done self-monitoring in the last 12 months (56%) are focused on developing action plans (Figure 22). Once again, a smaller proportion of respondents (36%) are progressing towards implementing action plans.

Figure 21: Methods used to self-monitor

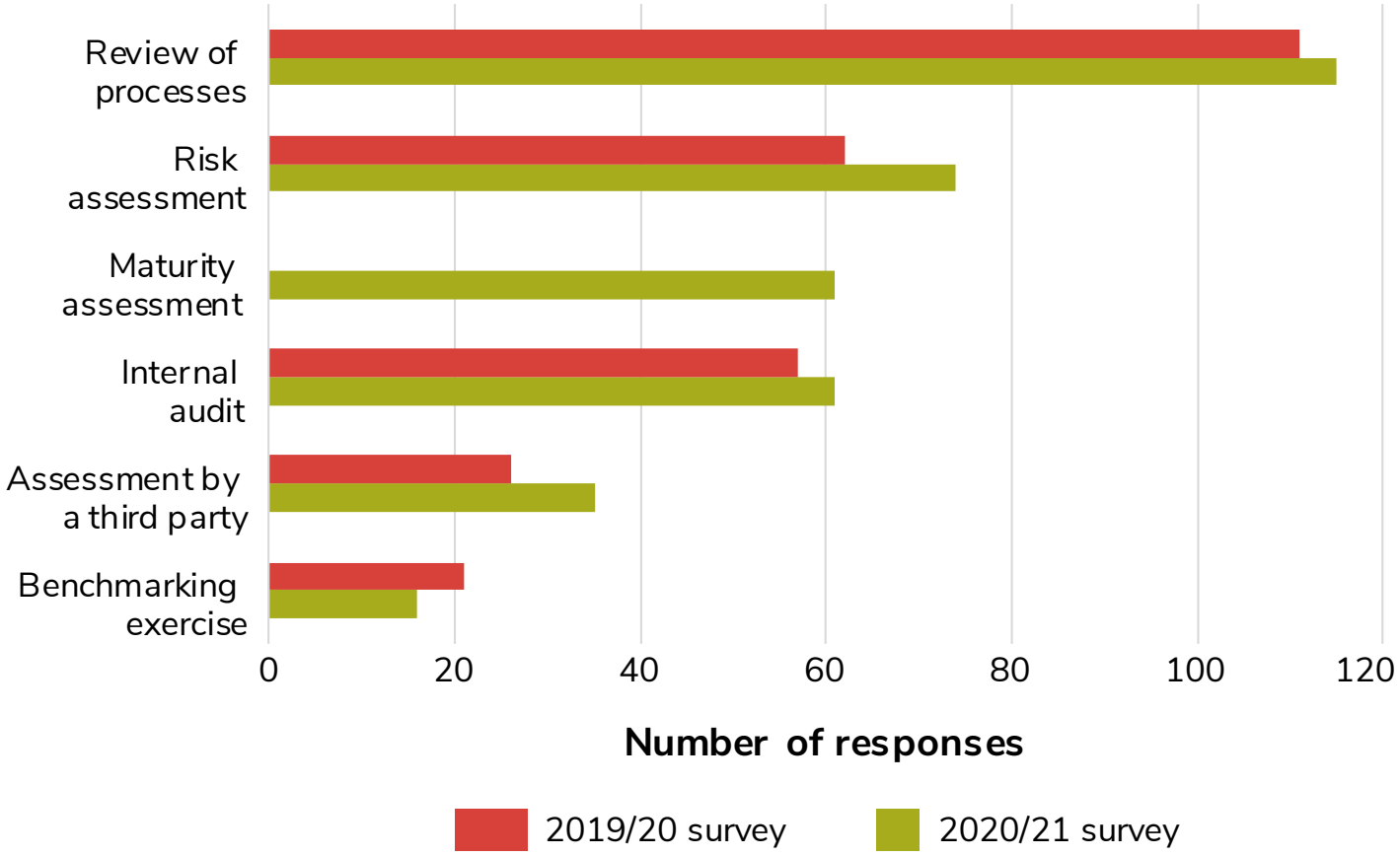
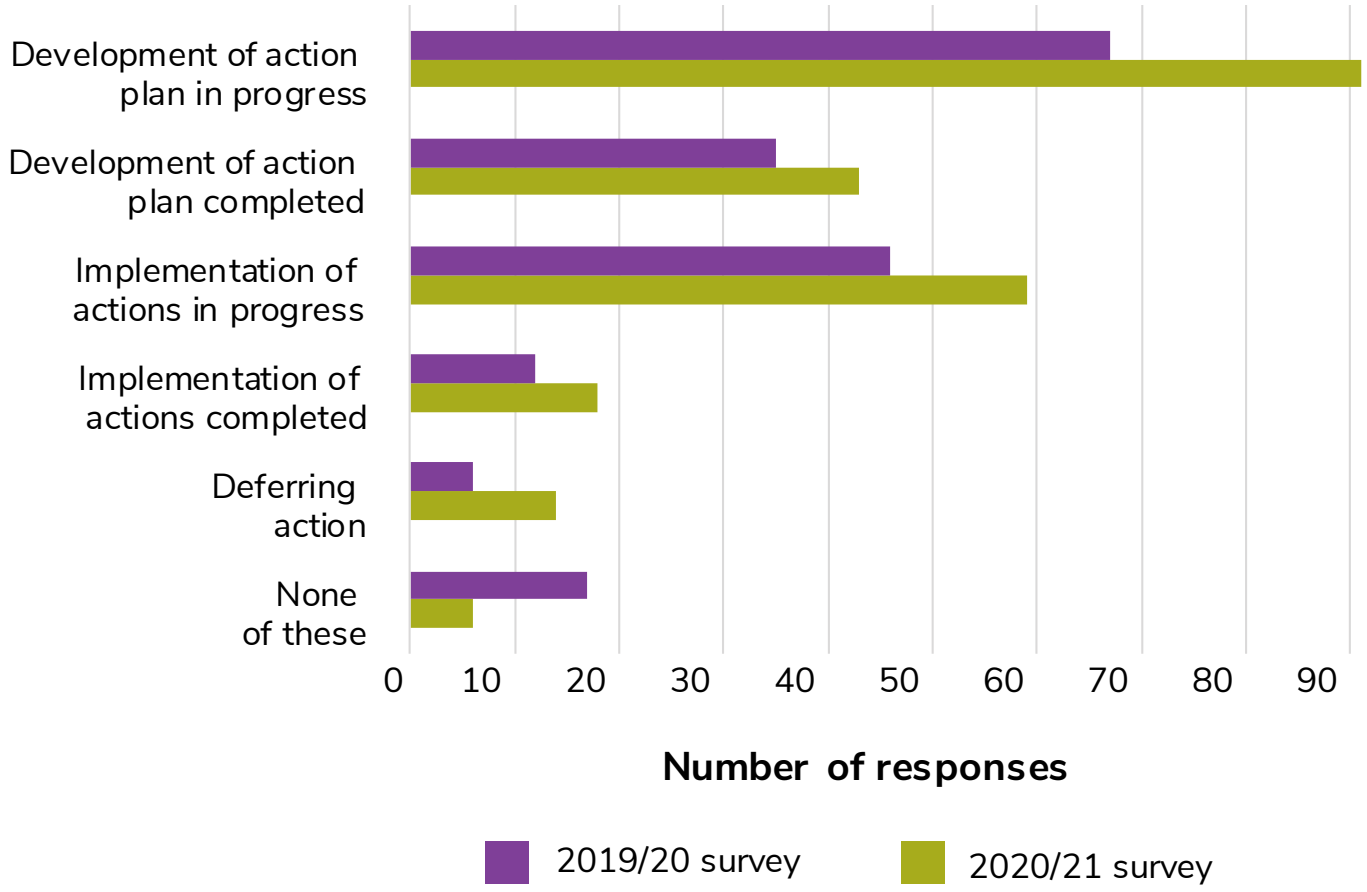


Figure 22: Steps taken as a result of self-monitoring



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.15).
- What professional development activities those staff have done in the last 12 months (Q.16).
- If and how the organisation informs staff, contractors and consultants about their IM responsibilities (Q.17 and Q.18).

Findings

Seventy-nine percent of respondents have some dedicated, specialised IM resources and the mean number of IM staff is 3.0, compared to 2.7[4] in 2019/20. Figure 23 shows the level of IM-focused staff split by organisation size (as measured by the total FTE). For organisations with fewer than 100 total FTEs (shaded red) it is common to have no IM staff.

82 percent of respondents said that their IM staff had participated in professional development activities, compared to 59% in 2019/20. Training courses and conference attendance were once again the most common activities (Figure 24).

While most respondents indicated that they inform staff at all levels of their IM responsibilities (95%) the rate is lower for contractors (64%) and consultants (48%). However, the percentage of respondents informing contractors has increased by 10% on last year's survey, which is an encouraging trend given that we highlighted this as an area for improvement in 2019/20.

Once again, a high proportion of respondents said that they use induction training to communicate responsibilities (82%) while around half use refresher training, contracts and codes of conduct (Figure 25). Consistent with 2019/20, job descriptions and performance development plans are used far less frequently. Other activities mentioned in the comments in addition to those listed in Figure 25, include:

- Documented policies and processes available as physical copies or online.
- Internal communication via intranet or email, e.g. posts, newsletters, blogs, videos.
- One-to-one meetings with IM staff to provide advice and support.
- Briefings at group meetings.

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

Figure 23: Number of IM FTEs compared with organisation size

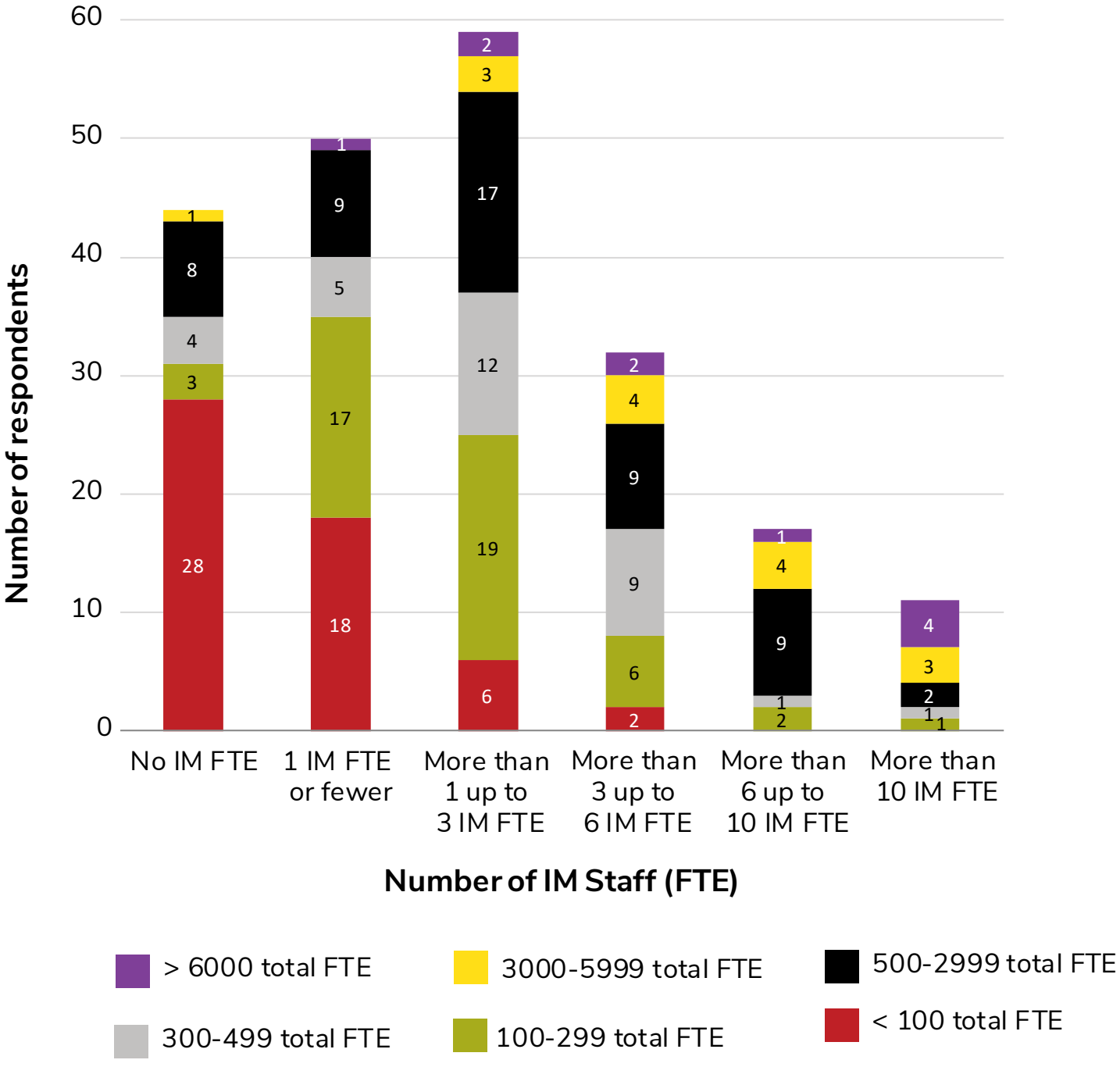


Figure 24: Professional development activities for IM staff

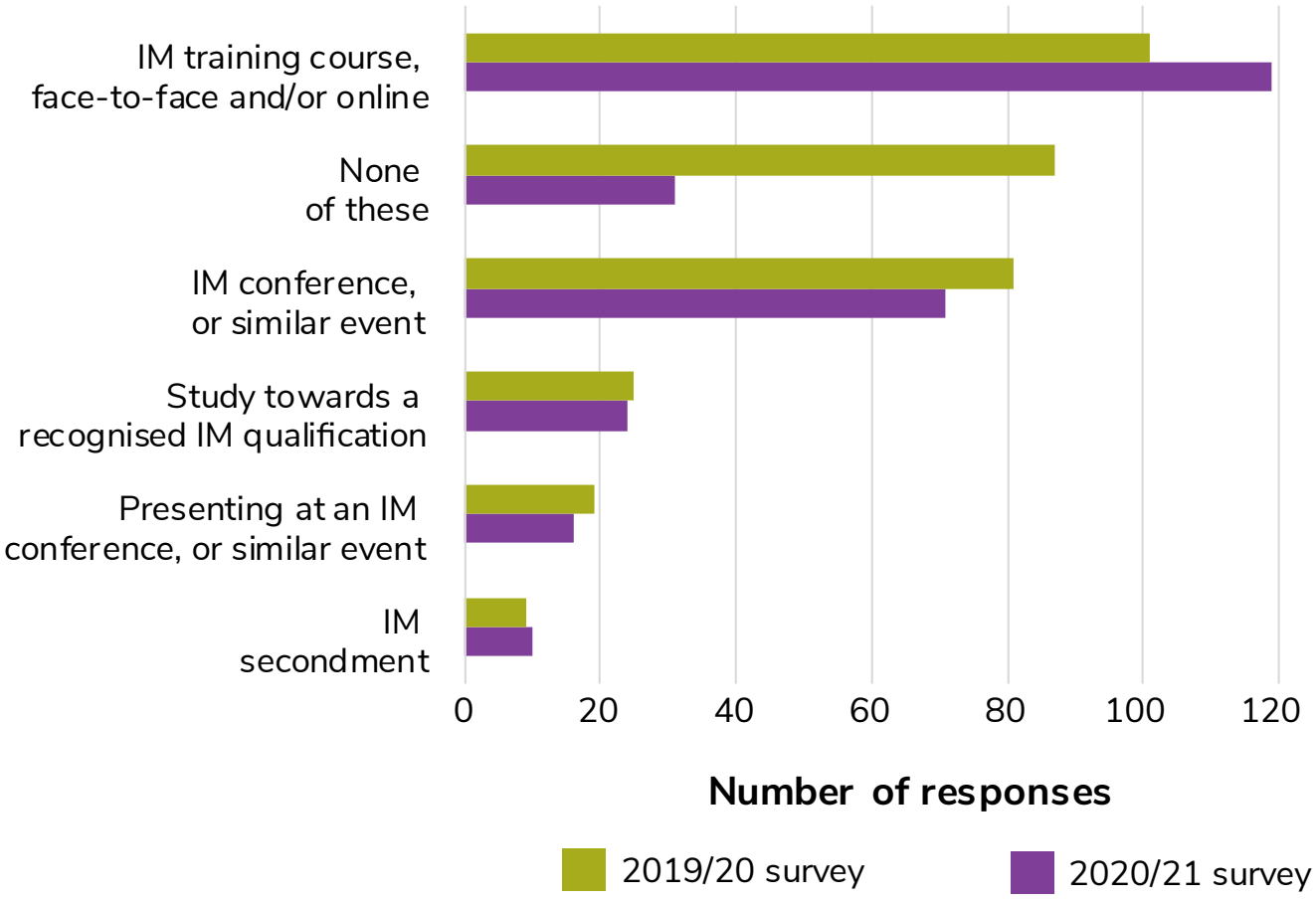
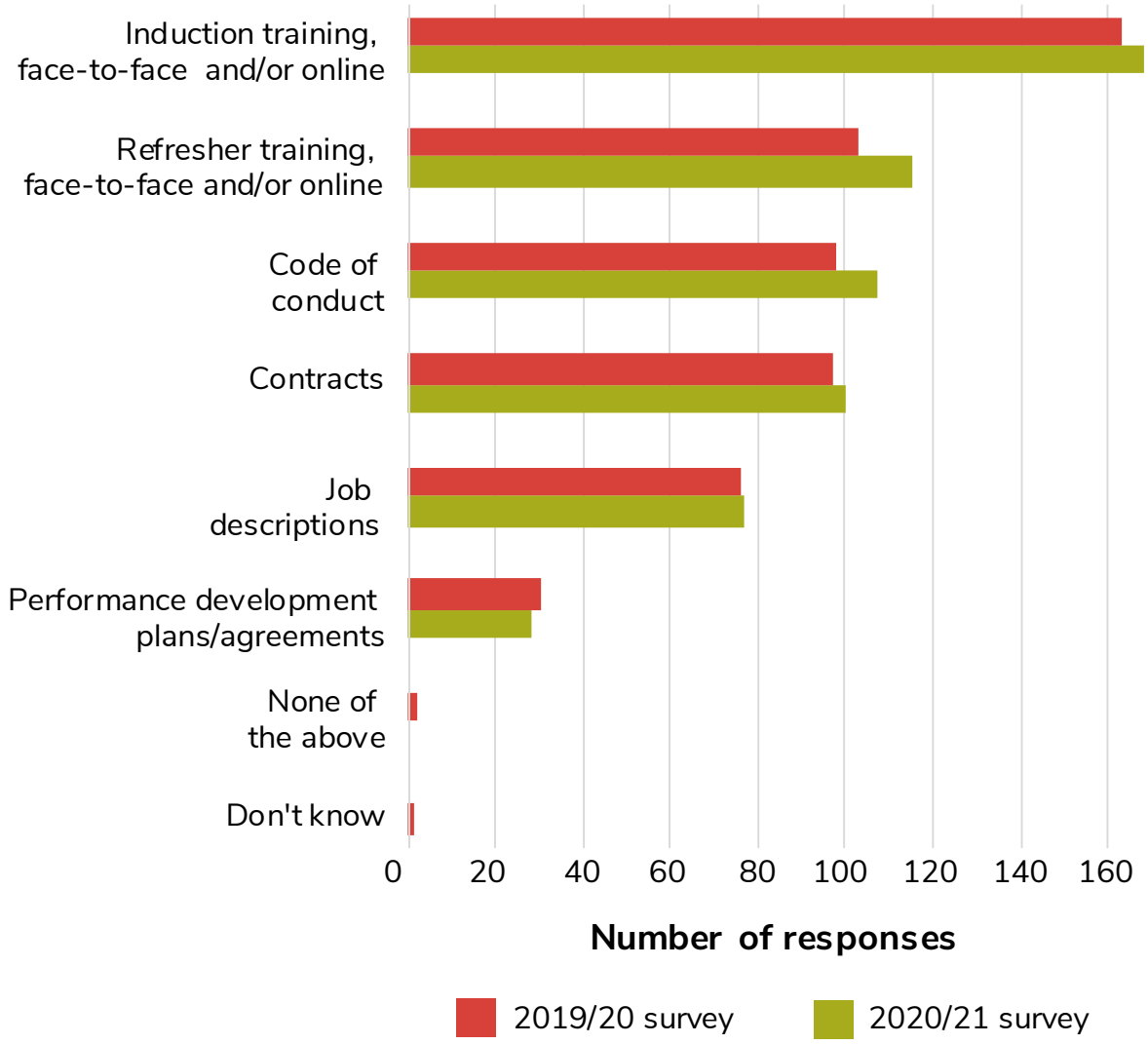


Figure 25: How organisations inform staff, contractors and consultants about their IM responsibilities



Key findings

There has been increase in the establishment of formal governance groups relating to IM in organisations compared with last year's survey.

Collaboration with iwi and Māori entities is paramount in developing Mātauranga Māori strategies and policies for IM. This has been demonstrated externally through consulting and working with Māori and iwi. While internally being incorporated into recruitment and induction staff training, there is also development of Māori advisory positions within organisations. While progress has been made, improving access and discoverability remain the most common activities within organisations. We encourage all public sector organisations to consider adding metadata fields or tagging capabilities for Māori metadata and/or metadata for iwi/Māori concepts. This is particularly important when organisations are implementing new enterprise content management systems, line-of-business systems, or collecting information on land, people and natural resources.

Self-monitoring and internal information capability actions have increased. An emphasis on internal influence is shown within organisations through annual audits whether they are informal internal audits or consultation with Archives New Zealand Information Management Maturity Assessment.

The reported rates at which respondents communicate IM responsibilities for contractors is once again lower than all staff. 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.

For more findings and recommendations concerning governance groups and numbers of IM staff, see the *Chief Archivist's Annual Report on the State of Government Recordkeeping 2020/21*.

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.19).
- What actions the organisation has taken to actively manage that information in the last 12 months (Q.20).
- If the organisation has an information asset register (IAR) or similar tool, and if that tool is current and in use (Q.21 and Q.22).
- If organisations that do not have an IAR or similar tool are planning to develop one (Q.23).

Findings

Thirty-five percent of respondents have identified their high-value/high-risk information, while 49% said that work is 'in progress'. This compares to 36% 'identified' and 43% 'in progress' in 2019/20.

Thirty-four percent of respondents said that they do not have an IAR, while a combined 55% responded 'yes' or 'in development', and 12% responded 'work started but deferred.' Of the 49 respondents who said they have an IAR or similar tool, 24 said that it was up-to-date and 36 said it was being used.

For managing high-value/high-risk information, we asked about a small set of common activities (Figure 26). Testing business continuity plans remains the top activity. This year we added two new response options based on our analysis of qualitative responses in 2019/20. They were 'developing information architecture and/or search tools' and 'implementing back up capability.'

Figure 26: 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.24).
- If a process for managing information through its lifecycle has been built into those systems (Q.25.)
- What challenges affect the organisation's ability to integrate IM requirements into new or upgraded systems (Q.26).
- If the organisation's current systems meet our minimum requirements for metadata (Q.27).

Findings

Sixty-five percent of respondents have implemented a new business information system (or systems) in the last 12 months, compared to 68% in 2019/20. Of those, just over half (52%) have built in a process for managing information through its lifecycle, while the remainder have either not built in requirements or 'don't know' whether they have.

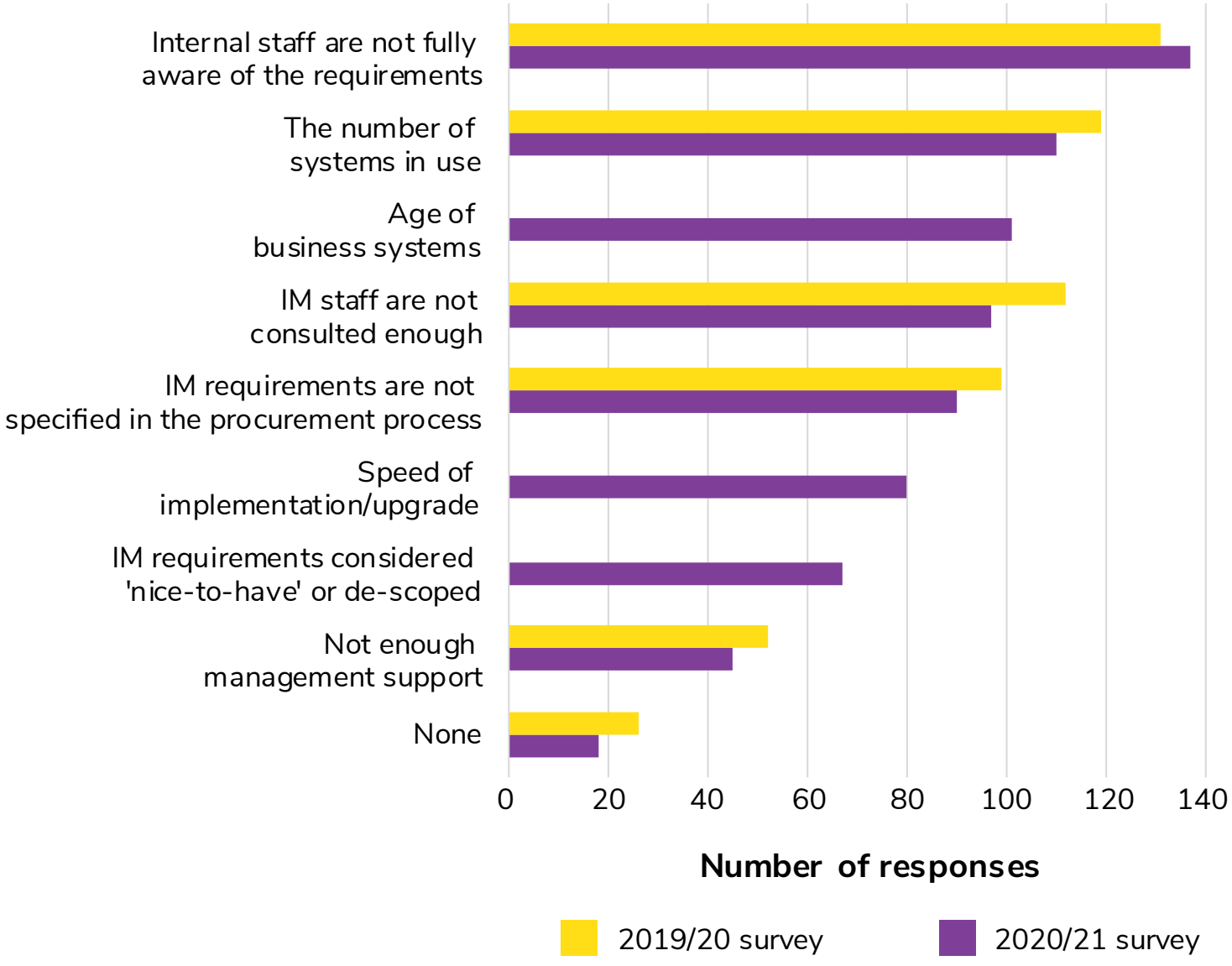
The most common challenges affecting respondents' ability to build in IM requirements are lack of awareness of the requirements amongst internal staff, the number of systems in use and the age of business systems (Figure 27). The latter was a new response option in 2020/21, alongside 'speed of implementation/upgrade' and 'IM requirements considered 'nice-to-have' or de-scoped'. Other challenges mentioned in the comments in addition to those listed in Figure 27, include:

- Lack of resourcing and capability.
- Complexity of system integration.

- Te Pukenga -The Reform of Vocational Education (ROVE).
- Impractical requirements.

Sixty-nine percent of respondents said that 'some' of their business systems meet our minimum requirements for metadata, compared to 71% in 2019/20. Far fewer said that all systems meet the requirements (16%), while a combined 15% responded 'no systems do' or 'don't know'.

Figure 27: Challenges for building IM requirements into new business information systems



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 can 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.28).
- What actions the organisation has taken in the last 12 months to make sure that information remains usable (Q.29).
- If the organisation has any digital information that is inaccessible (Q.30).
- Why that information is inaccessible (Q.31).

Findings

Eighty-eight percent of respondents (189 organisations) told us that they have digital information with long-term value. Of those, the majority (65%) have identified information that needs to be retained long-term (Figure 28).

A combined 64% of respondents 'definitely have' or 'possibly have' digital information that is inaccessible, compared to 53% in 2019/20 (Figure 29). The most common reasons for inaccessibility are information being stored in personal systems, inadequate metadata and obsolete file formats (Figure 30). These were also the most common reasons in 2019/20.Other reasons mentioned in the comments in addition to those listed in Figure 30, include:

- Corrupted, encrypted or password protected files.
- Information stored in non-corporate tools/Shadow IT such as Google Drive.
- Staff with required knowledge have left the organisation.
- Systems that are in remote locations with reduced connectivity.

Figure 28: Actions to maintain usability in the last 12 months

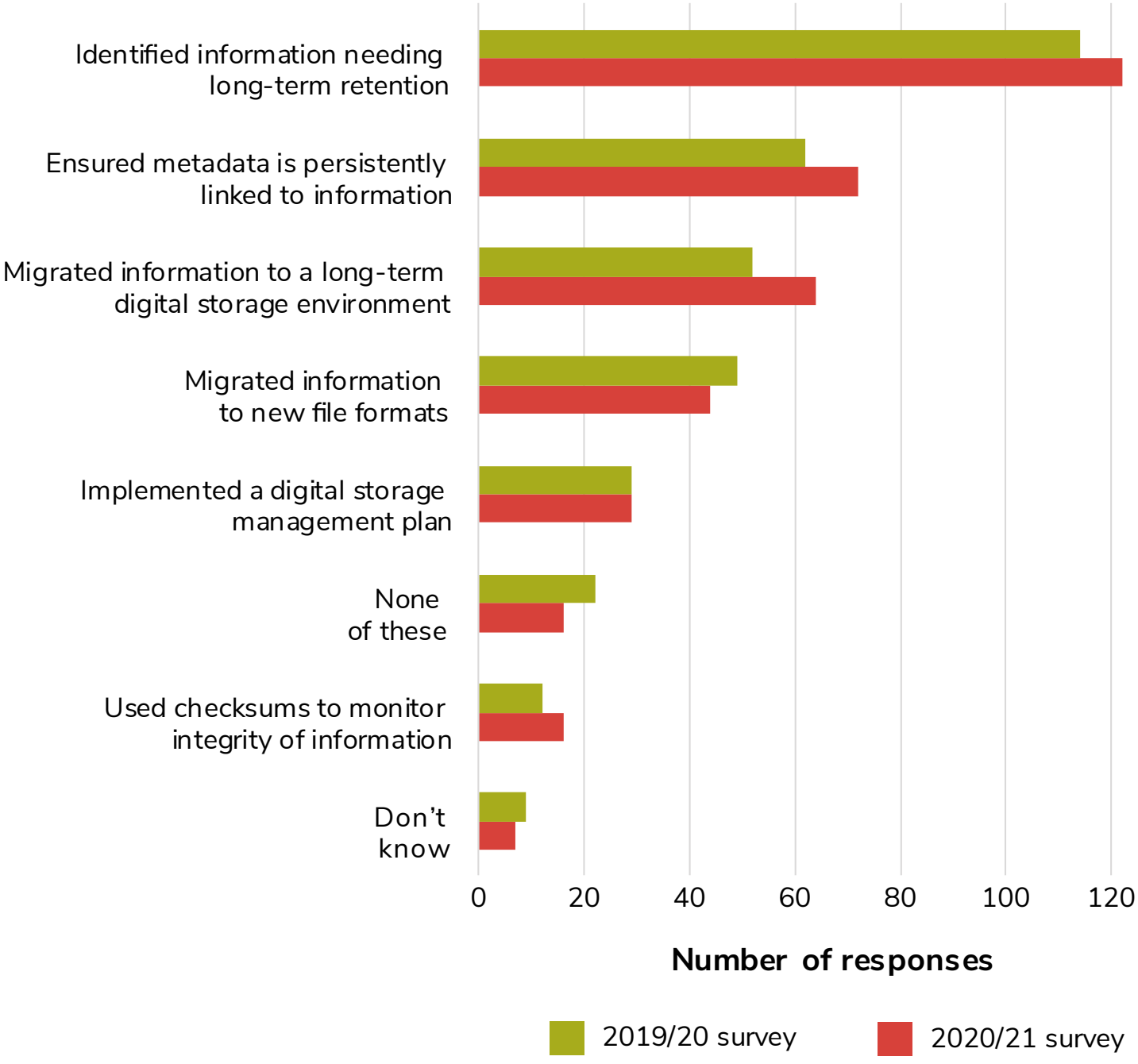


Figure 29: Do organisations hold any digital information that is inaccessible?

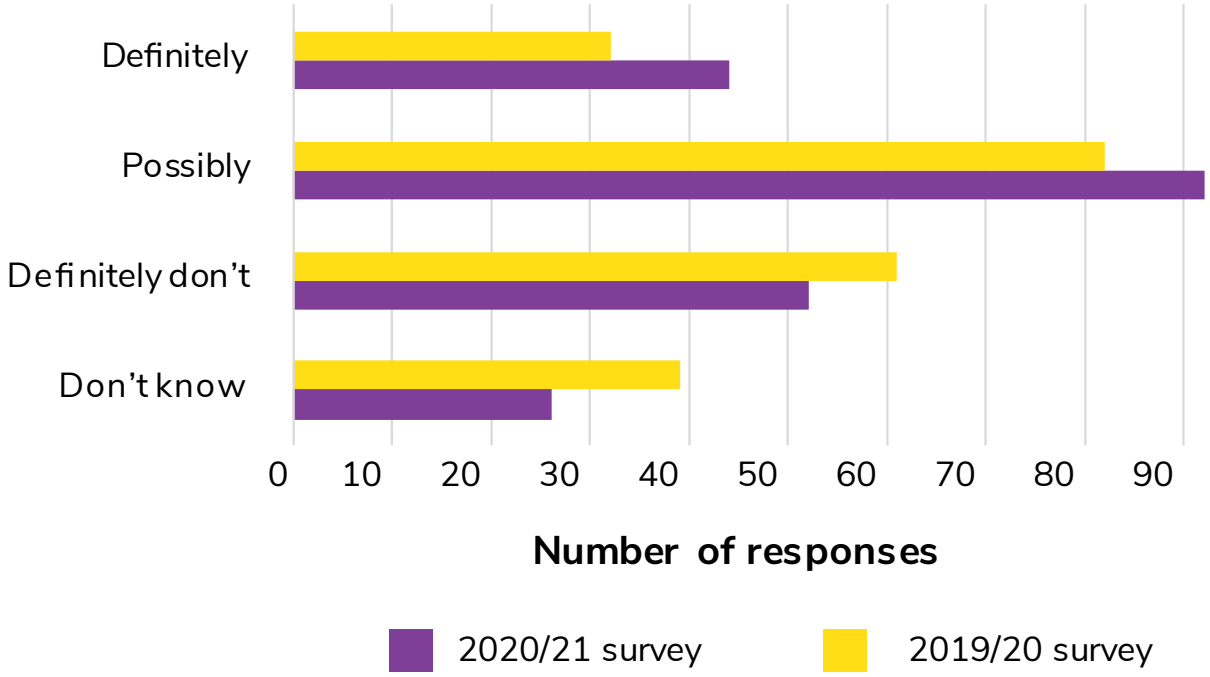
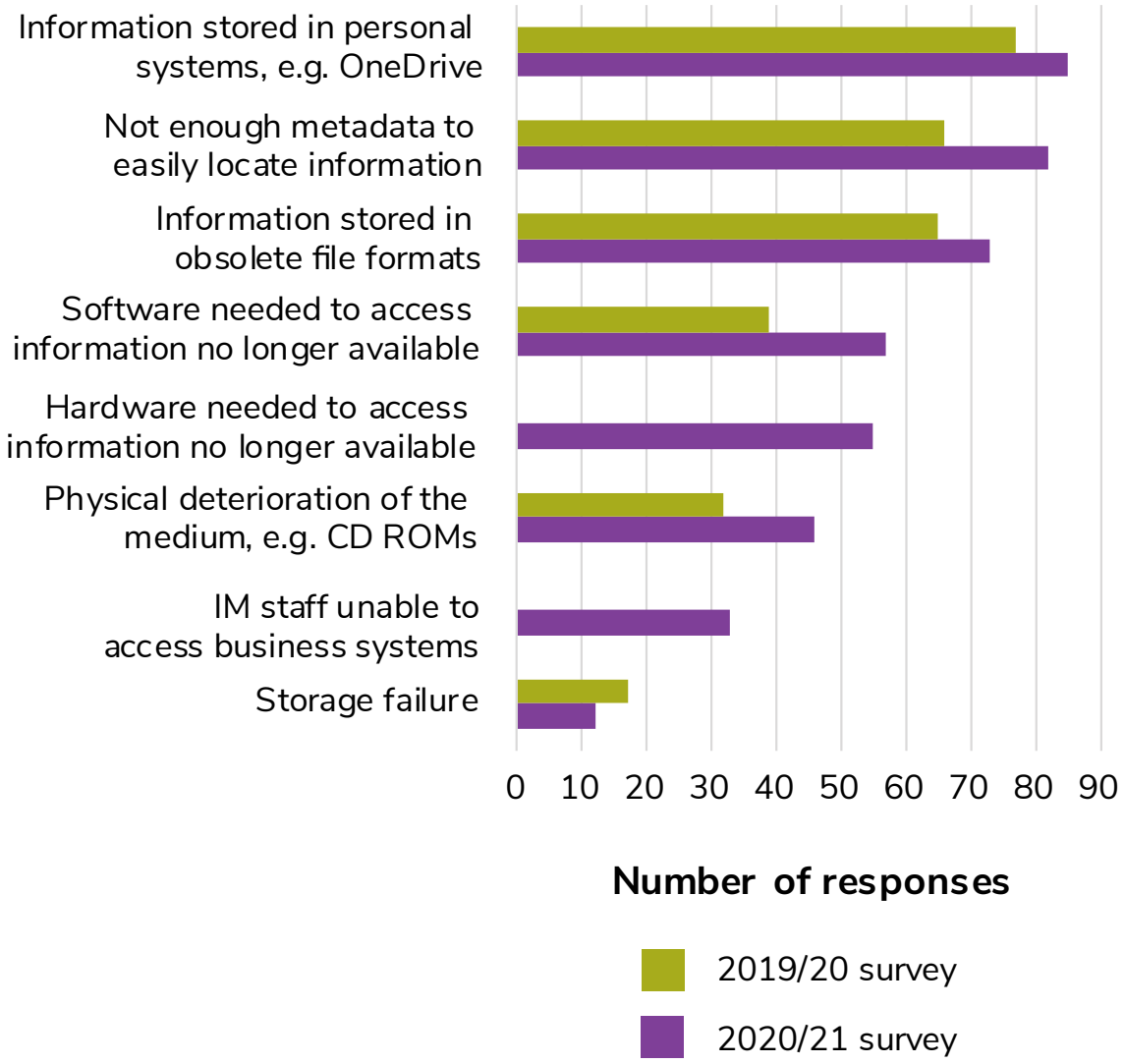


Figure 30: Reasons why digital information is inaccessible?



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:

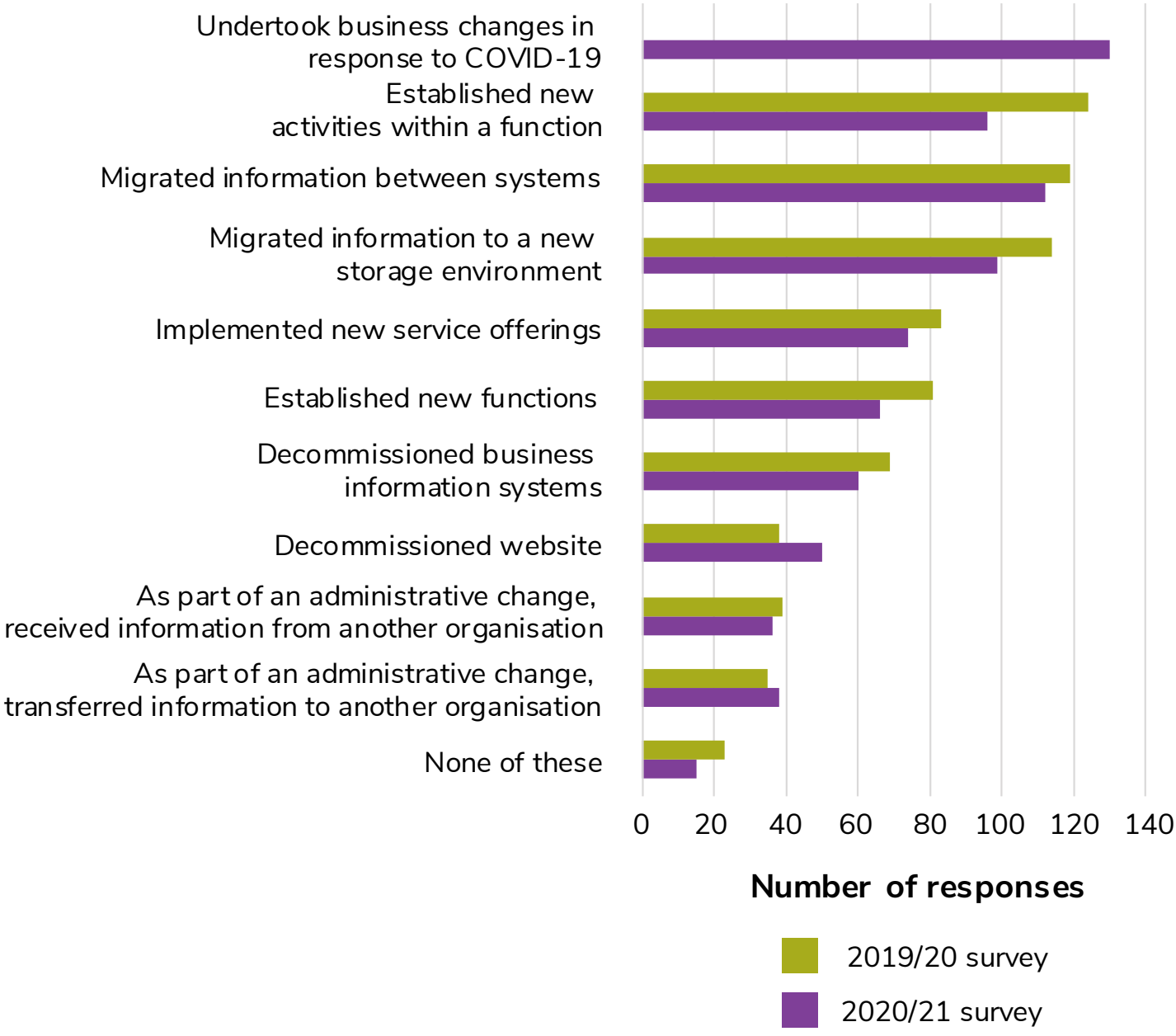
- What business changes have occurred in the last 12 months that have implications for IM (Q.32).
- If the organisation took actions to guarantee the integrity of information during those changes (Q.33).

Findings

Figure 31 shows that the most common type of organisational change reported this year is business changing in response to COVID-19. This was a new response option based on our analysis of qualitative responses in 2019/20. The quantity of responses indicates that it was a valid addition. Once again, migrating information between systems (52%) migrating information to a new storage environment (46%) and establishing a new business activity (45%) were other commonly reported types of change.

Of the 199 respondents who reported organisational changes listed in Figure 31, over half (59%) said that the integrity of information had been guaranteed in all instances of organisational change, while 37% said that this had been done 'in some cases.'

Figure 31: Organisational change in the last 12 months



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.

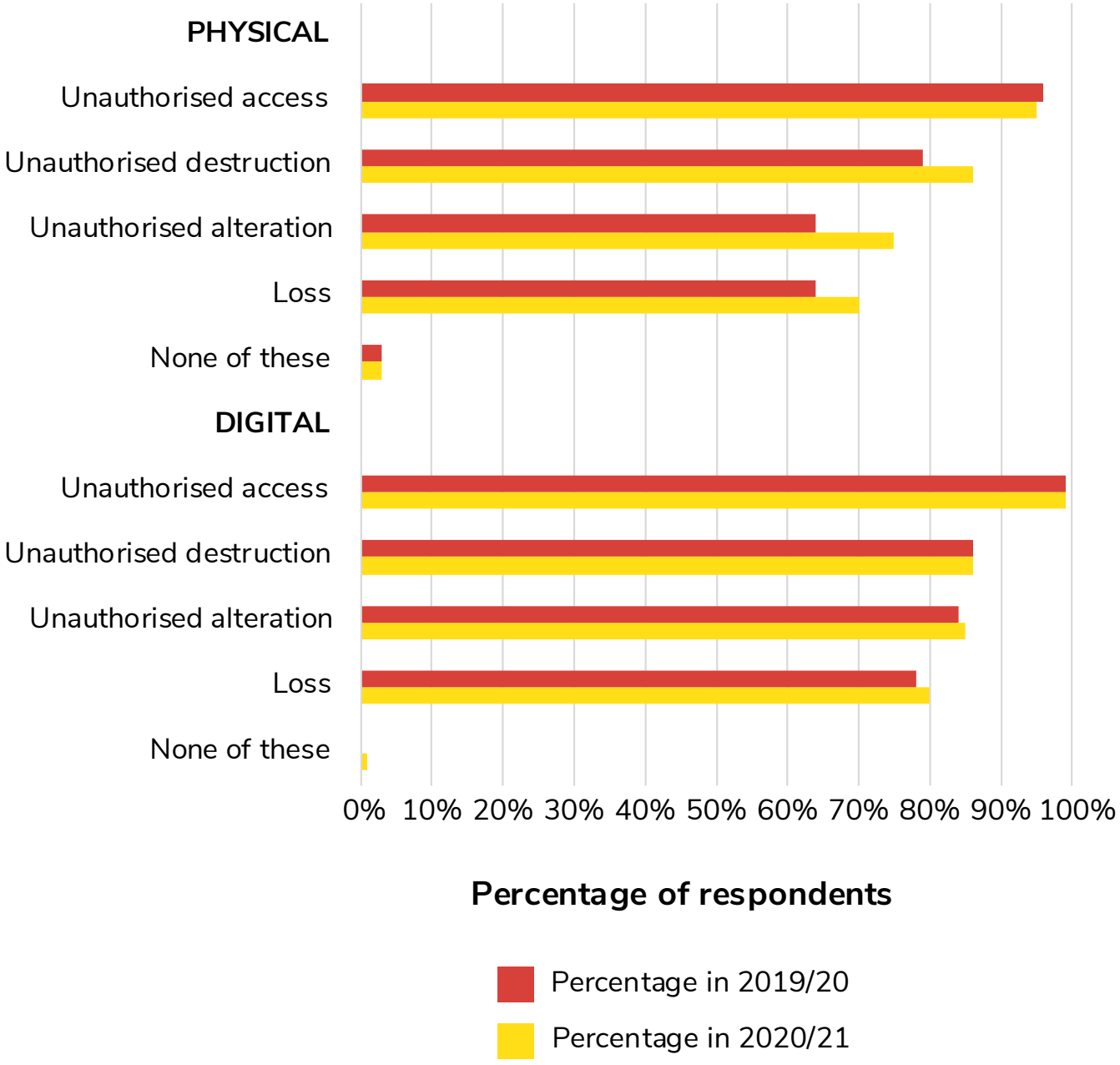
What we asked

We asked survey participants what security risks they protect their physical and digital information against (Q.34 and Q.35).

Findings

A high proportion of respondents said that they protect both physical and digital information against loss and unauthorised alteration, destruction and access (Figure 32).

Figure 32: 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.

What we asked

We asked survey participants:

- If they hold information that is more than 25 years old (Q.42).
- How much of that information has been classified as either open or restricted (Q.43).

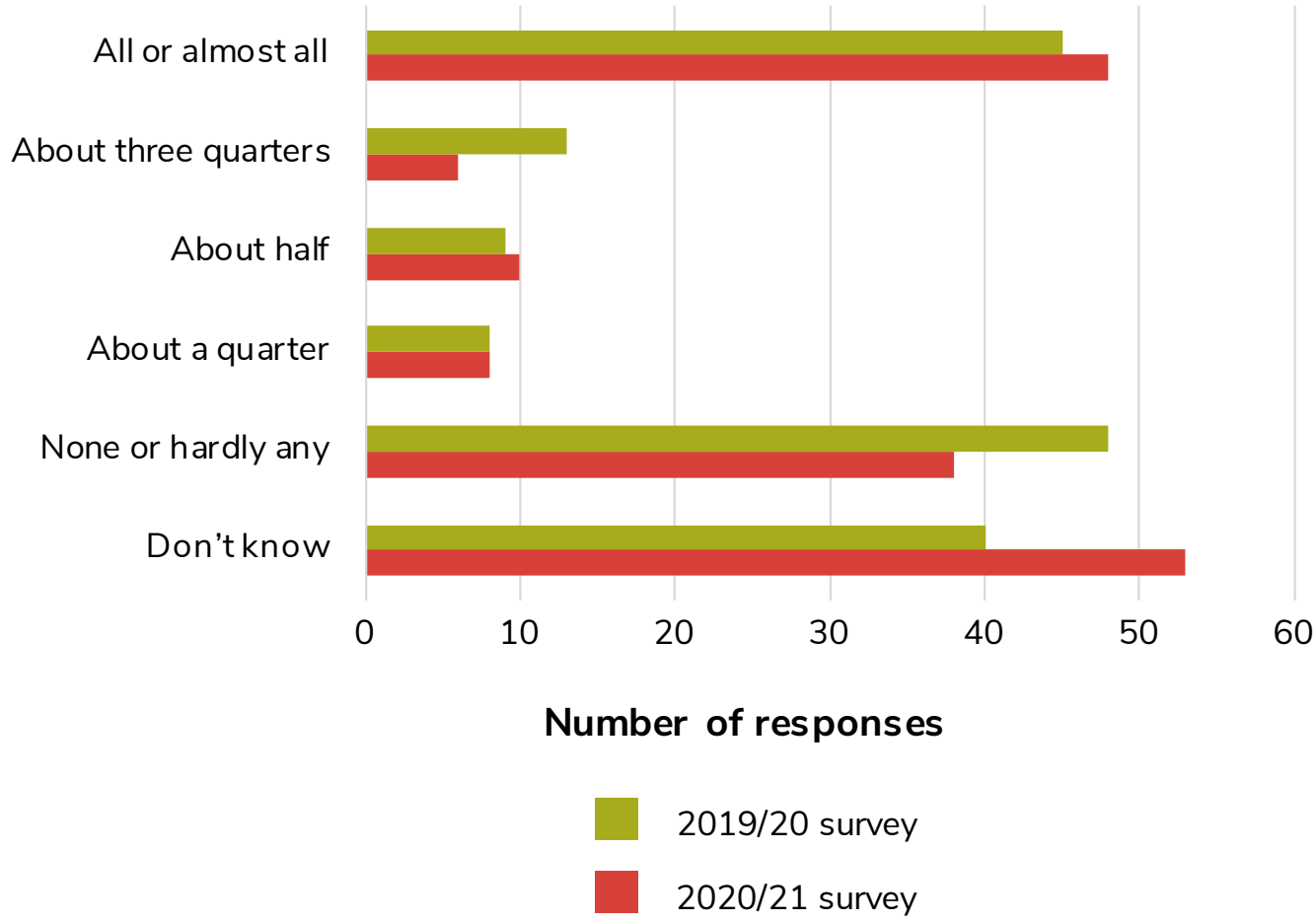
5 (2019). Office of the Ombudsman. Right to know essential to democracy in a digital world .

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)

Findings

Seventy-six percent of respondents said that they hold information that is more than 25 years old, the same percentage as 2019/20. Of those, only 29% have classified all or almost all of that information as open or restricted (Figure 33). Twenty-three percent have classified hardly any or no information, compared to 29% in 2019/20, while 33% replied 'don't know'. The high proportion of 'don't know' is informative ie. organisations did not realise they should be doing this at all.

Figure 33: 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 has not increased compared with our 2019/20 survey. However we can see an increase in internal standards which staff must meet with emphasis on relevance to the work done and security, multiple performance reviews throughout the year, inclusion of relevant legislation and policies into employment induction or e-learning modules available for existing staff. It is good to see emphasis being placed on IM within organisations and information asset registers are in use or being developed.

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.

For more findings and 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 2020/21.

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 is 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 includes in its brief the resourcing and prioritising of 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 is covered by authorised disposal authorities (Q. 36).
- How soon the organisation plans to improve disposal authority coverage (Q.37).
- What actions the organisation has taken in the last 12 months to prepare for doing disposal (Q.38).

Findings

More than half of respondents (57%) said that almost all of their information was covered by authorised disposal authorities (Figure 34). This represents no change since the 2019/20 survey. Of the 93 respondents who were asked when they plan to improve coverage, 48% provided a timeframe while 37% said that appraisal to improve coverage was underway.

For the second year, the most common actions to prepare for doing disposal were obtaining approval to dispose from business owners and sentencing information in offsite storage, i.e. physical information (Figure 35). Once again, there is far less activity focused on preparing digital information for disposal.

Figure 34: Proportion of information covered by disposal authorities

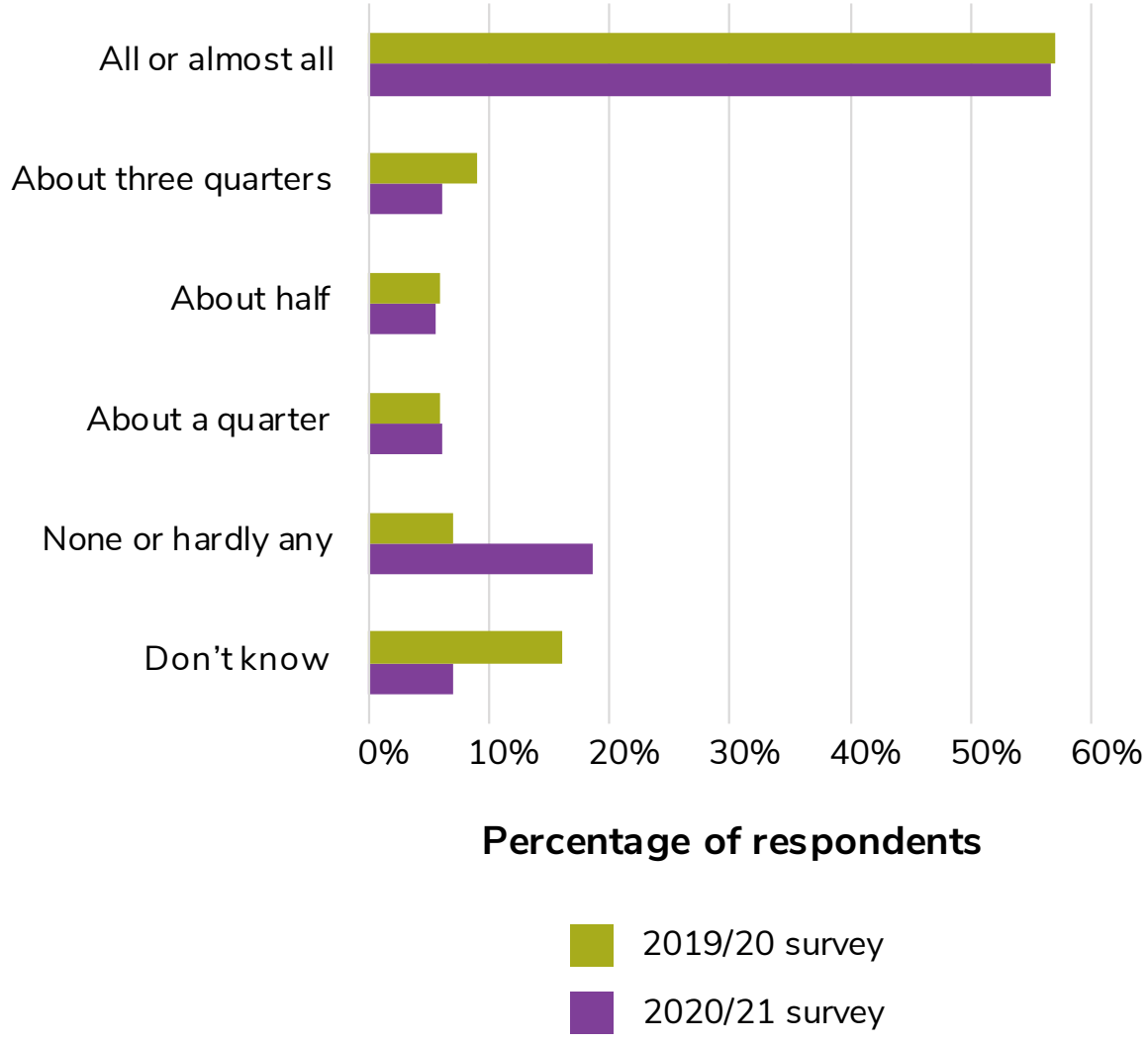
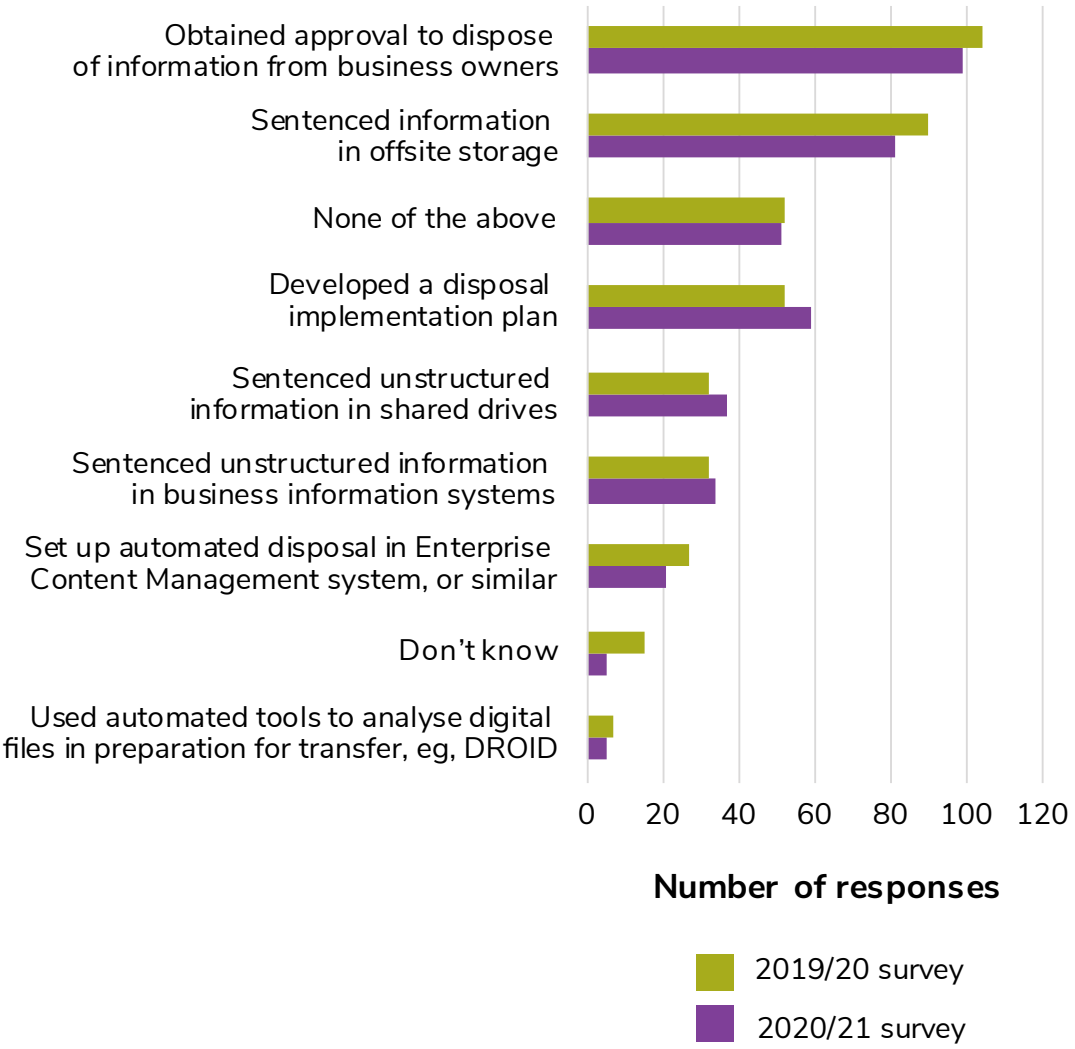


Figure 35: Actions to prepare for disposal over the last two surveys



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 or when no longer in current use. 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.39 and Q.40).
- What challenges affect their ability to undertake regular, authorised destruction (Q.41).
- If they have plans to transfer physical or digital information in the next 12 months, and if so the transfer destination (Q.44, Q.45, Q.47).
- If they hold physical information that is ready to transfer to our new Wellington repository when it becomes fully operational (Q.46).
- What challenges affect their ability to undertake regular transfer (Q.48).

Findings

Fifty-six percent of respondents have done some form of destruction (i.e. either physical or digital) compared to 58% in 2019/20. Figure 36 shows that the proportion of respondents who have destroyed physical information is much higher than digital information: 52% have destroyed physical, while only 29% have destroyed digital.

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 37). Other challenges mentioned in the comments in addition to those listed in Figure 37, include:

- Moratorium on the disposal of records relating to a Royal Commission Inquiry.
- Complexity of Disposal Authority, e.g. categorisations of information classes and the numerous exclusions.
- Lack of staff awareness of their responsibilities.
- Insufficient resources - staff, budget.

Figure 36: Authorised destruction over the last two surveys

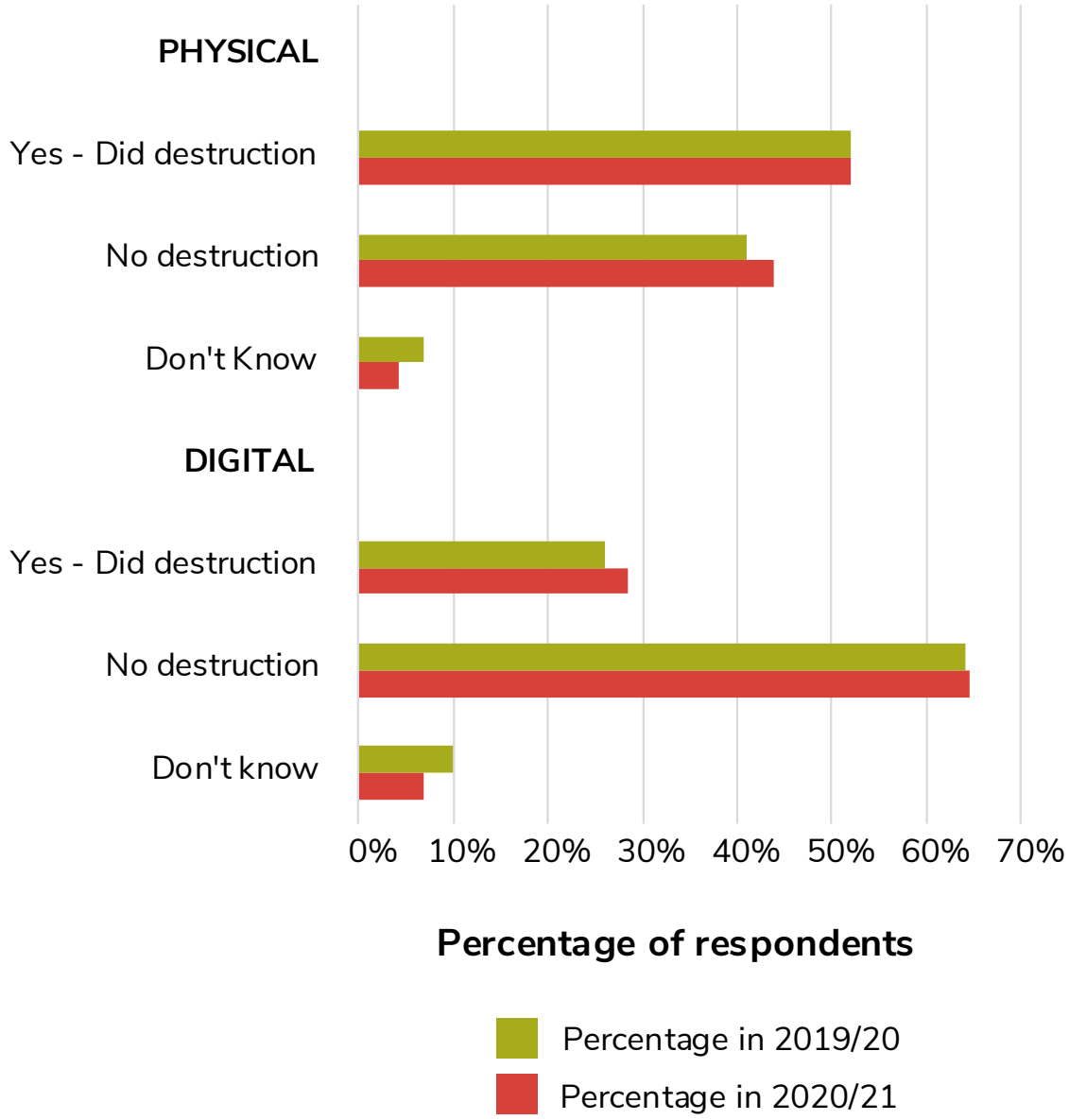
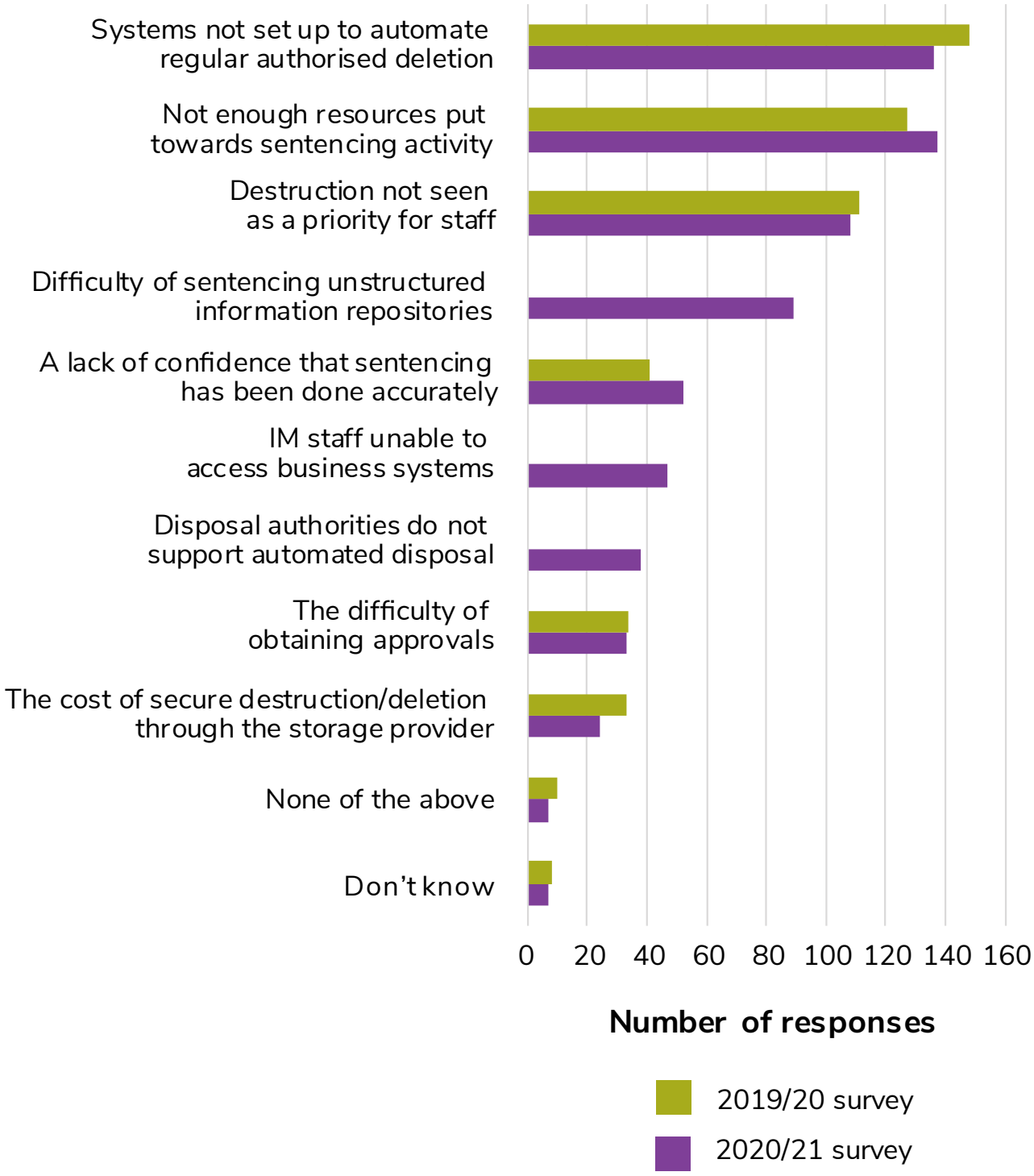


Figure 37: Challenges for doing authorised destruction of information

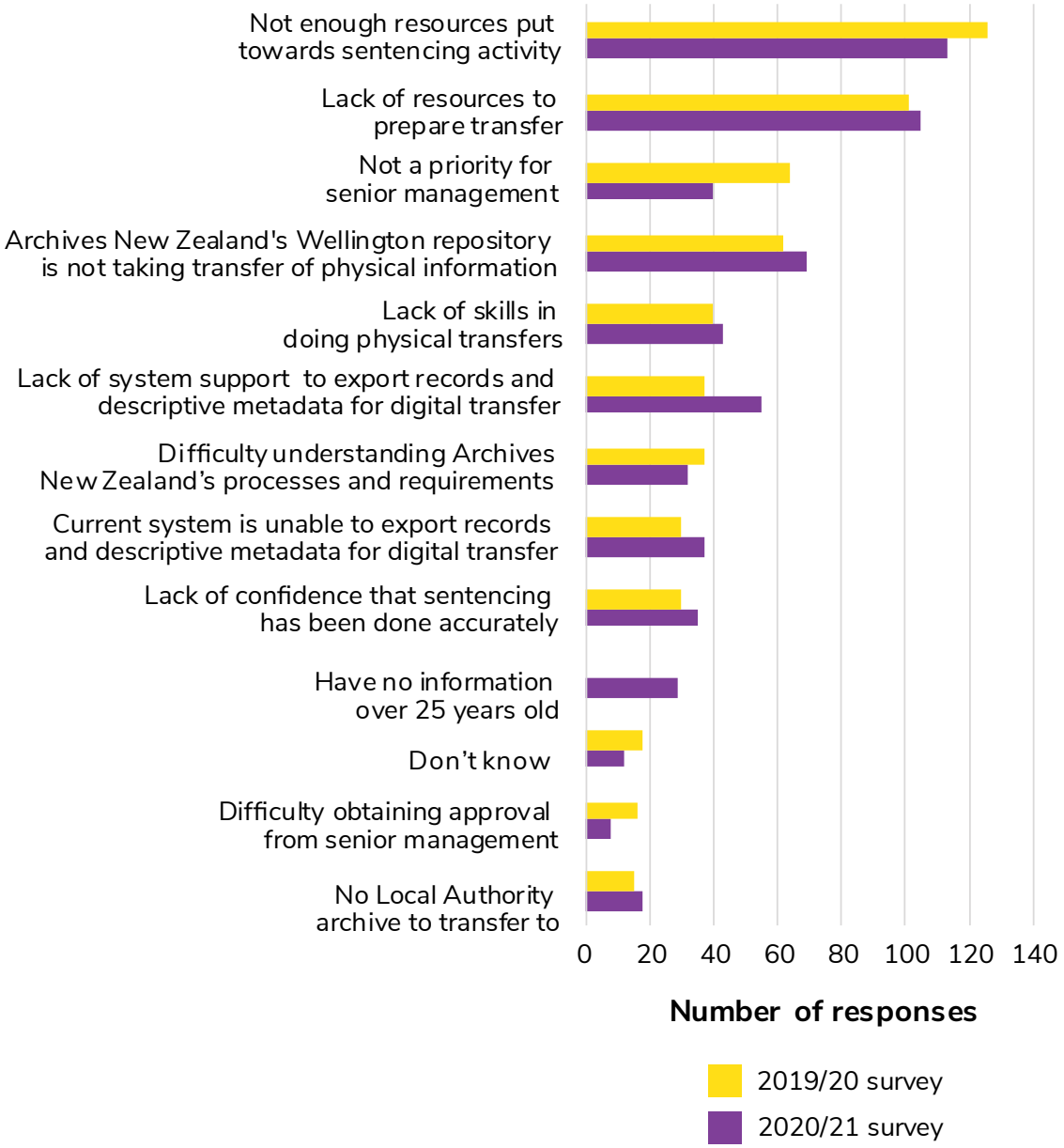


Only a minority of respondents have plans to transfer physical (23%) or digital (13%) information the next 12 months. This year we added a new question to the survey, to help us start planning for transfers into the future repositories. Twenty percent of respondents said that they hold physical information that is ready to transfer to our new Wellington repository when it becomes fully operational.

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 38). Other challenges mentioned in the comments in addition to those listed in Figure 38 include:

- Lack of an approved disposal authority
- Records are still needed
- Lack of skills in doing digital transfers
- Legislative changes required to enable transfer of some records

Figure 38: Challenges for transferring information



Key findings

A consistent challenge identified by respondents regarding disposal is Archives New Zealand's current moratorium on transfers especially regarding records related to the Royal Commission of Inquiry into Historical Abuse. Issues identified within organisations are the lack of staff or staff knowledge to carry out authorised disposal especially regarding digital information.

There appears to be a lack of understanding regarding disposal authorities set out by Archives. We acknowledge that there is plenty of work required to improve our instruments, tools, processes and guidance so that they better support disposal especially digital.

For more findings and recommendations concerning regular, authorised destruction of information, see the *Chief Archivist's Annual Report on the State of Government Recordkeeping 2020/21.*

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.49).
- Challenges affect good IM in their organisation (Q.50).
- Key risks to their organisation's information have been identified (Q.51 and Q.52).

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. The care for IM should rest on benefits for the business and compliance requirements that deliver benefits for others.

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 39 shows that the strongest drivers for IM are risk management and compliance with legislative requirements. This is consistent with our findings from 2019/20. Eighty-one 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 39, include:

- Building better resilience and supporting responses to crisis (especially in the light of COVID 19).
- Supporting strategic goals of our organisation/sector.
- Information/data has high value for future research on our sector.
- The majority of respondents rated all but two of the challenges we asked about as either 'reasonably big' or 'huge' (Figure 40). The biggest challenges are lack of understanding of the importance of IM, insufficient resourcing for IM, and adequately addressing IM during project planning. This is fairly consistent with our 2019/20 findings, although resourcing for IM has moved up in the rankings. Other challenges mentioned in the comments in addition to those listed in Figure 40, include: IM staff training for digital preservation.
- The complex nature of our sector and the size of our organisation.
- Format and arrangement of the Disposal Authorities a barrier to automated disposal of information.

Figure 41 shows that the most common risks to information are shadow IT or personal repositories, lack of contextual information and unsupported business systems. 'Shadow IT and personal repositories' was a new response option based on our analysis of qualitative responses in 2019/20. The quantity of responses indicates that it was a valid addition. We also added a 'collaboration tools' option this year. Other risks mentioned in the comments in addition to those listed in Figure 41, include:

- Cybersecurity threats (e.g. hacking, ransomware, phishing).
- Inadvertent release of information.
- Information held by contractors and not accessible by organisation.
- Behaviour of staff, e.g. not following proper procedures.
- Lack of cohesive planning for ongoing adoption of MS 365 applications.

Figure 39: Drivers for good IM

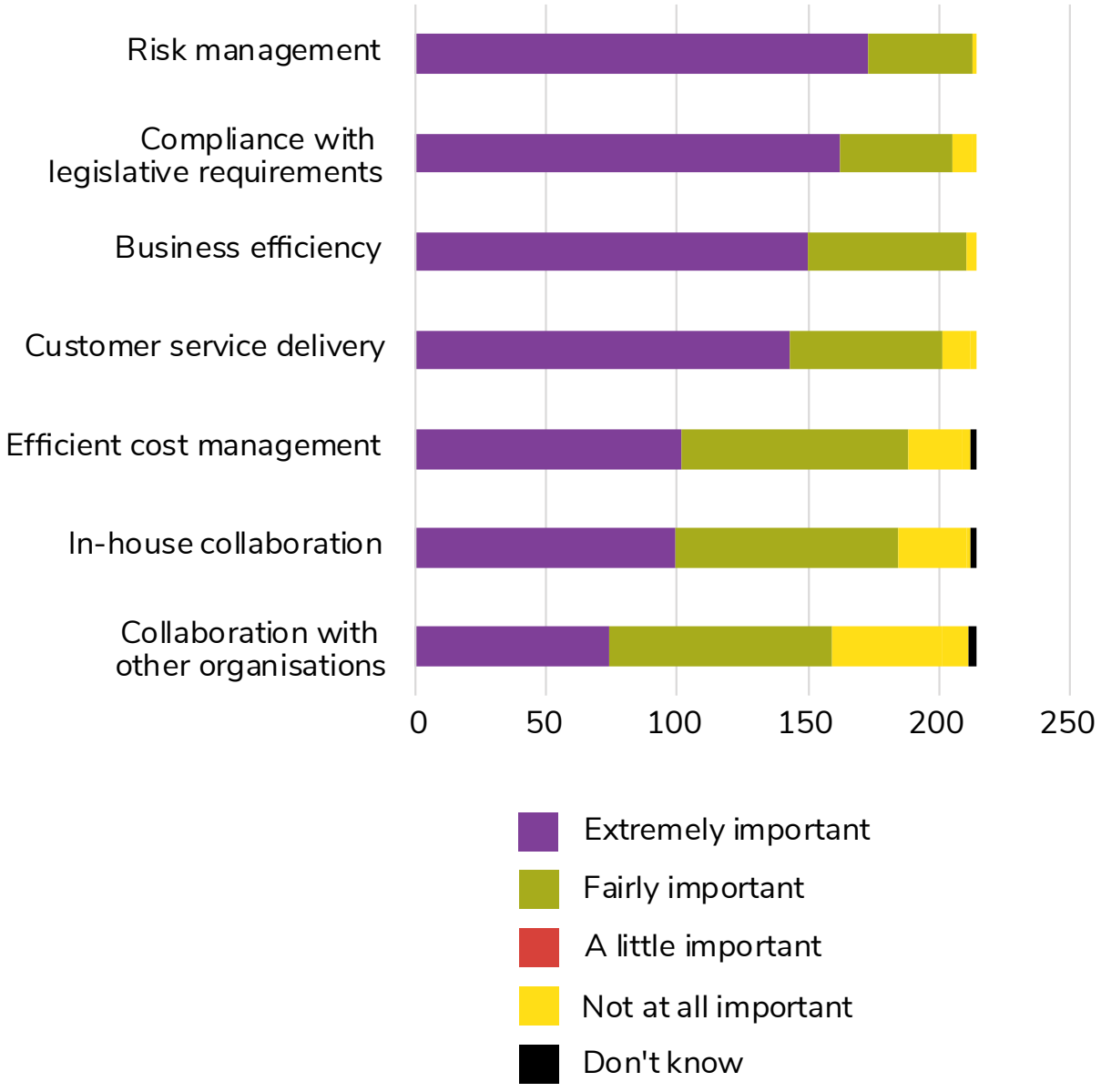


Figure 40: Challenges for good IM

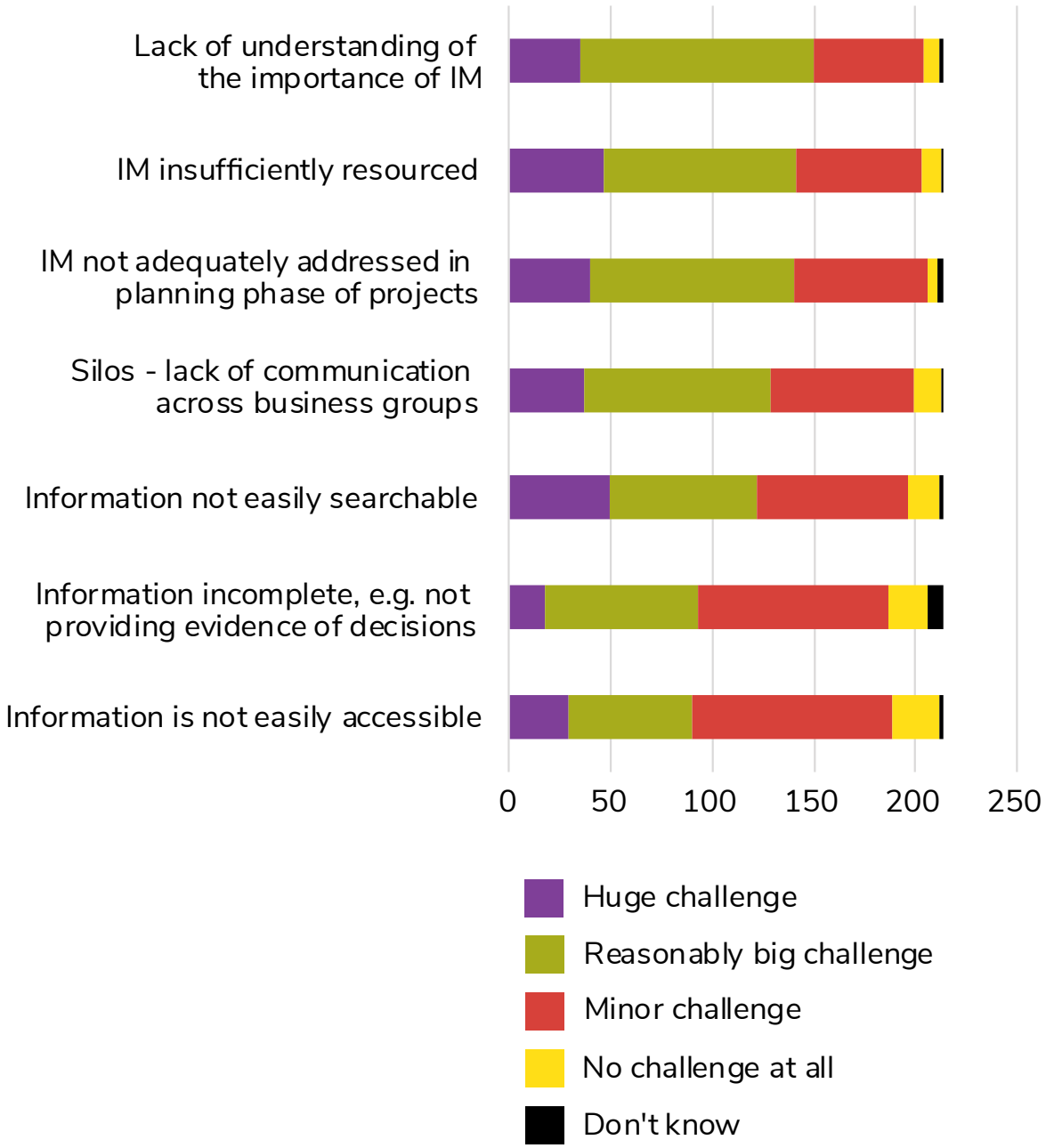
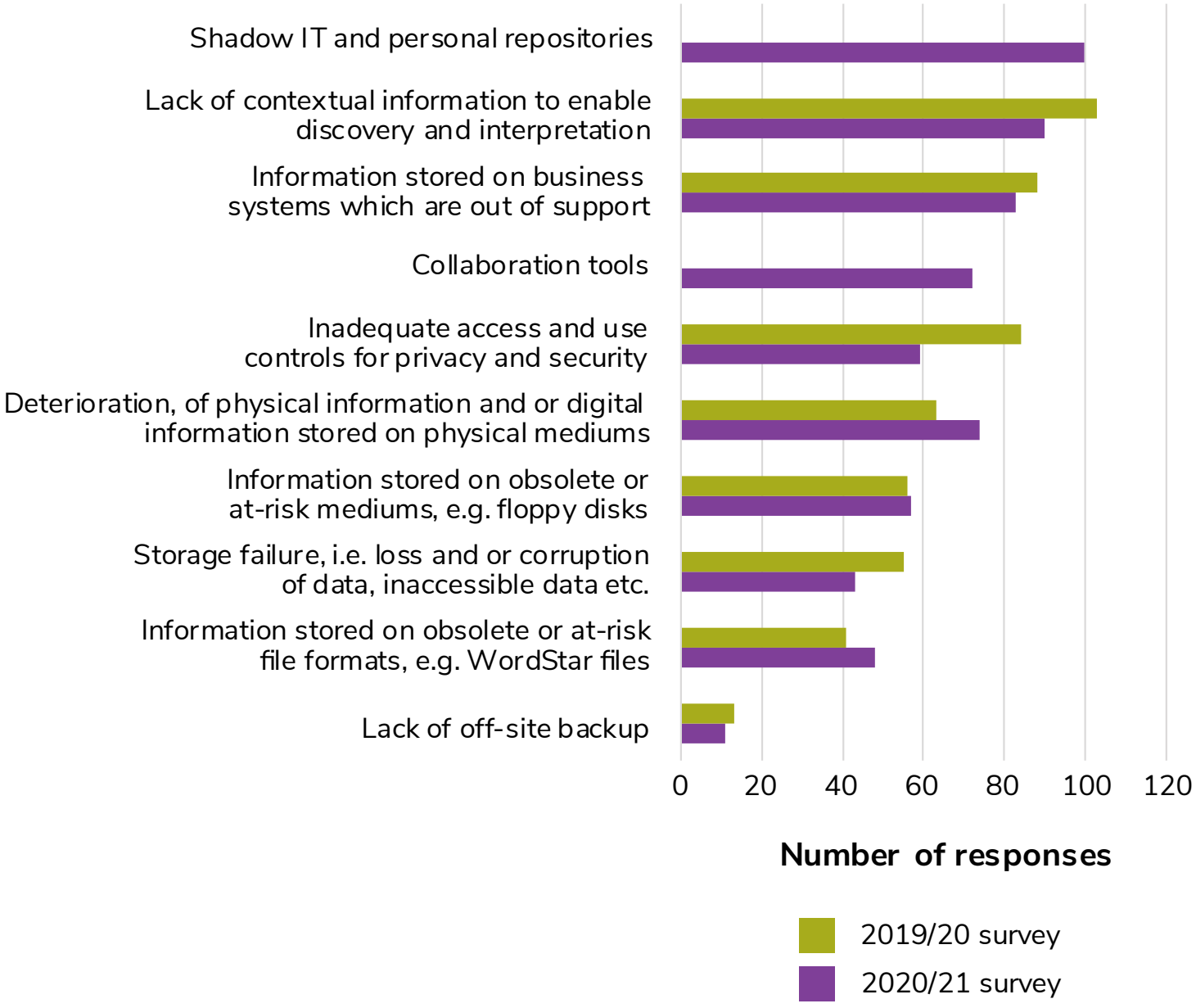


Figure 41: Risks to information



Requests for official information

What we asked and why

We asked survey participants:

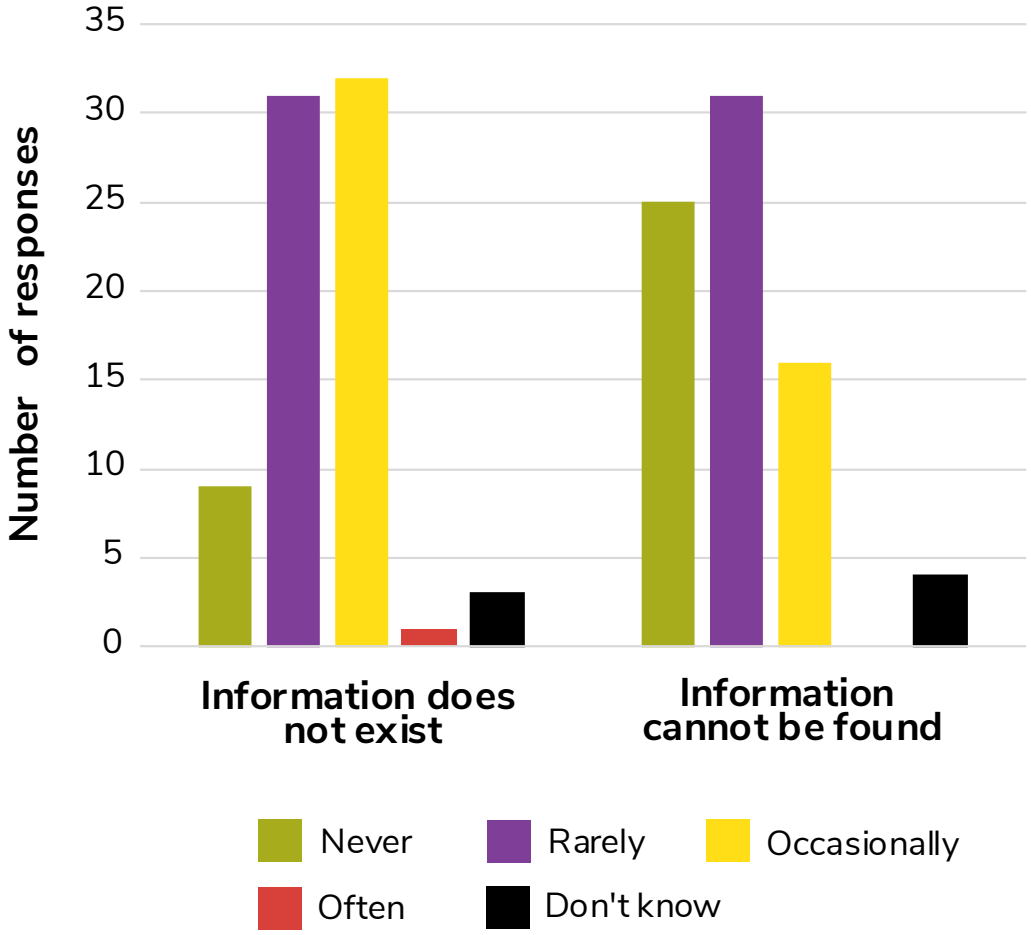
- About instances in the last 12 months when they have been unable to provide information requested under an official information request (Q.53 and Q.54).
- How often the reason for not being able to provide information is that it does not exist or cannot be found (Q.55 and Q.56).

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. 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 204 respondents who received requests for official information in the last 12 months, 38% (77 organisations) said that there were occasions when they were unable to provide the information requested. Of those, a combined 52% said that the reason for this was ‘rarely’ or ‘never’ because the information does not exist (Figure 42). A combined 73% said the reason for this was ‘rarely’ or ‘never’ because the information cannot be found.

Figure 42: Frequency with which information does not exist or cannot be found



Key findings

Information accessed through Official Information requests has increased, however a consistent issue remains whether information was produced in the first place.

The most common risk identified is digital instability, whether this is use of shadow IT, or outdated digital storage which compromises the integrity of the information stored. External cyber-attacks have also been identified as a significant concern for organisations. A collaborative relationship between IM and IT staff is essential to protect and ensure the accessibility of government information of long-term value, and to ensure digital continuity. Upskilling to meet the challenges of digital IM is clearly an issue for public sector IM staff.

It is unsurprising that risk management remains 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.

COVID-19 remains the largest impact on organisations and their IM practices. The ability to access information remotely and digitally has been shown to be more important than ever.

Appendix 1

Survey questionnaire and tables

Note: Except from Q10, 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.

Q1. What is the name of your organisation?

Table: Q2 What type of organisation is it?

Response Options	Number	Percent
State sector	158	73.8%
Local government	56	26.2%
Total	214	100.0%

Explanatory note: 'State sector' includes public service and non-public service departments, organisations that are part of the legislative branch of government, all categories of Crown entities, Public Finance Act schedule 4 organisations and state-owned enterprises.

Note for Q2: Although 'Other' responses were permitted in the survey questionnaire, these were subsequently checked and recoded as 'State sector' or 'Local government'

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

Response Options	Number	Percent
Offices located across more than one town city but all in New Zealand	123	57.5%
One office only	40	18.7%
More than one office, all of them in the same town city	37	17.3%
Offices located across more than one country	14	6.5%
Total	214	100.0%

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

Response Options	Number	Percent
None	1	0.5%
Less than 100	54	25.2%
100 to 299	48	22.4%
300 to 499	32	15.0%
500 to 2999	54	25.2%
3000 to 5999	15	7.0%
More than 6000	10	4.7%
Total	214	100.0%

Table: Q5 Does your organisation have a formal governance group which:

Response options	Number	Percent
Has IM oversight as part of its mandate	103	48.1%
Is dedicated to IM	26	12.1%
Neither of the above	85	39.7%
Total	214	100.0%

Table: Q6 Does the formal governance group meet at least twice a year?

Response Options	Number	Percent
Yes	120	93.0%
No	7	5.4%
Don't know	2	1.6%
Total	129	100%

Table: Q7 Is your Executive Sponsor part of the formal governance group?

Response Options	Number	Percent
Yes	117	90.7%
No	12	9.3%
Total	129	100%

Table: Q8 Does your organisation have a documented IM policy?

Response Options	Number	Percent
Yes	179	83.6%
No	34	34.6%
Don't know	1	0.5%
Total	214	100%

Table: Q9 Has your organisation identified information it holds that is of importance to Māori?

Response Options	Number	Percent
Yes	74	34.6%
No	97	45.3%
Don't hold any	15	7.0%
Don't know	28	13.1%
Total	214	100%

Table: Q10 Does your organisation have criteria or methodologies for assessing this?

Response options	Number	Percent
Yes, please specify	30	40.5%
No	30	40.5%
Don't know	14	18.9%
Total	74	100.0%

Table: Q11 Which of the following has your organisation done to improve the usage of information that is of importance to Māori? (tick all that apply) (N=74)

Response Options	Number	Percent
Documented IM implications from Te Tiriti o Waitangi agreements	14	18.9%
Improved access	35	47.3%
Improved discoverability e.g. improved metadata	27	36.5%
Improved levels of care	19	25.7%
Involved IM staff in negotiating agreements with Māori	9	12.2%
Worked with Māori to change IM practices	19	25.7%
No action taken	19	9.5%

Note for Q11: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=74). Similarly, the percents do not add to 100%.

Table: Q12 In the last 12 months, has your organisation done any self-monitoring of its compliance with: (tick all that apply) (N=214)

Response Options	Number	Percent
Archives New Zealand's requirements	127	59.3%
This organisation's own IM policy	116	54.2%
Neither of these	52	24.3%

Note for Q12: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%.

Table: Q13 What method(s) were used for that self-monitoring? (tick all that apply) (N=162)

Response Options	Number	Percent
Assessment by a third party	35	21.6%
Bench-marking exercise	16	9.9%
Internal audit	61	37.7%
Maturity assessment	61	37.7%
Review of processes	115	71.0%
Risk Assessment	74	45.7%

Note for Q13: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=162). Similarly, the percents do not add to 100%.

Table: Q14 As a result of that self-monitoring, what action is your organisation taking? (tick all that apply) (N=162)

Response Options	Number	Percent
Developing an action plan	91	56.2%
Developed an action plan	43	26.5%
Implementing an action plan	59	36.4%
Implemented an action plan	18	11.1%
Deferring action	14	8.6%
None of these	6	3.7%

Note for Q14: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=162). Similarly, the percents do not add to 100%.

Table: Q15 How many full-time-equivalent (FTEs) are dedicated IM staff?

Explanatory note: This question is about dedicated information management staff. It does not include staff whose work is focused on:

- Geographic information systems
- Business intelligence
- Data management
- Medical records
- Business support

Response Options	Number	Percent
None	45	21.0%
1 IM FTE or less	50	23.4%
More than 1 up to 3 IM FTE	59	27.6%
More than 3 up to 6 IM FTE	32	15.0%
More than 6 up to 10 IM FTE	17	7.9%
More than 10 IM FTE	11	5.1%
Total	214	100%
Total FTE of dedicated IM staff across all 214 organisations	646.9	

Note for Q15: Respondents were asked to enter an exact number. Their responses have been classified into the options presented in the table.

Table: Q16 In the last 12 months, which of the following has any dedicated IM staff member(s) done? (tick all that apply) (N=169)

Response Options	Number	Percent
Attended an IM conference (or similar event)	71	42.0%
Attended an IM training course (face-to-face and or/online)	119	70.4%
Had an IM-relevant secondment	10	5.9%
Presented at an IM conference (or similar event)	16	9.5%
Studied towards a recognised IM qualification	24	14.2%
None of these	31	18.3%

Note for Q16: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=169). Similarly, the percents do not add to 100%.

Table: Q17 Which of the groups below does your organisation inform about their IM responsibilities (tick all that apply) (N=214)

Response Options	Number	Percent
Staff at all levels	203	94.9%
Contractors	137	64.0%
Consultants	103	48.1%
None of these	10	4.7%

Note for Q17: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%.

Table: Q18 In which way(s) are the groups that you ticked in the previous question informed about their IM responsibilities? (tick all that apply) (N=204)

Response Options	Number	Percent
Code of Conduct	107	52.5%
Contracts	100	49.0%
Induction training (face-to-face and/or online)	168	82.4%
Job descriptions	77	37.7%
Performance development plans /agreements	28	13.7%
Refresher training (face-to-face and/or online)	115	56.4%
Don't know	0	0.0%
None of the above	0	0.0%

Note for Q18: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=204). Similarly, the percents do not add to 100%

Table: Q19 Has your organisation identified its most important high value/high risk information?

Response Options	Number	Percent
Yes	74	34.6%
In progress	104	48.6%
No	27	12.6%
Don't know	9	4.2%
Total	214	100%

Table: Q20 In the last 12 months, in order to actively manage its high-value/high-risk information, what action(s) has your organisation taken? (tick all that apply) (N=214)

Explanatory note: 'Business information systems' include human resources information systems (HRIS), financial systems, specialised databases etc

Response Options	Number	Percent
Developed information architecture and/or search tools	77	36.0%
Implemented a new business information system to mitigate risks to information	65	30.4%
Implemented back-up capability	76	35.5%
Redeveloped systems to improve long-term accessibility of information	65	30.4%
Tested its business continuity plan	78	36.4%
Don't know	21	9.8%

Note for Q20: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%

Table: Q21 Does your organisation have an information asset register (or similar way of recording information assets)?

Response Options	Number	Percent
Yes	49	22.9%
In development	68	31.8%
Work started but deferred	25	11.7%
No	72	33.6%
Total	214	100.0%

Table: Q22 Is that register:

Response Options	Number	Percent
Up-to-date?	24	49.0%
Being used?	36	73.5%
Neither of these	7	14.3%
Total	49	100.0%

Table: Q23 Is your organisation planning to have an information asset register (or similar)?

Response Options	Number	Percent
Yes	37	51.4%
No	16	22.2%
Don't know	19	26.4%
Total	72	100.0%

Table: Q24. In the last 12 months, has your organisation implemented any new business information system(s)?

Explanatory note: Business information systems include human resources information systems (HRIS) financial systems, specialised databases etc.

Response Options	Number	Percent
Yes	139	65.0%
No	69	32.2%
Don't know	6	2.8%
Total	214	100.0%

Table: Q25. Is a process for managing information through its life-cycle built into those new business information system(s)?

Response Options	Number	Percent
Yes	72	51.8%
No	47	33.8%
Don't know	20	14.4%
Total	139	100.0%

Table: Q26 Which challenge(s) affect your organisation's ability to integrate IM requirements into new or upgraded business information systems? (tick all that apply) (N=214)

Response Options	Number	Percent
Age of business system(s)	101	47.2%
IM requirements are not specified in the procurement process	90	42.1%
IM requirements considered 'nice-to-have' or de-scoped	67	31.3%
IM staff are not consulted enough	97	45.3%
Internal staff are not fully aware of the requirement	137	64.0%
Not enough management support	45	21.0%
Speed of implementation/upgrade	80	37.4%
The number of systems in use	110	51.4%
Don't know	3	1.4%
None	18	8.4%

Note for Q26: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%

Table: Q27 Do your organisation's current systems for managing documents and records meet the minimum requirements set in Archives New Zealand's Minimum Requirements for Metadata?

Response options	2020/21 survey	2019/20 survey
Don't know	21	21
Implementing a new business information system to mitigate risks to information	65	74
Redeveloping systems to improve long-term accessibility of information	65	82
Implementing back up capability	76	0
Developing information architecture and/or search tools	77	0
Testing Business Continuity Plan	78	126
Total	382	303

Table: Q28. Does your organisation have any digital information of long-term value (i.e. required for more than 10 years)?

Response Options	Number	Percent
Yes	189	88.3%
No	13	6.1%
Don't know	12	5.6%
Total	214	100.0%

Table: Q29 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 your organisation taken for that purpose? (tick all that apply) (N=189)

Response Options	Number	Percent
Ensured metadata is persistently linked to information	72	38.1%
Identified information needing long-term retention	122	64.6%
Implemented a digital storage management plan	29	15.3%
Migrated information to a long-term digital storage environment	64	33.9%
Migrated information to new file formats	44	23.3%
Used checksums to monitor integrity of information	16	8.5%
Don't know	7	3.7%
None of the above	16	8.5%

Note for Q29: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=189). Similarly, the percents do not add to 100%

Table: Q30. Does your organisation have any digital information that is inaccessible (i.e. cannot be located, retrieved or used)?

Response Options	2020/21 survey	2019/20 survey
Don't know	26	39
Definitely don't	52	61
Possibly	92	82
Definitely	44	32

Table: Q 31. What are the reasons your organisation is unable to access that digital information? (tick all that apply) (N=136)

Response Options	Number	Percent
Hardware needed to access information no longer available	55	40.4%
IM staff unable to access business systems	33	24.3%
Information stored in obsolete file format(s)	73	53.7%
Information stored in personal system (e.g. OneDrive)	85	62.5%
Not enough metadata to easily locate information	82	60.3%
Physical deterioration of the medium (e.g. CD-ROMS)	46	33.8%
Software needed to access information no longer available	57	41.9%
Storage failure	12	8.8%

Note for Q31: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=136). Similarly, the percents do not add to 100%

Table: Q32 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) (N=214)

Response Options	Number	Percent
As part of an administrative change, received information from another organisation	36	16.8%
As part of an administrative change, transferred information to another organisation	38	17.8%
Decommissioned business information system(s)	60	28.0%
Decommissioned website	50	23.4%
Established new activity/activities within a function	96	44.9%
Established new function(s)	66	30.8%
Implemented new service offering(s)	74	34.6%
Migrated information between systems	112	52.3%
Migrated information to a new storage environment	99	46.3%
Undertook business changes in response to COVID-19	130	60.7%
None of these	15	7.0%

Note for Q32: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%

Table: Q33 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 your organisation take action to guarantee the integrity of the information involved?

Response Options	Number	Percent
In every case	118	59.3%
In some cases	73	36.7%
Don't know	8	4.0%
Total	199	100.0%

Table: Q34. This question is about physical information. Which security risk(s) does your organisation take measures to protect against? (tick all that apply) (N=214)

Response Options	Number	Percent
Unauthorised access	204	95.3%
Unauthorised alteration	161	75.2%
Unauthorised destruction	184	86.0%
Loss	150	70.1%
None of these	6	2.8%

Note for Q34: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%.

Table: Q35. This question is about storage of digital information. Which security risk(s) does your organisation take measures to protect against? (tick all that apply) (N=214)

Response Options	Number	Percent
Unauthorised access	211	98.6%
Unauthorised alteration	181	84.6%
Unauthorised destruction	184	86.0%
Loss	172	80.4%
None of these	2	0.9%

Note for Q35: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%

Table: Q 36. How much of the information held by your organisation is covered by authorised disposal authorities?

Response Options	Number	Percent
None or hardly any	40	18.7%
About a quarter of it	13	6.1%
About half of it	12	5.6%
About three-quarters of it	13	6.1%
All or almost all	121	56.5%
Don't know	15	7.0%
Total	214	100.0%

Table: Q37. This question is about the information not covered by disposal authorities. When does your organisation plan to start improving coverage?

Response Options	Number	Percent
We are currently appraising our information	34	36.6%
In less than 12 months	17	18.3%
In the next 1-3 years	27	29.0%
In the next 4-5 years	1	1.1%
Don't know	14	15.1%
Total	93	100.0%

Table: Q 38. This question is about both physical and digital information. In the last 12 months, which action(s) has your organisation carried out in preparation for disposal? (tick all that apply) (N=214)

Explanatory note: 'Sentenced' means the process of applying a disposal authority and its disposal actions across an organisation's information. 'Unstructured information' means information that either does not have a predefined data model or is not organised in a pre-defined manner.

Response Options	Number	Percent
Developed a disposal implementation plan	59	27.6%
Obtained approval to dispose of information from business owners	99	46.3%
Sentenced information in offsite storage	81	37.9%
Sentenced unstructured information in business information systems	34	15.9%
Sentenced unstructured information in shared drives	37	17.3%
Set-up automated disposal in Enterprise Content Management System (or similar)	21	9.8%
Used automated tools to analyse digital files in preparation for transfer (e.g. DROID)	5	2.3%
Don't know	5	2.3%
None of the above	51	23.8%

Note for Q38: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%.

Table: Q39. In the last 12 months, has your organisation carried out authorised destruction of physical information?

Response Options	Number	Percent
Yes	111	51.9%
No	94	43.9%
Don't know	9	4.2%
Total	214	100.0%

Table: Q 40. In the last 12 months, has your organisation carried out authorised destruction of digital information?

Response Options	Number	Percent
Yes	61	28.5%
No	138	64.5%
Don't know	15	7.0%
Total	214	100.0%

Table: Q 41. This question is about both physical and digital information. Which challenge(s) affect your organisation's ability to undertake regular authorised destruction of information? (tick all that apply) (N=214)

Response Options	Number	Percent
A lack of confidence that sentencing has been done accurately	52	24.3%
Destruction not seen as a priority for staff	108	50.5%
Difficulty of sentencing unstructured information repositories	89	41.6%
Disposal authorities do not support automated disposal	38	17.8%
IM staff unable to access business systems	47	22.0%
Not enough resources put towards sentencing activity	137	64.0%
Systems not set up to automate regular authorised deletion	136	63.6%
The cost of secure destruction/deletion through the storage provider	24	11.2%
The difficulty of obtaining approvals	33	15.4%
Don't know	7	3.3%
None of the above	7	3.3%

Note for Q41: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%.

Table: Q42. Does your organisation hold any information that is more than 25 years old?

Response Options	Number	Percent
Yes	163	76.2%
No	39	18.2%
Don't know	12	5.6%
Total	214	100.0%

Table: Q 43. How much of that information over 25 years old has been classified as either open or restricted access?

Response Options	Number	Percent
None or hardly any	38	23.3%
About a quarter of it	8	4.9%
About half of it	10	6.1%
About three quarters of it	6	3.7%
All or almost all	48	29.4%
Don't know	53	32.5%
Total	163	100.0%

Table: Q 44. In the next 12 months, is your organisation planning to transfer any physical information?

Explanatory note: Public offices can transfer to an Archives New Zealand repository or an approved repository. Local authorities can transfer to a local authority archive.

Response Options	Number	Percent
Yes	49	22.9%
No	143	66.8%
Don't know	22	10.3%
Total	214	100.0%

Table: Q45. Where are you planning to transfer the physical information to?

Response Options	Number	Percent
A local authority archive	17	34.7%
Archives New Zealand's Auckland repository	13	26.5%
Archives New Zealand's Christchurch repository	3	6.1%
An approved repository, please specify	12	24.5%
Don't know	4	8.2%
Total	49	100.0%

Table: Q46. Does your organisation hold physical information that it is ready to transfer to Archives New Zealand's new Wellington repository when it becomes fully operational?

Explanatory note: Archives New Zealand's Wellington repository is unable to accept transfers at present, but we need to start planning ahead. It is expected that the new Wellington repository will be operational in 2026/27. 'Ready to transfer' means that your organisation has authority to dispose of the information and it has been listed to Archives New Zealand's requirements. If you select 'Yes' to this question we may contact you for further information.

Response Options	Number	Percent
Yes	42	19.6%
No	114	53.3%
Not applicable, local authorities select this option	58	27.1%
Total	214	100.0%

Table: Q47. In the next 12 months, is your organisation planning to transfer any digital information to:

Response Options	Number	Percent
Archives New Zealand	20	9.3%
A local authority archive	9	4.2%
Neither of these	149	69.6%
Don't know	36	16.8%
Total	214	100.0%

Table: Q48. This question is about both physical and digital information. What challenge(s) affect your organisation's ability to undertake regular transfer of information? (tick all that apply) (N=214)

Response Options	Number	Percent
Have no information over 25 years old	29	13.6%
Archives New Zealand s Wellington repository is not taking transfers of physical information	69	32.2%
Current system is unable to export records and descriptive metadata for digital transfer	37	17.3%
Difficulty obtaining approval from senior management	8	3.7%
Difficulty understanding Archives New Zealand s processes and requirements	32	15.0%
Lack of confidence that sentencing has been done accurately	35	16.4%
Lack of resources to prepare transfer	105	49.1%
Lack of skills in doing physical transfers	43	20.1%
Lack of system support to export records and descriptive metadata for digital transfer	55	25.7%
No local authority archive to transfer to	18	8.4%
Not a priority for senior management	40	18.7%
Not enough resources put towards sentencing activity	113	52.8%
Don't know	12	5.6%

Note for Q48: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=214). Similarly, the percents do not add to 100%.

Table: Q49. What current drivers for good IM practice and processes are important to your organisation? (N=214)

Response Options	Not important	A little important	Fairly important	Extremely important	Don't know
Business efficiency	0	4	60	150	0
Risk management	0	1	40	173	0
Customer service delivery	2	11	58	143	0
Compliance with legislative requirements	1	8	43	162	0
Efficient cost management	3	21	86	102	2
In-house collaboration	2	26	85	99	2
Collaboration with other organisations	10	42	85	74	3

Table: Q50. Below are some challenges for good IM practices and processes. In your organisation, how big a challenge are these to the organisation's IM? (N=214)

Response Options	No challenge at all	Minor challenge	Reasonably big challenge	Huge challenge	Don't know
Lack of understanding of the importance of IM	8	54	115	35	2
IM not adequately addressed in planning phase of projects	5	66	100	40	3
IM insufficiently resourced	10	62	94	47	1
'Silos' - lack of communication across business groups	14	70	92	37	1
Information incomplete, e.g. not providing evidence of decisions	19	94	75	18	8
Information not easily searchable	16	74	72	50	2
Information is not easily accessible	23	99	61	29	2

Table: Q51. Has your organisation identified any key risks to its information?

Response Options	Number	Percent
Yes	161	75.2%
No	36	16.8%
Don't know	17	7.9%
Total	214	100.0%

Table: Q52 What key risks to your organisation's information have been identified? (tick all that apply) (N=161)

Response Options	Number	Percent
Collaboration tools	72	44.7%
Deterioration (of physical information and/or digital information stored on physical mediums)	74	46.0%
Inadequate access and use controls for privacy and security	59	36.6%
Information stored on business systems which are out-of-support	83	51.6%
Information stored on obsolete or at-risk file formats (e.g. WordStar files)	48	29.8%
Information stored on obsolete or at-risk mediums (e.g. floppy disks)	57	35.4%
Lack of contextual information to enable discovery and interpretation	90	55.9%
Lack of off-site backup	11	6.8%
Shadow IT and personal repositories	100	62.1%
Storage failure (i.e. loss and/or corruption of data, inaccessible data etc.)	43	26.7%

Note for Q52: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=161). Similarly, the percents do not add to 100%.

Table: Q53. In the last 12 months, has your 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	204	95.3%
No	7	3.3%
Don't know	3	1.4%
Total	214	100.0%

Table: Q54. In the last 12 months, has your organisation ever been unable to provide the official information asked for?

Response Options	Number	Percent
Yes	77	37.7%
No	108	52.9%
Don't know	19	9.3%
Total	204	100.0%

Table: Q55. 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
Often	1	1.3%
Occasionally	32	41.6%
Rarely	31	40.3%
Never	9	11.7%
Don't know	3	3.9%
Missing response	1	1.3%
Total	77	100.0%

Table: Q 56. 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	25	32.5%
Rarely	31	40.3%
Occasionally	16	20.8%
Often	0	0.0%
Don't know	4	5.2%
Missing response	1	1.3%
Total	77	100.0%

Appendix 2

IM Maturity Assessment Topics based on Monitoring Criteria

Categories	Criteria	
Governance	1	IM Strategy - An information management (IM) strategy is a high-level document outlining the organisation's systematic approach to managing information. The strategy is a key document for an organisation's information management programme. It provides a long-term and organisation-wide direction for the management of the organisation's information.
	2	IM Policy and Processes - An information management policy gives a clear directive from the senior management to all staff, describing expected information management behaviour and practices. It highlights that the management of information is the responsibility of all staff and assigns roles and responsibilities at all levels of the organisation. An information management policy supports the organisation's information management strategy and provides a foundation for information management processes.
	3	Governance Arrangements and Executive Sponsor - The IM governance group is a high-level inter-disciplinary group that oversees all aspects of information management within the organisation ranging from strategy, risk and compliance through to metadata standards and privacy. Archives New Zealand's Information and records management standard (16/S1) requires a designated Executive Sponsor from every public office and local authority. The Executive Sponsor has strategic and executive responsibility for overseeing the management of information in a public sector organisation.
	4	IM Integration into Business Processes - All staff should be responsible for the information they create, use and maintain. Business owners should be responsible for ensuring that the information created by their teams is integrated into business processes and activities. The IM team support business owners and staff to do this.
	5	Outsourced Functions and Collaborative Arrangements - Organisations may need to contract external parties to perform various business functions and activities or collaborate with external parties. Outsourcing a business function or activity or establishing collaborative initiatives does not lessen an organisation's responsibility to ensure that all requirements for the management of information are met.

Categories	Criteria	
	6	Te Tiriti o Waitangi - The Public Records Act 2005 and the Information and records management standard supports the rights of Māori under Te Tiriti o Waitangi / Treaty of Waitangi (ToW) to access, use and reuse information that is important to Māori. This may include enhancing metadata to make information easier to find by or for Māori or ensuring that information of importance to Māori (for example: information about people, natural resources and land, or information required to support specific Te Tiriti commitments) is easy to access and use.
Self-monitoring	7	Organisations should monitor all aspects of their information management. Regular monitoring ensures that information is managed efficiently and effectively according to best practice and that this management continues to meet the business needs and legislative requirements of the organisation.
Capability	8	Capacity and Capability - Organisations should have IM staff or access to appropriate expertise to support their IM programme. This is required to meet the expectations of the organisation, the government and the wider community
	9	Roles and Responsibilities - Staff and contractors should be aware of their responsibility to manage information. These responsibilities should be documented and communicated to all staff and contractors so that the organisation's information is managed appropriately.
Creation	10	Creation and Capture of Information - Every public office and local authority must create and maintain full and accurate information documenting its activities. This information should be accessible, usable and reflect the organisation's business functions and activities.
	11	High-Value/High-Risk Information - High-value / high-risk information is information collected or created by the organisation that has particular value. The risk of loss or damage to this information will negatively impact individuals and/or communities. For example: information about rights and entitlements, natural resources, the protection and security of the state or infrastructure would come into this category.
Management	12	IM Requirements Built into Technologies - IM requirements must be identified, designed and integrated into all of your organisation's business systems. Taking a "by design" approach ensures that the requirements for the management of information are considered before, at the start of, and throughout the development and improvement of both new and existing business systems.

Categories	Criteria	
	13	Integrity of Information - Information integrity is about providing assurance that the information created and maintained by the organisation is reliable, trustworthy and complete. Information should be managed so that it is easy to find, retrieve and use, while also being secure and tamper-proof.
	14	Information Maintenance and Accessibility - Information maintenance and accessibility covers strategies and processes that support the ongoing management and access to information over time. This includes changes to business operations, activities and structures and/or system and technology changes.
	15	Business Continuity and Recovery - This covers the capability of the organisation to continue delivery of products or services, or recover the information needed to deliver products or services, at acceptable pre-defined levels following a business disruption event.
Storage	16	Appropriate Storage Arrangements - The storage of information is a very important factor that influences information protection and security. Appropriate storage arrangements for both physical and digital information ensures information remains accessible and usable throughout its life.
	17	Local Authority Storage Arrangements for Protected Information and Local Authority Archives - The storage of information is a very important factor that influences information protection and security. Protected information and local authority archives have specific requirements for appropriate storage arrangements for both physical and digital information to ensure information remains accessible and usable throughout its life.
Access	18	Information Access, Use and Sharing - Ongoing access to and use of information is required to enable staff to do their jobs. To facilitate this, organisations will need mechanisms to support the findability and usability of information. Information and data that is shared between organisations is identified and managed.
	19	Local Authority Archives Access Classification - The access status of local authority archives must be determined. They must be identified as either “open access” or “restricted access”. Access decisions and access conditions should be recorded in a publicly available register maintained by the local authority.

Categories	Criteria	
Disposal	20	Current Organisation-Specific Disposal Authorities - A disposal authority is the legal mechanism that the Chief Archivist uses to provide approval for disposal actions for specified information. This topic is about an organisation having its own specific disposal authority, not the implementation of the disposal actions authorised by the authority. This topic is not about the General Disposal Authorities.
	21	Implementation of Disposal Decisions - Implementation of approved disposal decisions is an IM activity that should be carried out routinely by organisations. This topic is about the implementation of disposal decisions, whether from organisation-specific disposal authorities or the General Disposal Authorities.
	22	Transfer to Archives New Zealand - Information of archival value, both physical or digital, should be regularly transferred to Archives New Zealand or a deferral of transfer should be put in place. As part of the transfer process, the access status of the information must be determined as either “open access” or “restricted access”.

Appendix 3

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

Organisation name	Response
Accident Compensation Corporation	Complete
AgResearch Limited*	**No response**
Airways Corporation of New Zealand Limited	Complete
Animal Control Products Limited	Complete
Ara Institute of Canterbury Limited	Incomplete
Arts Council of New Zealand Toi Aotearoa	Complete
Ashburton District Council	Complete
AsureQuality Limited*	**No response**
Auckland Council	Complete
Auckland District Health Board	Complete
Auckland University of Technology	Complete
Bay of Plenty District Health Board	Complete
Bay of Plenty Regional Council	Complete
Broadcasting Commission	Complete
Broadcasting Standards Authority	Complete
Buller District Council	No response
Callaghan Innovation	No response
Canterbury District Health Board / West Coast District Health Board	Complete
Canterbury Regional Council	Complete
Capital and Coast District Health Board	Complete
Carterton District Council	No response
Central Hawke's Bay District Council	Complete
Central Otago District Council	Complete
Chatham Islands Council	No response
Children's Commissioner	Complete
Christchurch City Council	Complete
Civil Aviation Authority	Complete
Classification Office	Complete
Climate Change Commission	Complete
Clutha District Council	Complete
Commerce Commission New Zealand	Complete
Commercial Fisheries Services	Complete

Organisation name	Response
Controller and Auditor-General	Complete
Counties Manukau District Health Board	Complete
Courts of New Zealand	Complete
Criminal Cases Review Commission	Complete
Crown Irrigation Investments Limited	Complete
Crown Law Office	Complete
Department of Conservation	No response
Department of Corrections	Complete
Department of Internal Affairs	Complete
Department of the Prime Minister and Cabinet	Complete
Drug Free Sport New Zealand	Complete
Dunedin City Council	Complete
Earthquake Commission	Complete
Eastern Institute of Technology Limited	Complete
Education New Zealand	Complete
Education Review Office	Complete
Electoral Commission	Complete
Electricity Authority	Complete
Energy Efficiency and Conservation Authority	Complete
Environment Southland Regional Council	Complete
Environmental Protection Authority	Complete
External Reporting Board	Complete
Far North District Council	Complete
Financial Markets Authority	Complete
Fire and Emergency New Zealand	Complete
Game Animal Council	Complete
Gisborne District Council	Complete
Gore District Council	No response
Government Communications Security Bureau	Complete
Government Superannuation Fund Authority	Complete
Greater Wellington Regional Council	Complete
Grey District Council	Complete
Guardians of New Zealand Superannuation	Complete
Hamilton City Council	Complete
Hastings District Council	No response

Organisation name	Response
Hauraki District Council	Complete
Hawke's Bay District Health Board	Late response
Hawke's Bay Regional Council	Complete
Health and Disability Commissioner	Complete
Health Promotion Agency	Complete
Health Quality and Safety Commission	No response
Health Research Council of New Zealand	Complete
Heritage New Zealand Pouhere Taonga	Complete
Horizons Regional Council	Complete
Horowhenua District council	Late response
Human Rights Commission	Complete
Hurunui District Council	No response
Hutt City Council	No response
Hutt District Health Board	Complete
Independent Police Conduct Authority	Complete
Inland Revenue Department	Complete
Institute of Environmental Science and Research Limited	Complete
Institute of Geological and Nuclear Sciences Limited	Complete
International Accreditation New Zealand	Complete
Invercargill City Council	No response
Judicial Conduct Commissioner	No response
Kaikōura 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 / New Zealand Railways Corporation	Complete
Kordia Group Limited	Complete
Lakes District Health Board	Complete
Land Information New Zealand	Complete
Landcare Research New Zealand Limited	Complete
Landcorp Farming Limited	Complete
Law Commission	Complete
Lincoln University	Complete
Mackenzie District Council	Complete

Organisation name	Response
Manawatu District Council	Complete
Manukau Institute of Technology Limited	Complete
Maritime New Zealand	Complete
Marlborough District Council	No response
Massey University	Complete
Masterton District Council	Complete
Matamata-Piako District Council	Complete
Meteorological Service of New Zealand Limited	Complete
MidCentral District Health Board	Complete
Ministry for Culture and Heritage	Complete
Ministry for Pacific Peoples	Complete
Ministry for Primary Industries	Complete
Ministry for the Environment	Complete
Ministry for Women	Complete
Ministry of Business, Innovation and Employment	Complete
Ministry of Defence	Complete
Ministry of Education	Complete
Ministry of Health	Complete
Ministry of Housing and Urban Development	Complete
Ministry of Justice	Complete
Ministry of Māori Development	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	Complete
National Pacific Radio Trust*	No response
Nelson City Council	Complete
Nelson Marlborough District Health Board	Complete
Nelson Marlborough Institute of Technology Limited	Complete
Netsafe Incorporated	Complete
New Plymouth District Council	Complete
New Zealand Antarctic Institute	Complete
New Zealand Artificial Limb Service	Complete
New Zealand Blood and Organ Service	Complete

Organisation name	Response
New Zealand Customs Service	Complete
New Zealand Defence Force	Complete
New Zealand Film Commission	Complete
New Zealand Fish and Game Council	Complete
New Zealand Green Investment Finance Limited	Complete
New Zealand Growth Capital Partners Limited	Complete
New Zealand Infrastructure Commission	Complete
New Zealand Lotteries Commission	Complete
New Zealand Ministry of Foreign Affairs & Trade	Complete
New Zealand Parole Board	No response
New Zealand Police	Complete
New Zealand Post Limited	Complete
New Zealand Productivity Commission	Complete
New Zealand Qualifications Authority	Late response
New Zealand Security Intelligence Service	Complete
New Zealand Symphony Orchestra*	**No response**
New Zealand Tourism Board	Complete
New Zealand Trade and Enterprise	Complete
New Zealand Transport Agency	Complete
New Zealand Walking Access Commission	No response
Northland District Health Board	Complete
Northland Polytechnic Limited	Complete
Northland Regional Council	Complete
Office for Māori Crown Relations - Te Arawhiti	Complete
Office of the Clerk of the House of Representatives	Complete
Office of the Ombudsman	Complete
Open Polytechnic of New Zealand	Complete
Opotiki District Council	No response
Oranga Tamariki - Ministry for Children	Complete
Otago Polytechnic Limited	Complete
Otago Regional Council	Complete
Otorohanga District Council	No response
Palmerston North City Council	No response
Parliamentary Commissioner for the Environment	Late response
Parliamentary Counsel Office	Complete

Organisation name	Response
Parliamentary Service	Complete
Pharmaceutical Management Agency	Complete
Pike River Recovery Agency	Complete
Porirua City Council	Complete
Privacy Commissioner	Complete
Public Service Commission	Complete
Public Trust	Complete
Queenstown-Lakes District Council	Complete
Quotable Value Limited	Complete
Radio New Zealand Limited	Complete
Rangitikei District Council	Complete
Real Estate Agents Authority	Complete
Reserve Bank of New Zealand	Complete
Retirement Commissioner*	**No response**
Rotorua Lakes Council	No response
Ruapehu District Council	Complete
SCION	Complete
Selwyn District Council	Incomplete
Serious Fraud Office	No response
Social Workers Registration Board	Complete
South Canterbury District Health Board	No response
South Taranaki District Council	Incomplete
South Waikato District Council	Complete
South Wairarapa District Council	Complete
Southern District Health Board	Complete
Southern Institute of Technology Limited	Complete
Southland District Council	Complete
Sport and Recreation New Zealand	Complete
Statistics New Zealand	Complete
Stratford District Council	Complete
Tai Poutini Polytechnic Limited	Complete
Tairāwhiti District Health Board	Complete
Takeovers Panel	Complete
Taranaki District Health Board	Complete
Taranaki Regional Council	No response

Organisation name	Response
Tararua District Council	Complete
Tasman District Council	Complete
Taupō District Council	Complete
Tauranga City Council	Complete
Te Māngai Pāho - Māori Broadcasting Funding Agency	Complete
Te Pūkenga - New Zealand Institute of Skills and Technology	Complete
Te Taura Whiri i Te Reo Māori	Complete
Te Wānanga o Aotearoa	Complete
Te Wānanga o Raukawa	No response
Te Whare Wānanga o Awanuiārangi	Complete
Television New Zealand Limited	No response
Tertiary Education Commission	Complete
Thames-Coromandel District Council	Complete
The Māori Trustee	Complete
The New Zealand Institute for Plant and Food Research Limited	Complete
The Treasury / New Zealand Government Property Corporation	Complete
Timaru District Council	Complete
Toi-Ohomai Institute of Techology Limited	Complete
Transport Accident Investigation Commission	Complete
Transpower New Zealand Limited	Complete
Unitec Institute of Technology Limited	Complete
Universal College of Learning Limited	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 District Council	Complete
Waikato District Health Board	Incomplete
Waikato Institute of Technology Limited	Complete
Waikato Regional Council	Complete
Waimakariri District Council	Complete
Waimate District Council	Complete
Waipa District Council	No response

Organisation name	Response
Wairarapa District Health Board	Complete
Wairoa District Council	Complete
Waitaki District Council	Late response
Waitemata District Health Board	Complete
Waitomo District Council	Complete
Wellington City Council	Complete
Wellington Institute of Technology Limited / Whitireia Community Polytechnic Limited	Complete
West Coast Regional Council*	**No response**
Western Bay of Plenty District Council	Complete
Western Institute of Technology at Taranaki Limited	Complete
Westland District Council	Complete
Whakatāne District Council	Complete
Whanganui District Council	Complete
Whanganui District Health Board	Complete
Whangarei District Council	Complete
WorkSafe New Zealand	Complete

We acknowledge that the highlighted organisations in the above table pro actively engaged with us following the closure of the survey. We thank them for their responses and good will.

Note: In the 2019/20 Survey Findings Report Te Pūkenga - New Zealand Institute of Skills and Technology was identified as no response in error. NZIST did not in fact receive a survey.

Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

archives.govt.nz