Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND

FINDINGS REPORT

Survey of public sector information management 2021/22

Te Kāwanatanga o Aotearoa
New Zealand Government

Contents

Overview – Survey

Te Rua Mahara uses monitoring as a key regulatory tool to assess the management of public sector information. Monitoring is critical for maintaining confidence in the quality of the stewardship of information and encouraging public organisations to ensure they are meeting the requirements of the Public Records Act 2005 (PRA), standards and good practice information management (IM).

One of the core mechanisms Te Rua Mahara uses to collect information for monitoring is through the Survey of public sector information management. This survey is part of our Monitoring Framework, which guides our monitoring activities and outputs.

Why do we survey?

Te Rua Mahara conducts this survey so we can better:

Understand how public sector organisations are performing against the requirements of the PRA, standards and good practice IM.

Track improvements in 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' IM performance.

What did we ask?

The survey questionnaire (Appendix 1) focused on:

Monitoring criteria

- based on the monitoring criteria from the Information Management Maturity Assessment (see Appendix 2 for topic summaries)
- repeated across annual surveys

Risks, challenges, opportunities, and emerging trends

- related to understanding the elements affecting IM in organisations
- designed to help us be a more responsive regulator
- may change across annual surveys

Please note the survey questions for the 2018/19 survey varied from the standardised questions we developed for the 2019/20 survey and continue to use. Due to this discrepancy, many of our graphs omit response data from 2018/19.

Who did we survey?

In 2021/2022, the survey was sent to 226 public sector organisations, including:

- 148 Public Offices, which were required to respond by direction to report (section 31 of PRA)
- 78 Local Authorities, which were invited to respond.

We used the online survey tool, SurveyMonkey, to send the questionnaire to Public Offices and Local Authorities. The survey was available from 30 June to 21 July 2022. Executive Sponsors from organisations in scope were asked to coordinate their organisation's response.

We do not yet survey the full range of entities covered by the PRA. To be consistent with previous years, we did not survey school boards, reserves boards, fish and game councils, Ministers of the Crown or council-controlled organisations in 2021/22. We also sought to reflect organisational change.

District health boards (DHBs) ceased to have a separate existence on 30 June 2022 and were not included in the survey. Te Whatu Ora Health New Zealand was not included in the survey because establishment activities, including records and IM system transfers were still underway in the survey period, precluding an accurate survey response for the new organisation.

In the skills and training sector, some polytechnics were to retain their separate existence until late in 2022, but others had already been merged into Te Pūkenga – New Zealand Institute of Skills and Technology by the time of the survey. We chose to set a baseline for Te Pūkenga by including it in the survey but excluding the remaining separate polytechnics.

Who responded?

The 2021/22 survey recorded a 94% response rate. 13 organisations did not respond. Of the 13, two were Public Offices and 11 were Local Authorities. A list of respondents and non-respondents can be found in Appendix 3.

226 Organisations invited to respond

212 Valid responses recieved

13 Organisations did not respond

94% Response rate

Please note the responses from the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS) are excluded from the analysis due to security reasons. The findings in this report therefore represent 210 responses, not the 212 valid responses received.

Additionally, we permitted some organisations to submit combined responses, such as when organisations share an Executive Sponsor and/or IM staff or systems. For the purposes of calculating response rates, these responses were counted as a single Public Office or Local Authority.

What did we find?

This section of the report will provide detailed findings and analysis from the 2021/22 survey. Findings and analyses will be separated into five areas:

1. Key indicators

- examines performance over time and measures the overall state of public sector IM

2. Governance, capability and self-monitoring

- the people component of IM

3. Creation and management

- activities that support the core requirements mandated by the PRA

4. Disposal

- IM activities that enable the disposal of public sector information when it is no longer required by an organisation

5. IM environment

- risks, challenges, opportunities and emerging trends that are affecting IM in organisations

Survey questions and response data from 2021/22 can be found in Appendix 1. The full dataset will be published on www.data.govt.nz. Much of the commentary and analysis in this report has been repeated from the 2020/21 report where the issues are unchanged.

Next steps and developments

The 2021/22 Chief Archivist's Report on the State of Government Recordkeeping includes information on the next steps Te Rua Mahara plans to take in response to these survey findings.

1. Key indicators

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 key indicators to measure the overall state of public sector IM. The key indicators are based on single survey questions or groups of questions. They provide a high-level perspective on whether IM is improving, deteriorating or remaining stable. They focus on:

- implementing governance groups for information management
- overall number of IM staff employed by public sector organisations
- identifying high-value and/or high-risk information
- building IM requirements into new business systems
- 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.

INDICATOR 1

Implementing governance groups for information management

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

- *Has IM oversight as part of its mandate*
- *Is dedicated to IM*
- *Neither of the above*

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

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

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 administrative head and senior leadership team
- involve staff with IM expertise and facilitate partnership between IM and related business activities, such as ICT, privacy, security and data management
- have the authority to plan, direct and allocate funding to IM.

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

Survey findings

61% of organisations responded they have a formal governance group. This number includes groups dedicated to IM and groups that have an IM component. 48% reported their governance group has IM oversight as part of its mandate. 13% reported their governance group is dedicated to IM. Most governance groups meet at least twice a year (93%). 84% of governance groups include an Executive Sponsor.

In comparison, the 2020/21 survey showed 60% of organisations reported having a governance group in place, 93% of governance groups met at least twice a year and 91% of groups included an Executive Sponsor. Figure 1 shows the type of governance groups in place across recent surveys.

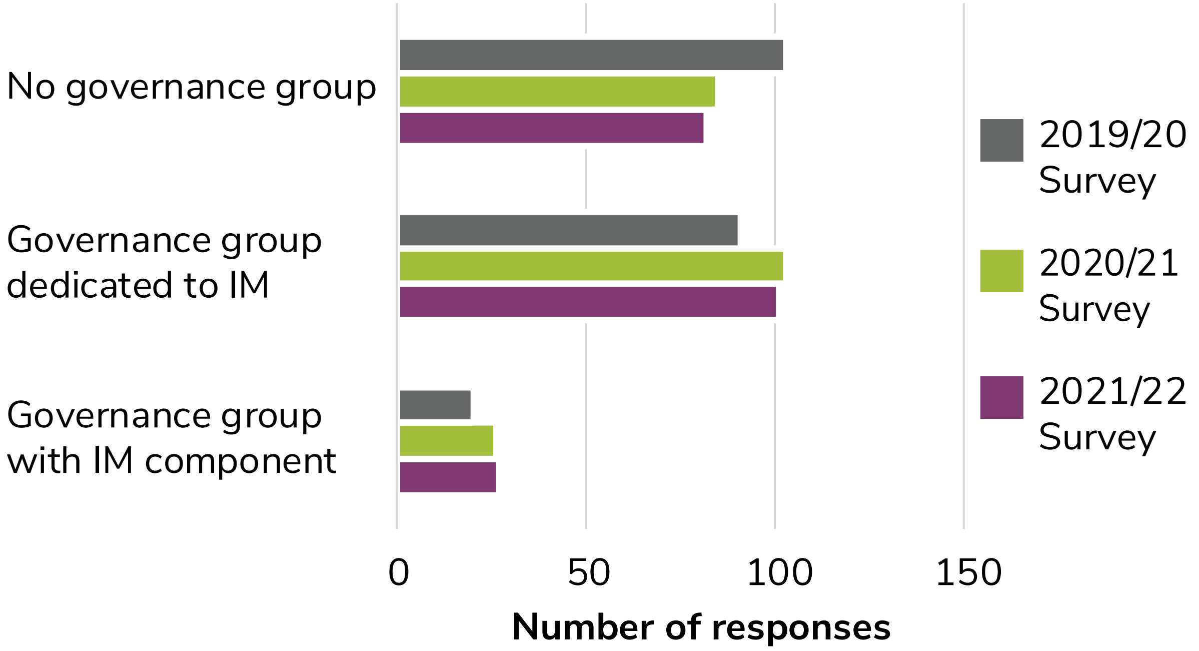

Figure 1: Type of IM governance groups

The survey data indicates Local Authority respondents are less likely to have a formal governance group in place than Public Offices (Figure 2).

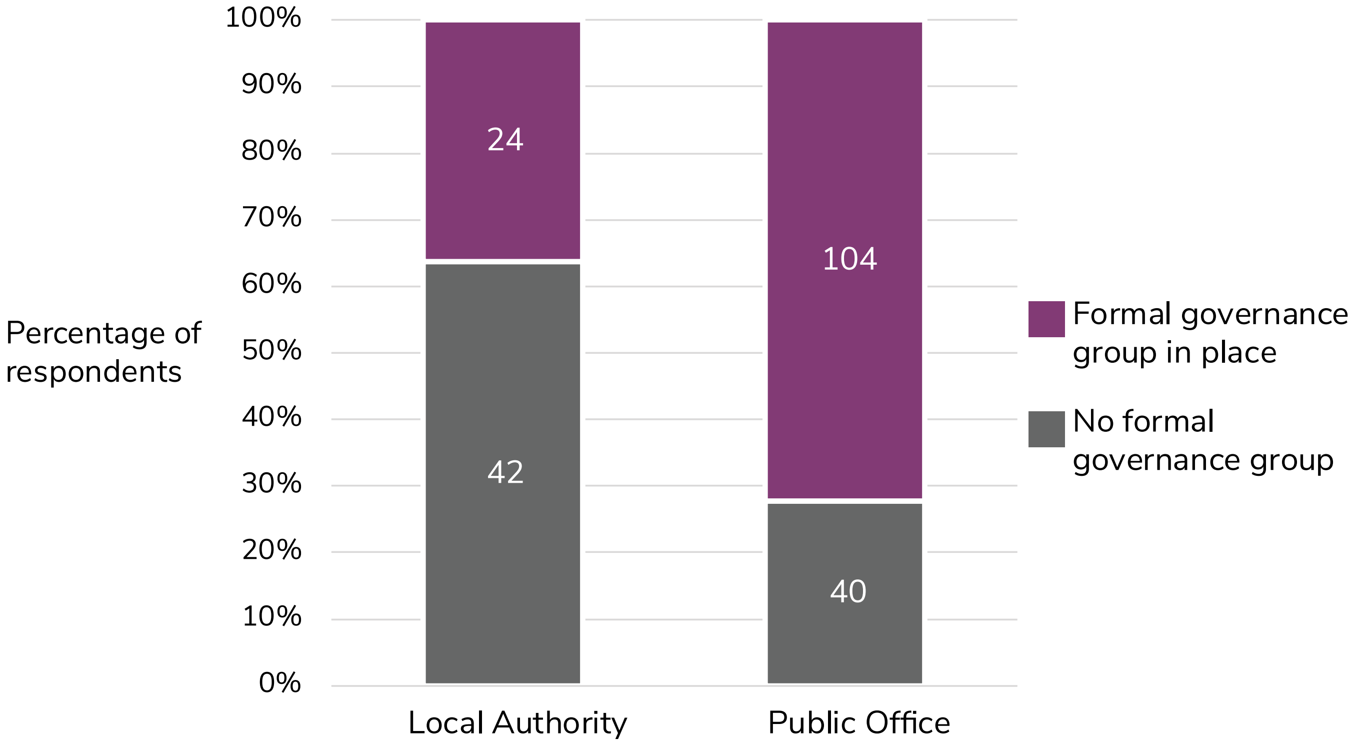

Figure 2: Proportion of total responses

INDICATOR 2

Overall number of IM staff employed by public sector organisations

Q16. How many full-time-equivalent (FTEs) are dedicated IM staff?

We asked how many dedicated, full-time equivalent (FTE) IM staff organisations employed (Q.16). 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, such as business support.

The Information and records management standard (the Standard) requires: 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.

Survey findings

Survey data from the last four years show the number of IM staff in responding public sector organisations is increasing (Figure 3). Note: When we first asked this question in the 2018/19 survey, we had survey respondents select from a numerical range of IM FTEs. From 2019 onward, we asked respondents to provide an exact number of IM staff.

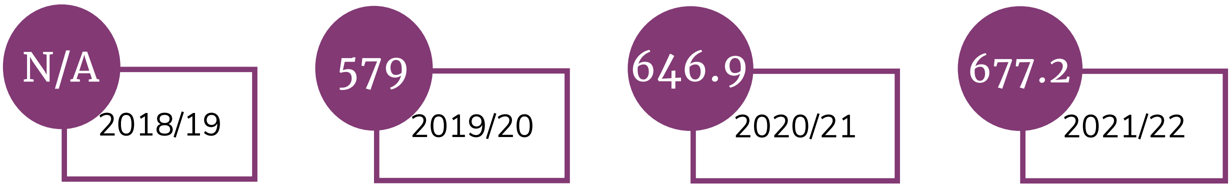

Figure 3: Total IM FTEs employed by public sector organizations[1]

77% of respondents have some dedicated, specialised IM resources. Figure 4 shows the number of Local Authorities and Public Offices that have 'some' vs 'no' IM FTEs.

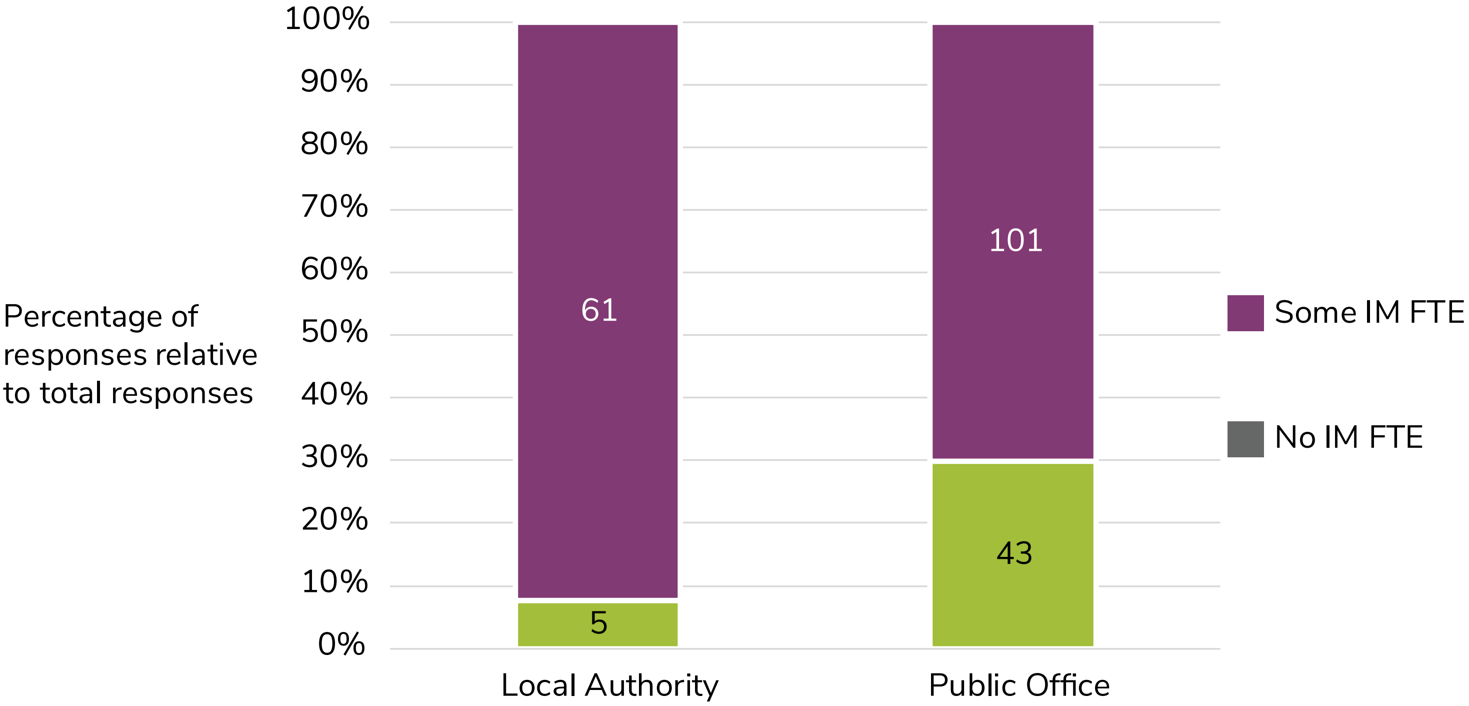

Figure 4: IM FTE compared to tier of government

[1] Data from 2018/19 is not plotted in Figure 3. The question was asked differently, with responding organisations selecting from a range rather than providing an exact number of FTEs.

The average number of IM staff across all organisations (including those with no IM staff) has increased to 3.2, compared to 3 in 2020/21[2]. Figure 5 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 purple) it is common to have no IM staff.

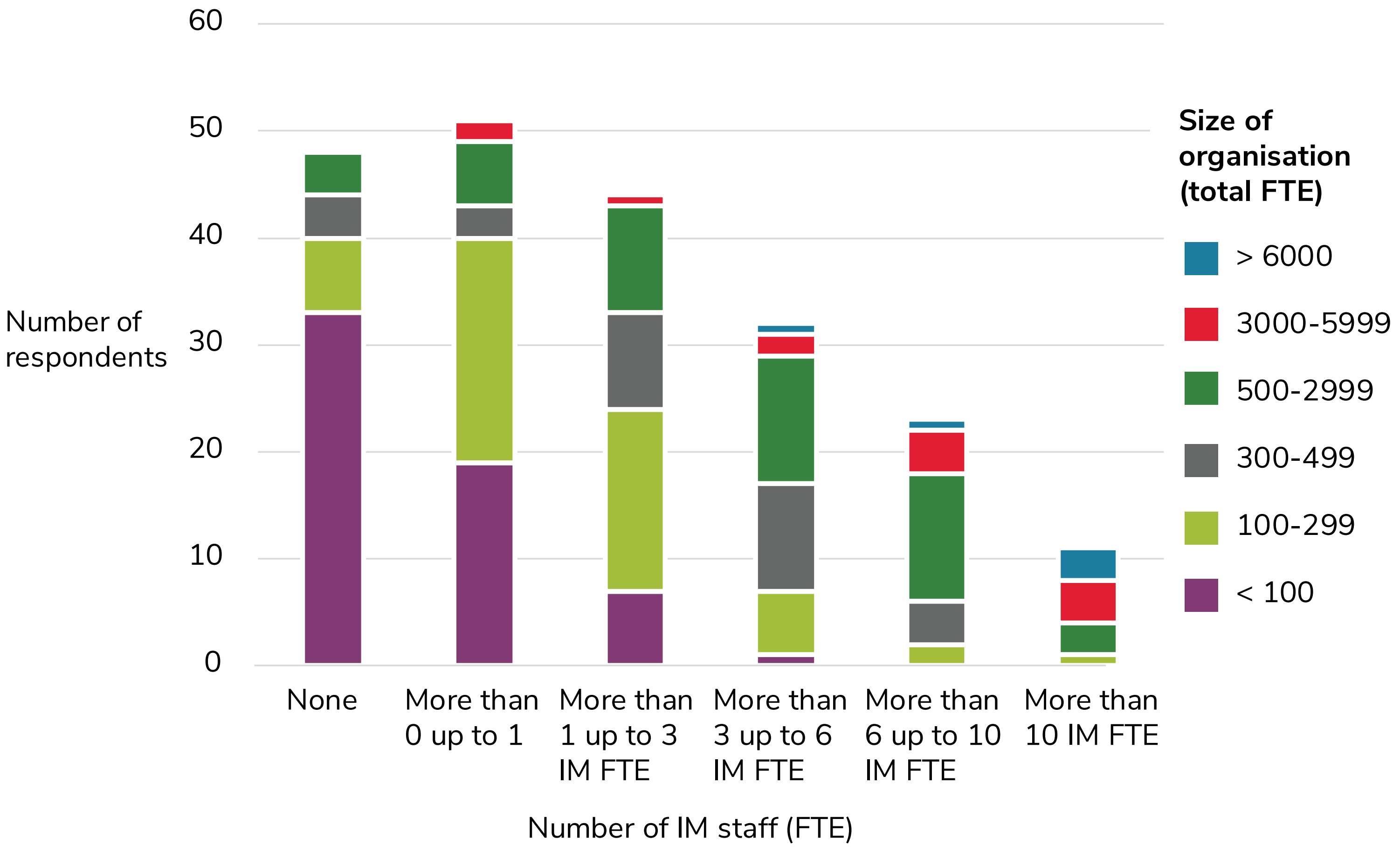

Figure 5: Number of IM FTEs compared to organisation size

[2] In the 2020/21 survey, responses that specified 'less than 0.5 FTE' were set to 0.25. We received no responses marked as 'less than 0.5 FTE' in 2021/22.

INDICATOR 3

Identifying high-value and/or high-risk information

Q20. Has your organisation identified its most important high value/high risk information?

We asked survey participants if they have identified their high-value and/or high-risk information (Q.20).

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.

Survey findings

Survey responses indicate that most organisations are working on identifying their high-value/high-risk information. 36% have identified their high-value/high-risk information. This number has stayed generally static across the last few surveys (Figure 6). There has been a slight increase every year of those reporting identification is 'in progress' (Figure 7). Note: The 2018/2019 survey (indicated by dashed line in Figure 6) did not offer an 'in progress' response option while subsequent surveys did. This likely explains the large decrease in 'yes' responses between the first and second surveys.

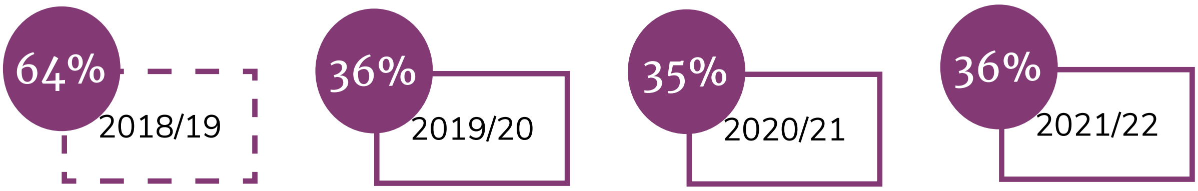

Figure 6: Percentage of organisations that have identified their high-value and/or high-risk information[3]

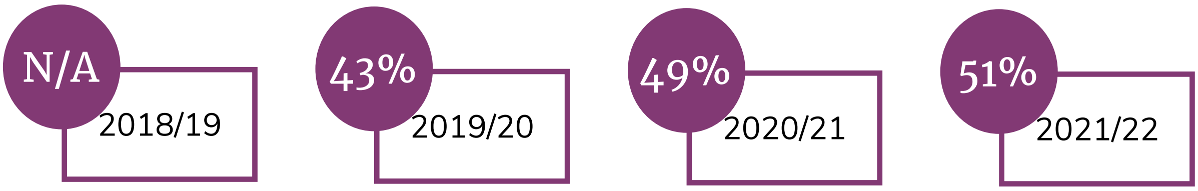

Figure 7: Percentage of organisations are 'in progress' of identifying their high-value and/or high-risk information

[3] 2018/19 survey responses include 'in progress' option.

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 (Figure 8). These responses are similar to 2020/21 survey data.

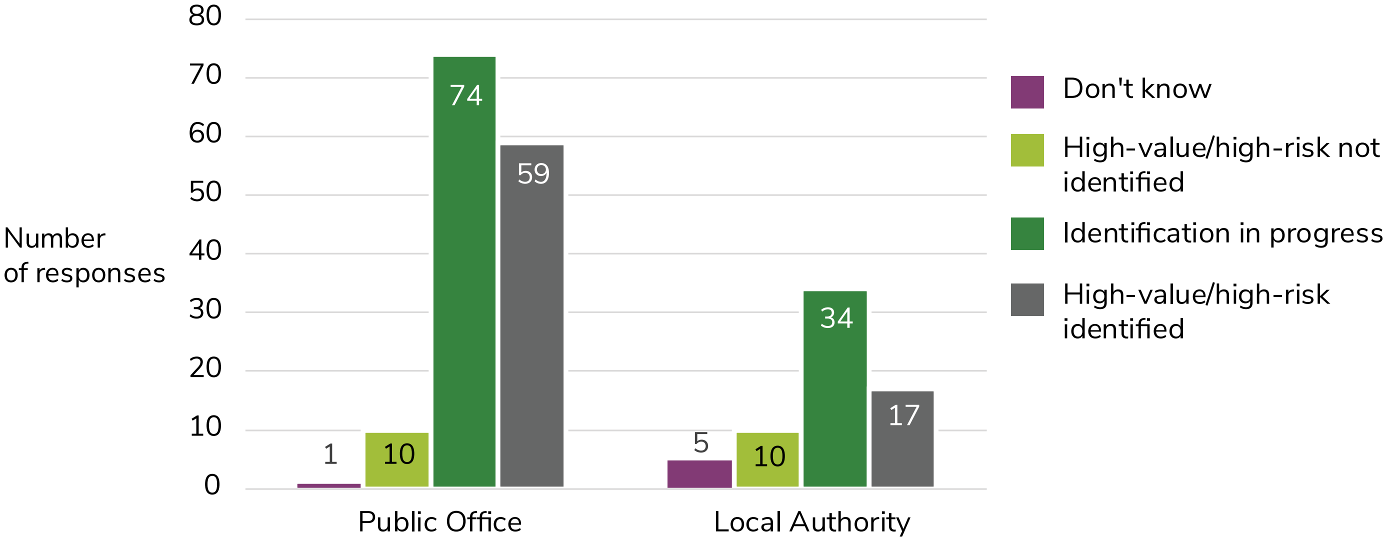

Figure 8: Identification of high-value/high-risk information compared to tier of government

There is a significant relationship between organisations identifying their high-value/high-risk information and identifying key risks associated with their information (Figure 9). These responses are similar to the 2020/21 year.

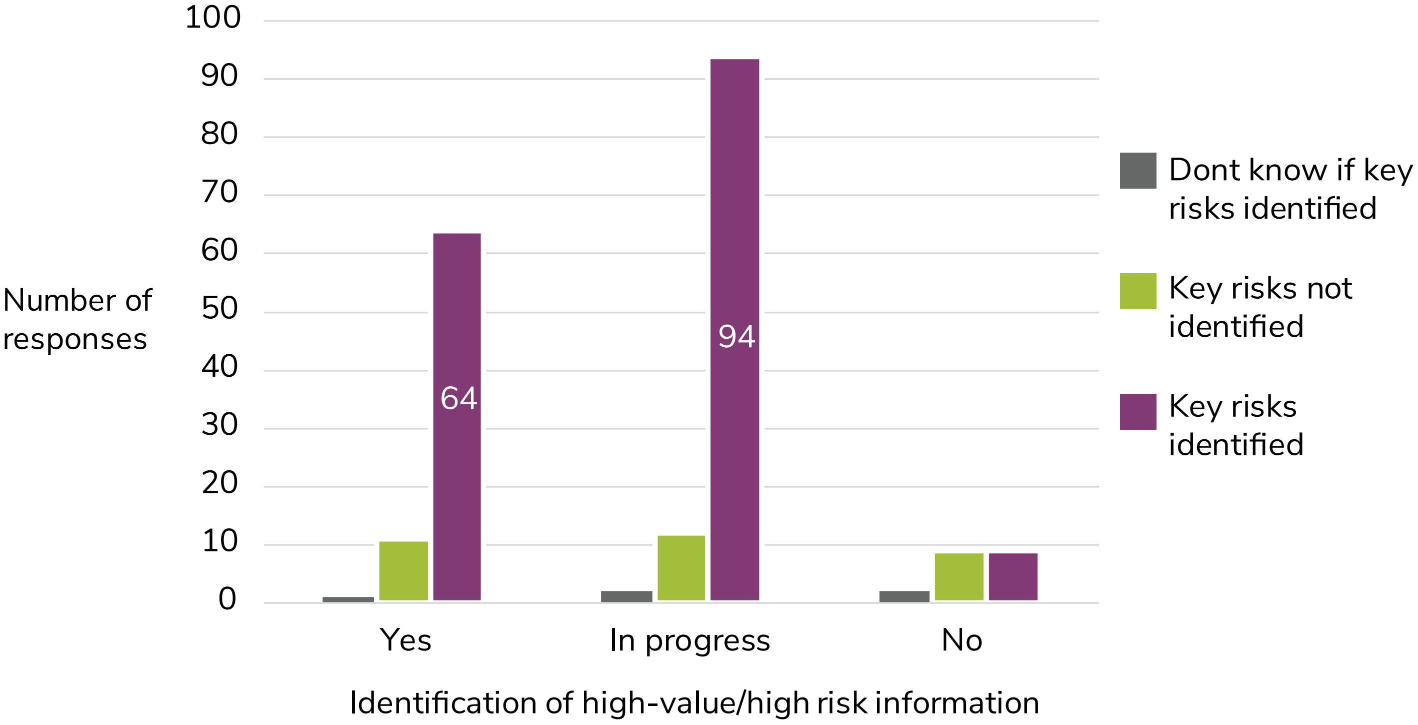

Figure 9: Identification of high-value/high-risk information compared to identification of key risks to information

INDICATOR 4

Building IM requirements into new business systems

Q25. In the last 12 months, has your organisation implemented any new business information system(s)?

Q26. Is a process for managing information through its lifecycle built into those new business information system(s)?

We asked survey participants whether they have built a process for managing information through its lifecycle into new business information systems (for example, systems implemented in the last 12 months) (Q.26).

The Standard requires: 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.

Survey findings

We surveyed respondents about whether they had implemented a new business information system in the last 12 months. If they had, we asked if they had built in the IM requirements for managing information through its lifecycle. 70% had reported implementing a new business information system in the last 12 months. Of those, 31% are Local Authorities and 69% are Public Offices.

Figure 10 shows the change in response data since 2019/20 survey results of those organisations that have, have not, or are not sure if they have fully or partially built IM requirements into new business systems. In 2021/22, 60% built in processes for managing information through its lifecycle, however 40% have not built in processes or 'don't know' whether they have built in IM requirements:

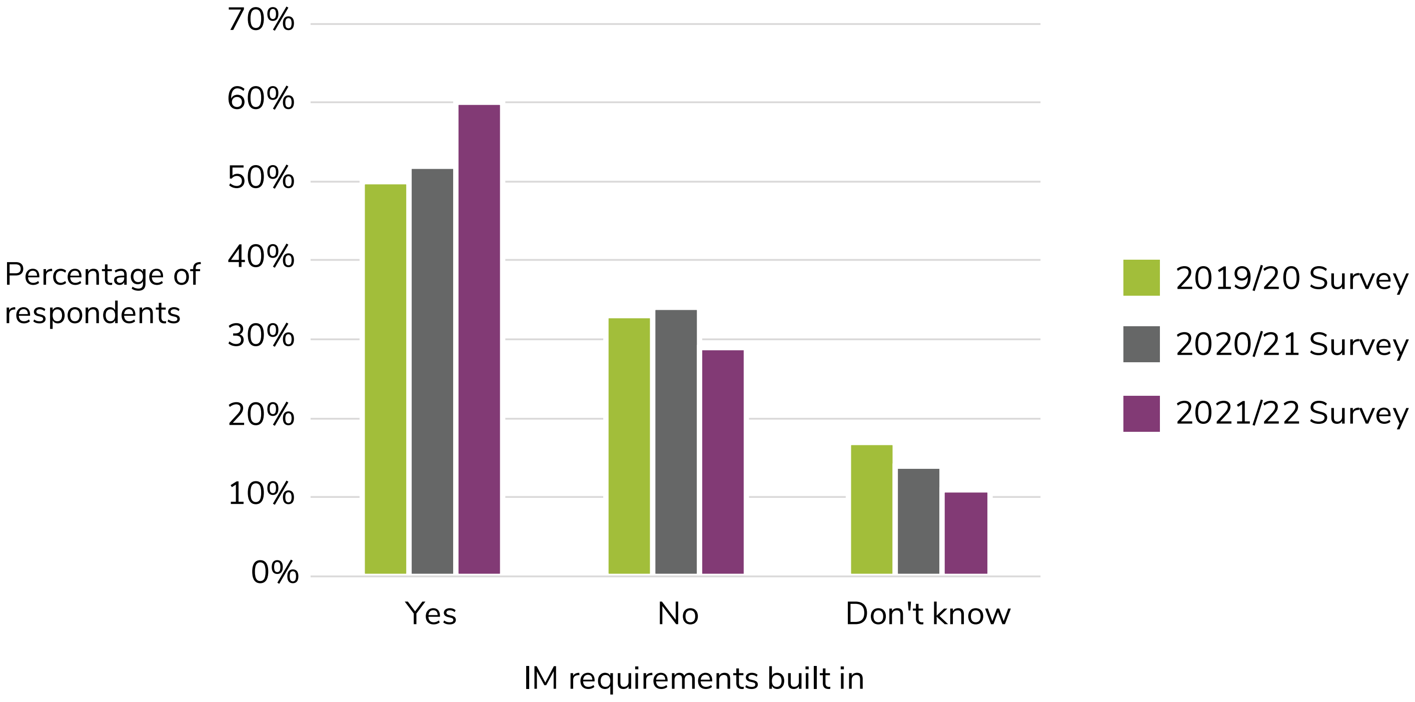

Figure 10: IM requirements built in (by year)[4]

[4] Data from 2018/19 is not plotted in Figure 10. The question was asked differently, with a 'partially' option provided.

When comparing the data against the presence of a formal governance group for IM, we found those organisations that have a formal governance group in place are more likely to build IM requirements into new business systems (Figure 11).

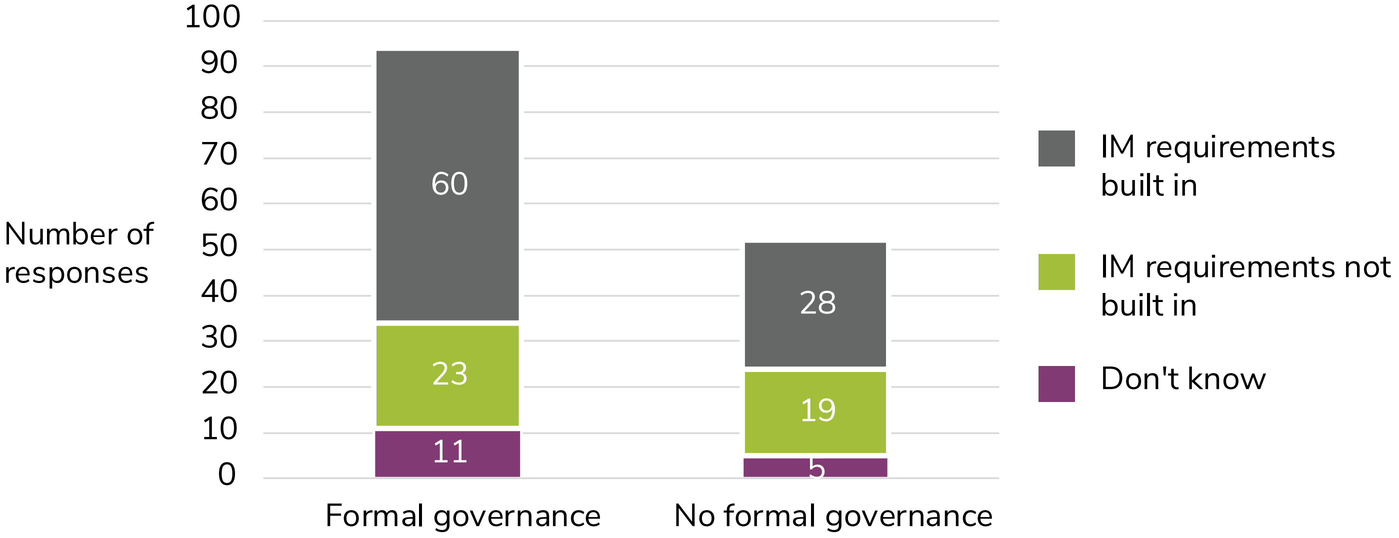

Figure 11: IM requirements built in compared to presence of formal governance group for IM

INDICATOR 5

Active, authorised destruction of information

Q40. In the last 12 months, has your organisation carried out authorised destruction of physical information?

Q41. In the last 12 months, has your organisation carried out authorised destruction of digital information?

We asked survey participants if they have carried out any authorised destruction of information in the past 12 months (Q.40 on physical information and Q.41 on digital information).

The Standard requires: 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 (for example, 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.

Survey findings

57% of respondents have done some form of destruction (that is, either physical or digital) compared to 56% in 2020/21. Figure 12 shows that the proportion of respondents who have destroyed physical information is much higher than digital information: 51% have destroyed physical, while only 34% have destroyed digital.

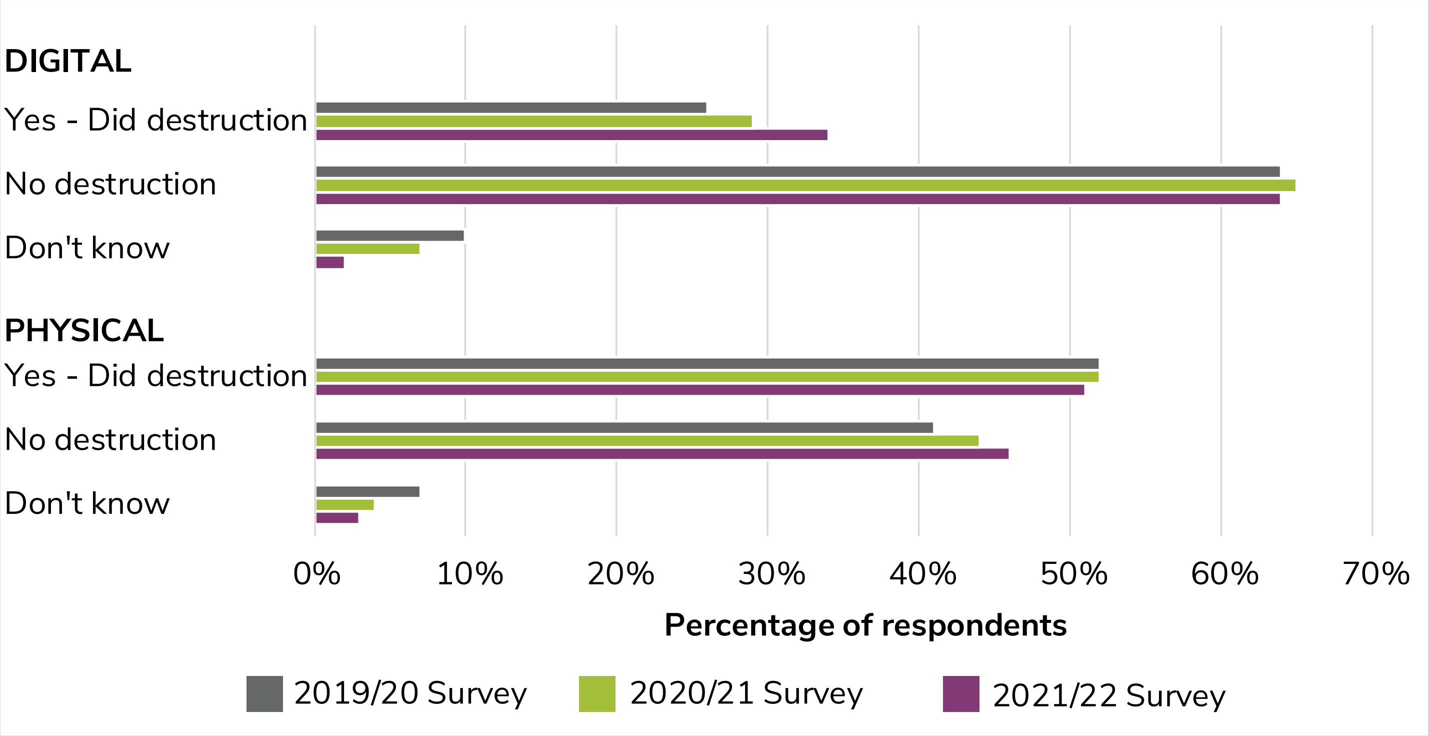

Figure 12: Authorised destruction over the last three surveys

Organisations that have done ‘no destruction’ has increased over the last four years of surveys (Figure 13).

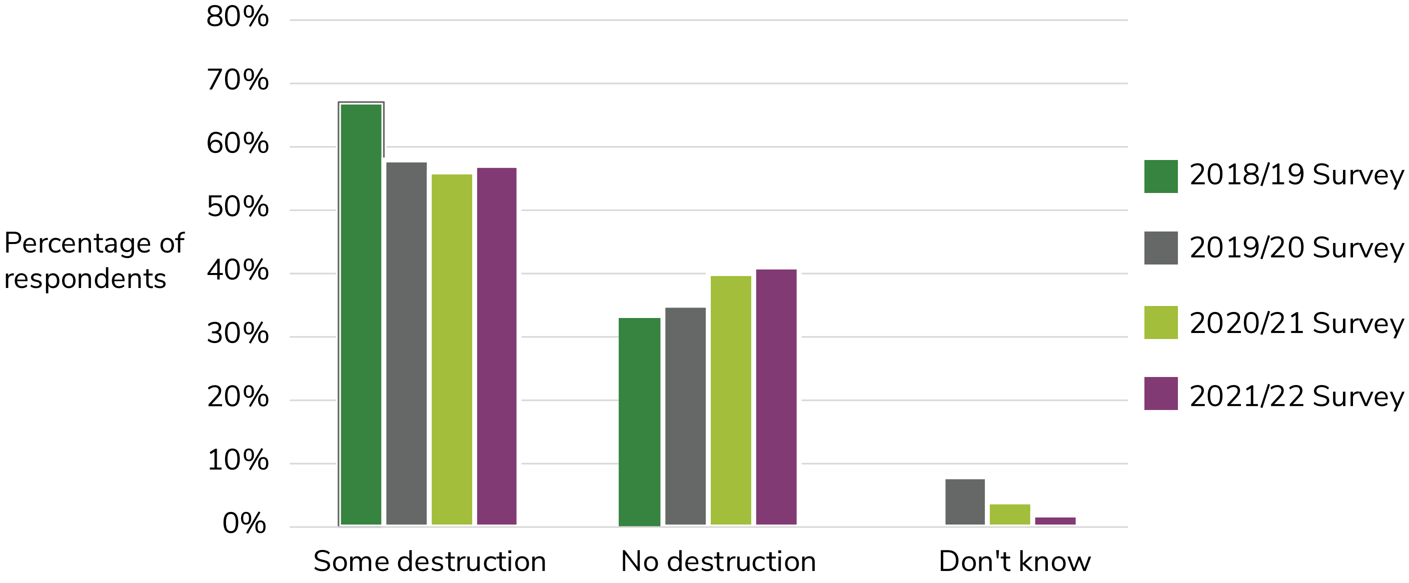

Figure 13: Percentage of organisations who have done authorised destruction (by year)

The data also shows authorised destruction of digital information is much lower than physical information (Figure 14) which is consistent with our previous survey findings.

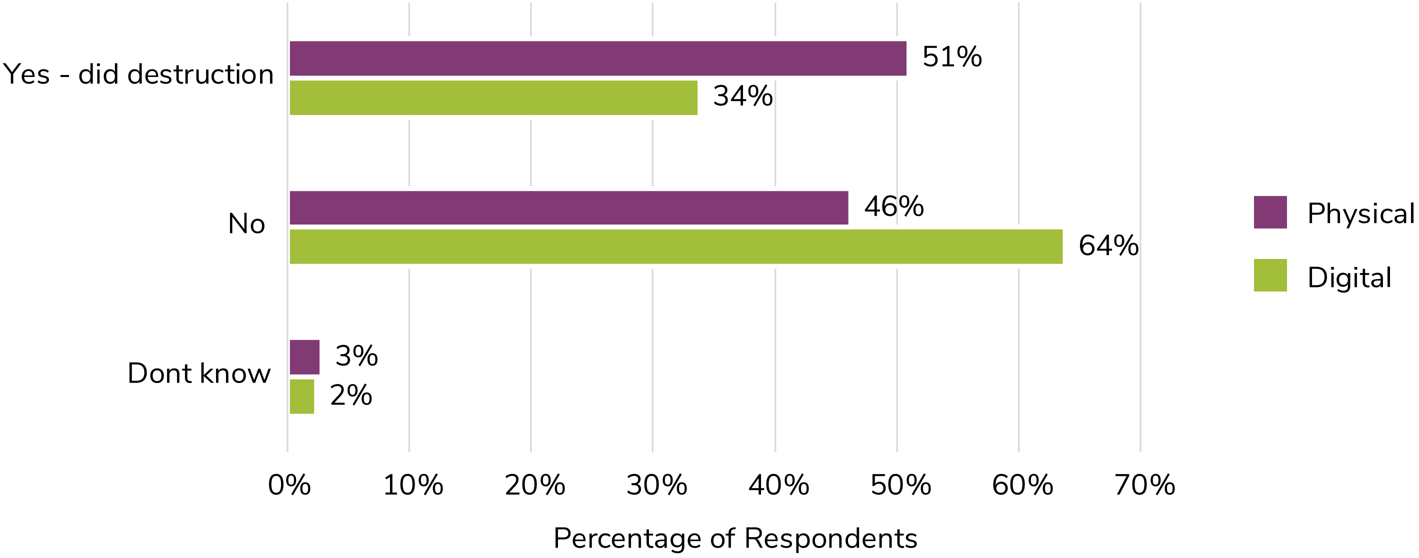

Figure 14: Authorised destruction by format in 2021/22

When separating the organisations by government tier, we found a higher proportion of Local Authorities did authorised destruction compared to Public Offices (Figure 15).

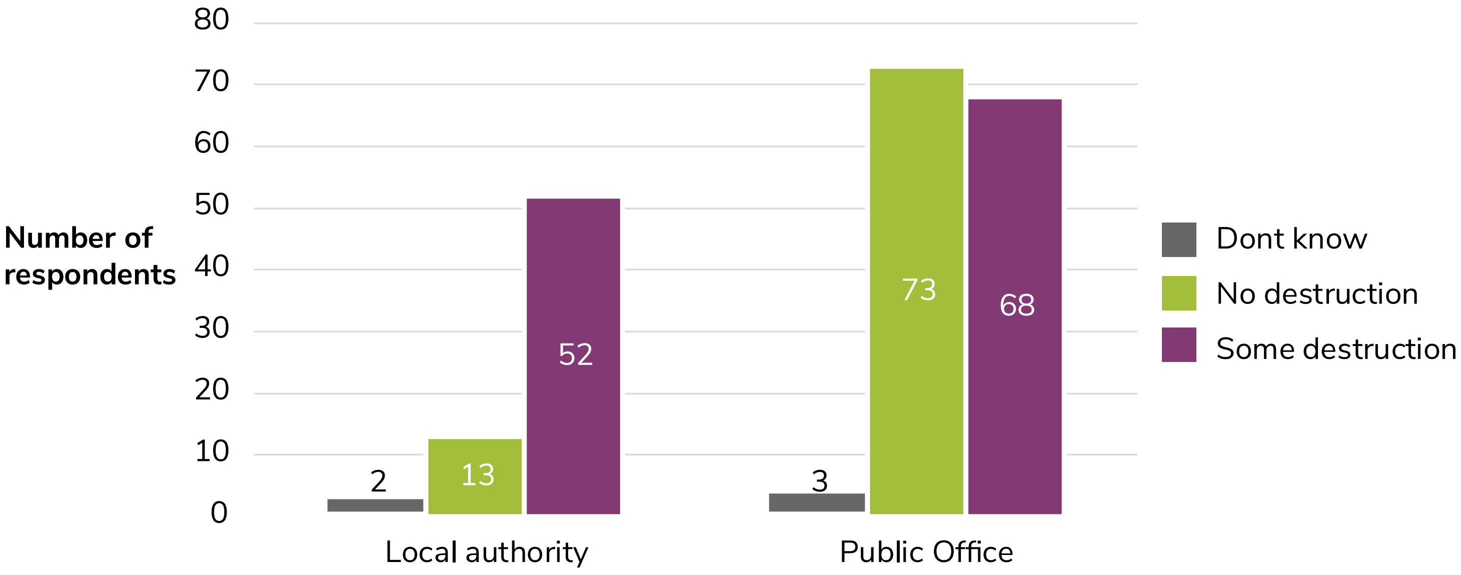

Figure 15: Authorised destruction compared to tier of government

The data also showed that proportionally the more IM FTE in place the greater the likelihood for destruction to occur (Figure 16).

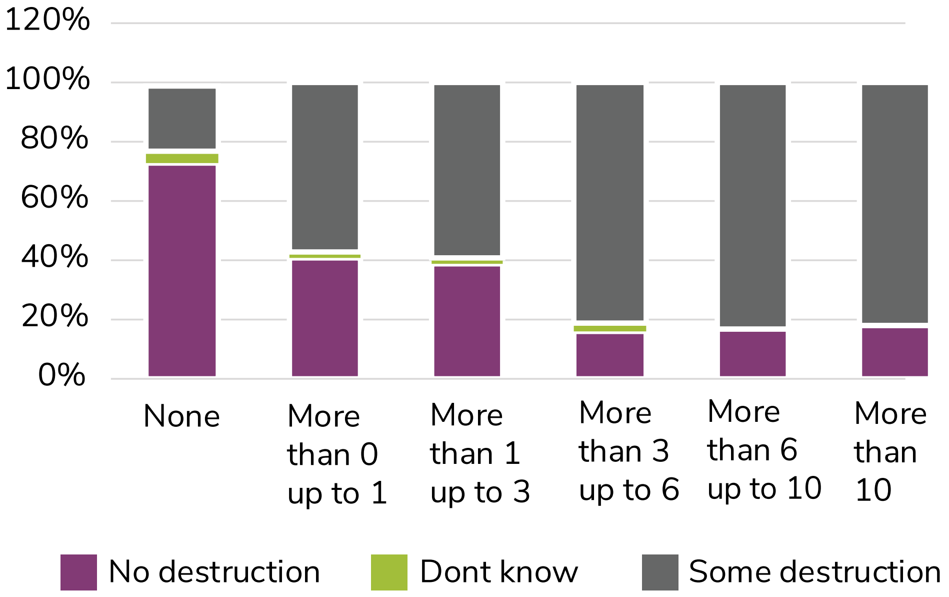

Figure 16: Authorised destruction compared to IM FTE

2. Governance, capability and self-monitoring

This section covers key findings and analysis of the people component of IM including:

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

Te Tiriti o Waitangi

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

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

Q11. Which of the following has your organisation done to improve the usage of information that is of importance to Māori?

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.

Survey findings

39% of respondents said they have identified information that is of importance to Māori, compared to 35% in 2020/21. However, despite the increase, respondents were still more likely to respond 'no' than 'yes' to identifying important information. Of those who responded yes, 42 respondents (51%) said that they had criteria or methodologies for assessing this. These included:

- reviewing, classifying and recording relevant information, including use of information (for example, cultural impact assessments)
- establishing relationships with iwi and making information easily accessible
- dedicated staff/teams or internal advisory groups to help identify and manage this information
- developing a Te Tiriti o Waitangi partnership group
- abiding by established frameworks (for example, Ngā Tikanga Paihere, developed by Stats NZ Tatauranga Aotearoa).

We asked the 82 respondents who have identified information of importance to Māori about the activities they are doing to improve usage (Figure 17). Note: One respondent can choose more than one activity. 'Improving discoverability' was the most common activity, compared to 'improving access' in previous years. Other activities mentioned in the comments in addition to those listed in Figure 17, include:

- established formal commitments to Te Tiriti o Waitangi
- establishing Māori data governance frameworks
- having entities in partnership with Māori
- having specialised staff, teams and/or internal advisory groups.

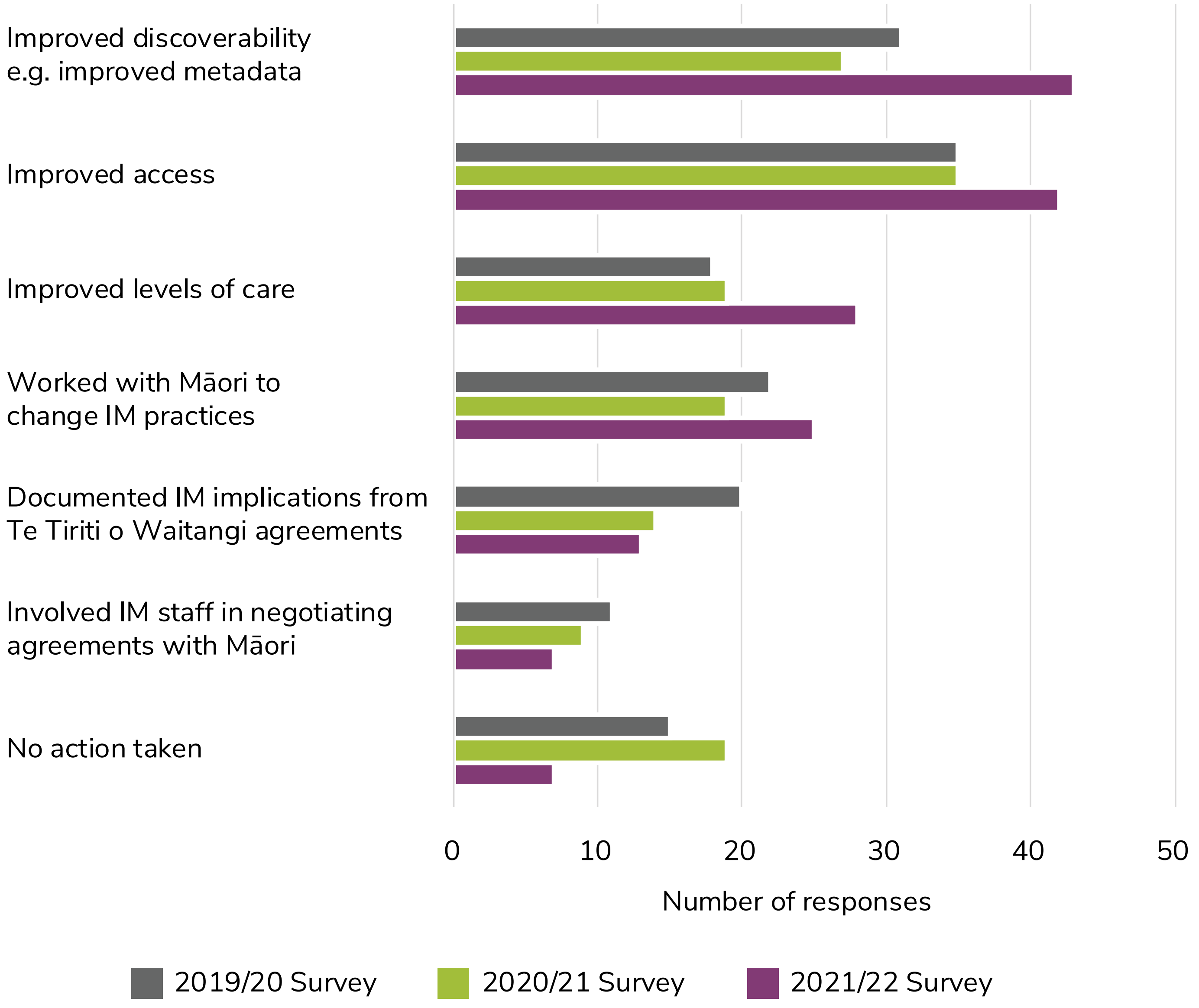

Figure 17: Activities to improve usage of information that is of importance to Māori

Self-monitoring

Q12. In the last 12 months, has your organisation done any self-monitoring of its compliance with:

- *Archives New Zealand's requirements*
- *This organisation's own IM policy*
- *Neither of these*

Q13. What method(s) were used for that self-monitoring?

- *Assessment by a third party*
- *Bench-marking exercise*
- *Internal audit*
- *Maturity assessment*
- *Review of processes*
- *Risk Assessment*

Q14. As a result of that self-monitoring, is your organisation developing or has it developed an action plan?

Q15. As a result of that self-monitoring, is your organisation implementing or implemented an action plan?

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.

Survey findings

84% percent of respondents said they have done self-monitoring in the last 12 months, compared to 76% in 2020/21. 69% have used Te Rua Mahara requirements to monitor, while 57% have used their own IM policy. A review of processes is once again the most common activity (65%) (Figure 18), followed by a maturity assessment (50%)[5] and internal audit (41%). Other activities mentioned in the comments in addition to those listed in Figure 18 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.

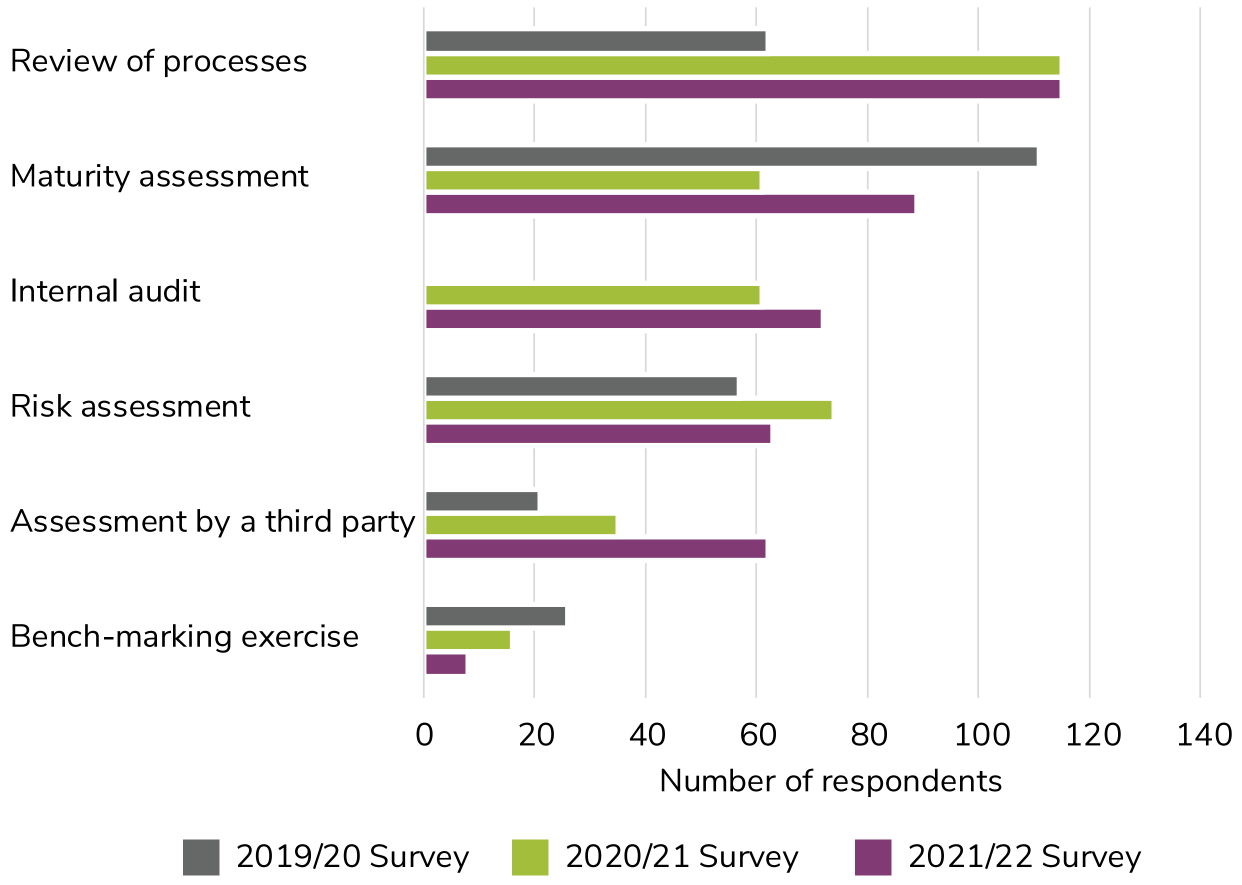

Figure 18: Methods used to self-monitor

[5] "Maturity assessment' option was not available for the 2019/20 survey.

In this year's survey 'steps taken as a result of self-monitoring' was split into two questions (refer to Appendix 1). Of the 177 respondents who have done self-monitoring in the last 12 months, 100 report they are focused on developing action plans and 50 are implementing an action plan (Figure 19). In 2020/21, 91 respondents reported developing action plans and 59 were implementing action plans. Please note 'Deferred development of an action plan' was added to the 2021/22 survey and 'Deferred implementation of action plan' was not available as an option for the 2019/20 survey.

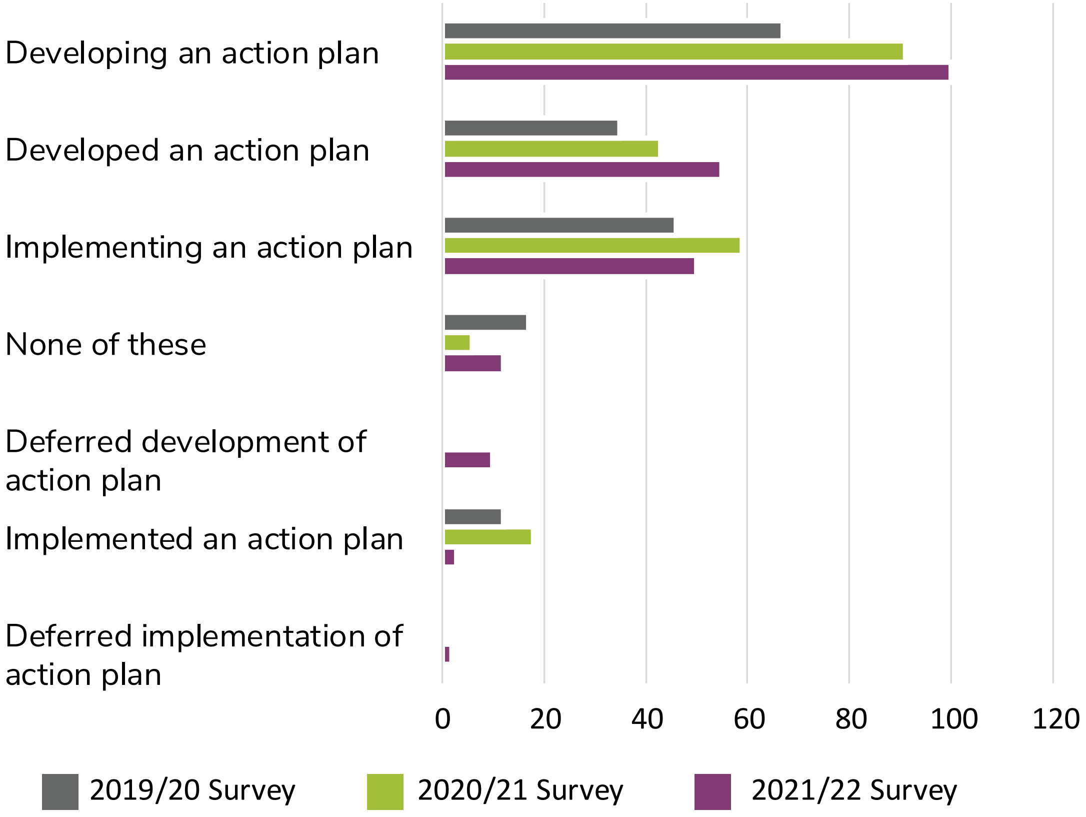

Figure 19: Actions taken as a result of self-monitoring

IM capability

Q16. How many full-time-equivalent (FTEs) are dedicated IM staff?

Q17. In the last 12 months, which of the following has any dedicated IM staff member(s) done?

- *Attended an IM conference (or similar event)*
- *Attended an IM training course (face-to-face and/or online)*
- *Had an IM-relevant secondment*
- *Presented at an IM conference (or similar event)*
- *Studied toward a recognised IM qualification*
- *None of these*

Q18. Which of the groups below does your organisation inform about their IM responsibilities?

- *Staff at all levels*
- *Contractors*
- *Consultants*
- *None of these*

Q19. In which way(s) are the groups that you ticked in the previous question informed about their IM responsibilities?

- *Code of Conduct*
- *Contracts*
- *Induction training*
- *Job descriptions*
- *Performance development plans/agreements*
- *Refresher training*
- *Don't know*
- *None of these*

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. We looked into the current status of IM staffing in the sector earlier in this report: Indicator 2, Overall number of IM staff employed by public sector organisations. 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 the information to perform their functions. 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.

Survey findings

The same proportion of employees participated in an IM professional development activity as compared to 2020/21 (81%). The most common activities were training courses and conference attendance, consistent with 2020/21 survey data (Figure 20).

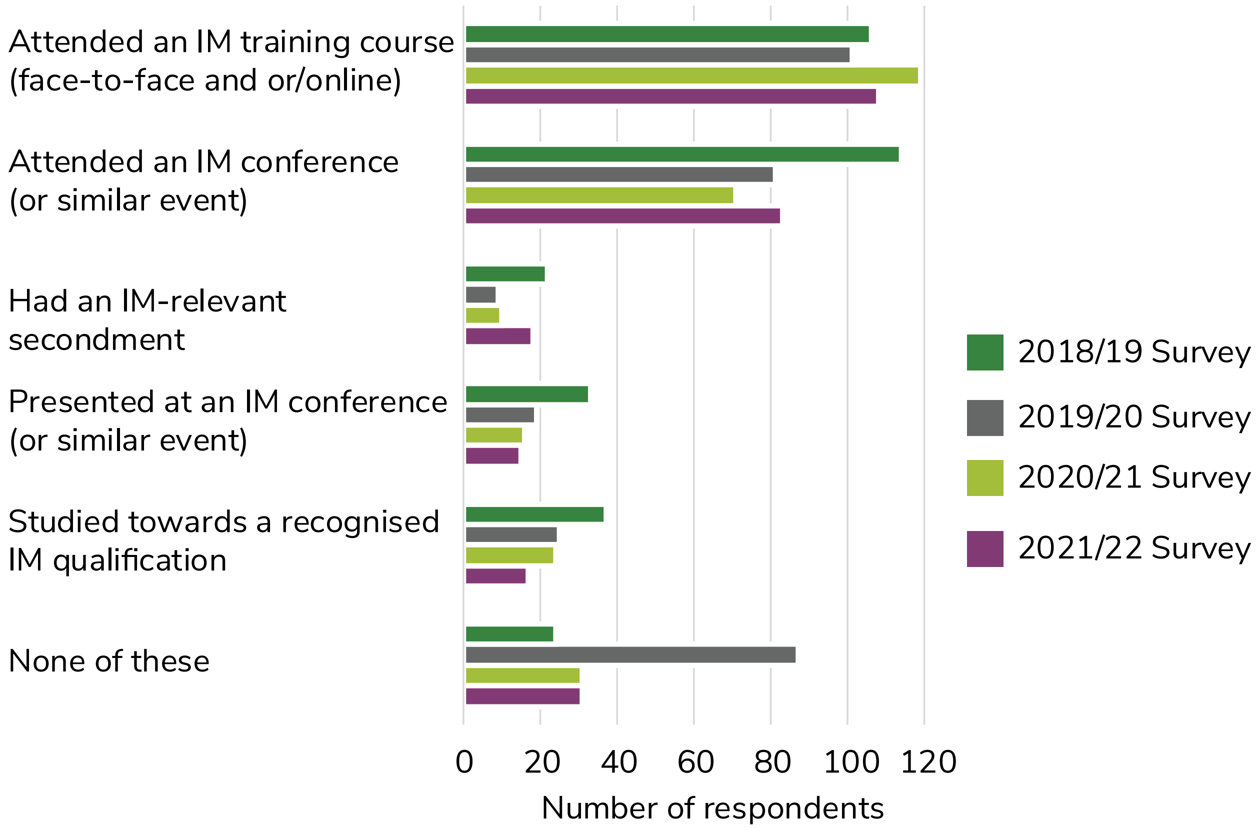

Figure 20: Professional development activities for IM staff

While most respondents indicated they inform staff at all levels of their IM responsibilities (95%) the rate is much lower for contractors (59%) and consultants (47%).

Once again, a high proportion of respondents said that they use induction training to communicate responsibilities (87%) while around half use refresher training, contracts and codes of conduct (Figure 21). Organisations also mentioned other activities in the comments in addition to those listed in Figure 21, including:

- employers read and sign documented policies and processes
- continuous internal communication, in person or online, for example, emails, intranet, newsletters, videos
- one-to-one meetings with IM staff to provide advice and support
- briefings at group meetings
- collaborating with other teams to establish online introductory guides.

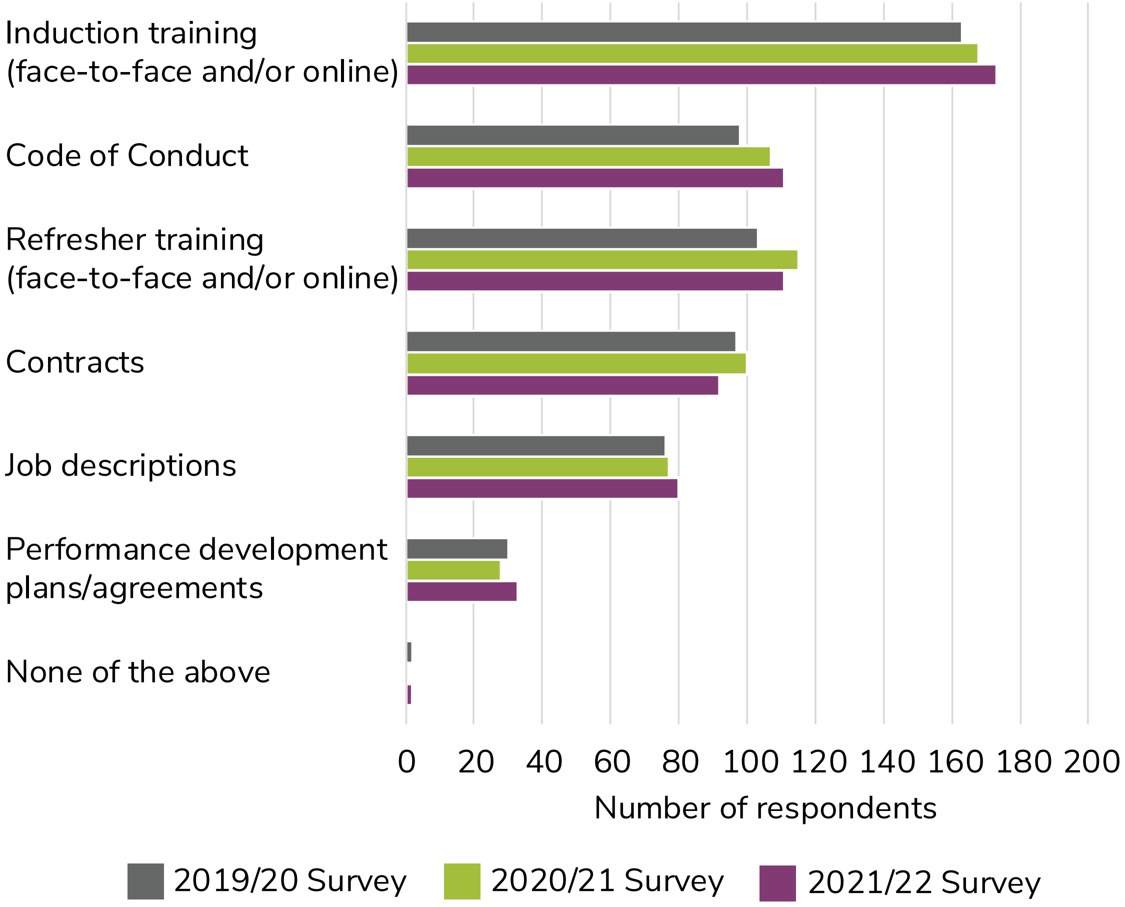

Figure 21: How organisations inform staff, contractors and consultants about their IM responsibilities

3. Creation and management

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

- create information
- maintain (or manage) information
- maintain information in accessible form.

Please note: Disposal is a component of managing information but as it is a large topic, we have addressed it in its own section.

High-value/high-risk information

Q20. Has your organisation identified its most important high value/high risk information?

Q21. In the last 12 months, in order to actively manage its high-value/high risk information, what action(s) has your organisation taken?

- *Developed information architecture and/or search tools*
- *Implemented a new business information system to mitigate risks to information*
- *Implemented back-up capability*
- *Redeveloped systems to improve long-term accessibility of information*
- *Tested its business continuity plan*
- *Don't know*

Q22. Does your organisation have an information asset register (or similar way of recording information assets)?

Q23. Is that register:

- *Up-to-date*
- *Being used*
- *Neither of these*

Q24. Is your organisation planning to have an information asset register (or similar)?

The reason we emphasise high-value/high-risk information in our standard, guidance and monitoring 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's perspective on what information is high-value/high-risk will be informed by its own organisational needs and those of 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.

Survey findings

We asked organisations whether they had an IAR and how they used it. In 2021/22, 28% had an IAR and 31% of respondents reported they were developing one. In 2020/21, 23% had an IAR and 32% were in development. There was an increase in updating IARs: 2020/21 data shows only 49% organisations surveyed had an 'up-to-date' IARs compared to 75% in 2021/22. However, there was a reported decrease in IARs 'being used': 74% in 2020/21 to 64% in 2021/22.

IARs 2021/22:

- 27% do not have an IAR
- 60% have or are developing and IAR
- 13% had deferred developing an IAR
- 44/59 respondants say their IAR is up-to-date
- 38/59 respondants say their IAR is being used

We asked about a small set of common activities for managing high-value/high-risk information (Figure 22). Of those activities, the most common activity was 'implemented back-up capability'. In 2020/21, the most common activity was 'tested business continuity plans'. Note that the 'developed information architecture and/or search tools' and 'implementing back up capability' response options were added to the 2020/21 survey and therefore were not available in the 2019/20 survey.

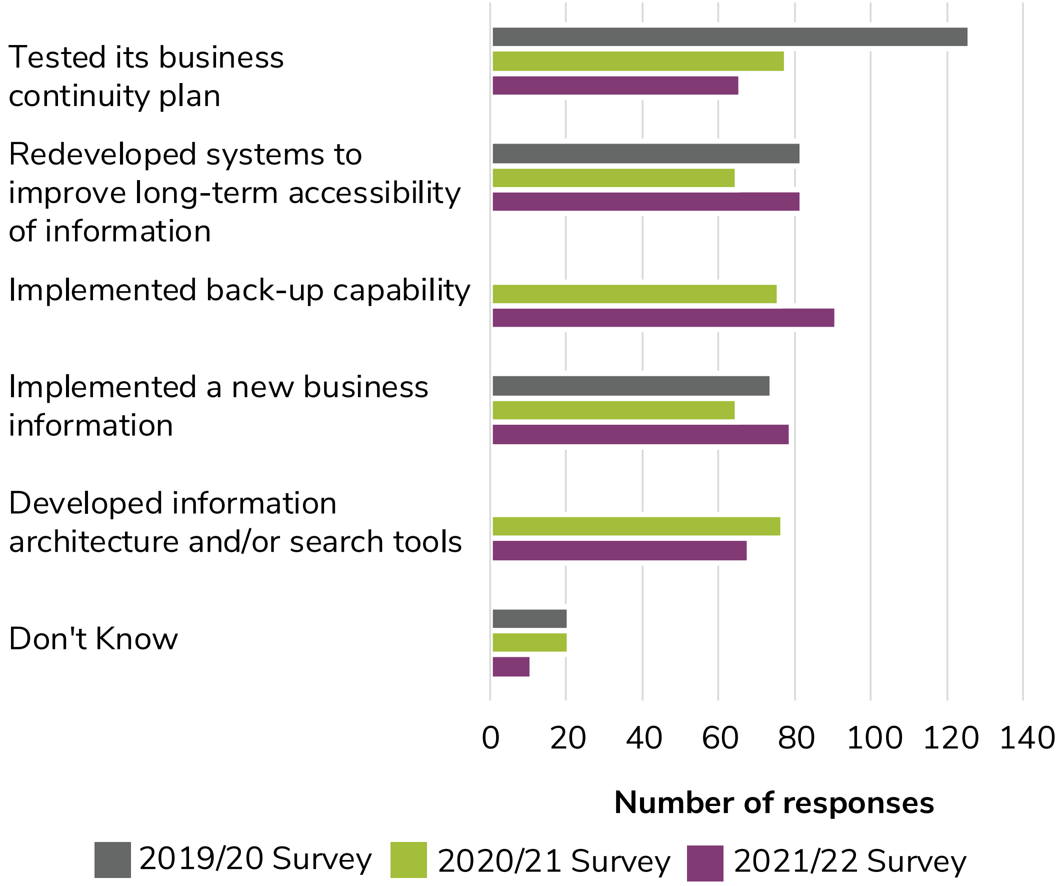

Figure 22: Actions to manage high-value/high-risk information

IM requirements built into new systems

Q25. In the last 12 months, has your organisation implemented any new business information system(s)?

Q26. Is a process for managing information through its lifecycle built into those new business information system(s)?

Q27. Which challenge(s) affect your organisation's ability to integrate IM requirements into new or upgraded business information systems?

- *Age of business system(s)*
- *IM requirements are not specified in the procurement process*
- *IM requirements considered 'nice-to-have' or de-scoped*
- *IM staff are not consulted enough*
- *Internal staff are not fully aware of the requirement*
- *Not enough management support*
- *Speed of implementation/upgrade*
- *The number of systems in use*
- *Don't know*
- *None*

Q28. Do your organisation's current systems for managing documents and records meet the minimum requirements set in Archive New Zealand's Minimum Requirements for Metadata?

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 for enabling 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 the "new" category. See Indicator 4 Building IM requirements into new business systems above for the results on this requirement.

Survey findings

We surveyed respondents about whether their business systems meet our minimum requirements for metadata. 69% say ‘some’ of their systems meet our minimum requirements for metadata (same percentage reported in 2020/21); 20% say ‘all’ of their systems meet our requirements (16% reported in 2020/21); and 11% say none of their systems meet or they ‘don’t know’ if their systems meet our requirements (compared to 15% in 2020/21).

Meet our minimum requirements for metadata?

- 69% say ‘some’ of their systems meet
- 20% say ‘all’ of their systems meet
- 11% say none of their systems meet or they ‘don’t know’ if their systems do

The most common challenges affecting respondents' ability to build in IM requirements are lack of awareness of the requirements among internal staff, the number of systems in use and the amount of consultation IM staff are given. These and other challenges mentioned are in Figure 23 (please note some of these options were not available for the 2019/20 survey).

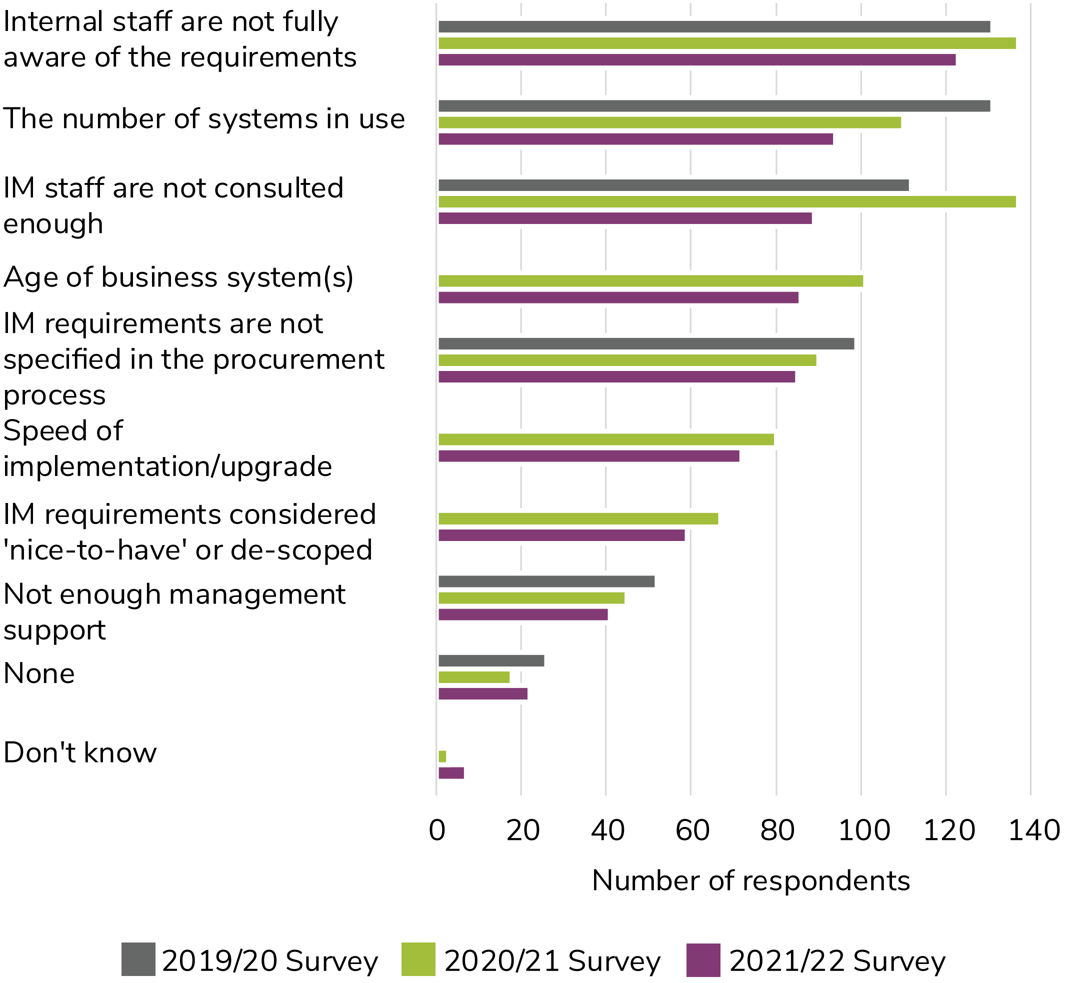

Figure 23: Challenges for building IM requirements into new business information systems[6]

[6] 'Age of business systems', 'speed of implementation/upgrade' and 'IM requirements considered 'nice-to-have' or 'de-scoped' were new response options in the 2020/21 survey.

Managing digital information over time

Q29. Does your organisation have any digital information of long-term value (that is, required for more than 10 years)?

Q30. 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?

- *Ensured metadata is persistently linked to information*
- *Identified information needing long-term retention*
- *Implemented a digital storage management plan*
- *Migrated information to a long-term digital storage environment*
- *Migrated information to new file formats*
- *Used checksums to monitor integrity of information*
- *Don't know*
- *None of the above*

Q31. Does your organisation have any digital information that is inaccessible (that is, cannot be located, retrieved or used)?

Q32. What are the reasons your organisation is unable to access that digital information?

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 10 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 (that is, 10 years or more)

- build collaborative relationships between IM and ICT to support digital continuity
- monitor and protect digital information over time.

Survey findings

Our survey results show 86% of respondents have digital information with long-term value compared to 88% in 2020/21. A combined 62% of respondents report that they 'definitely' or 'possibly' have digital information that is inaccessible (Figure 24), compared to 64% in 2020/21.

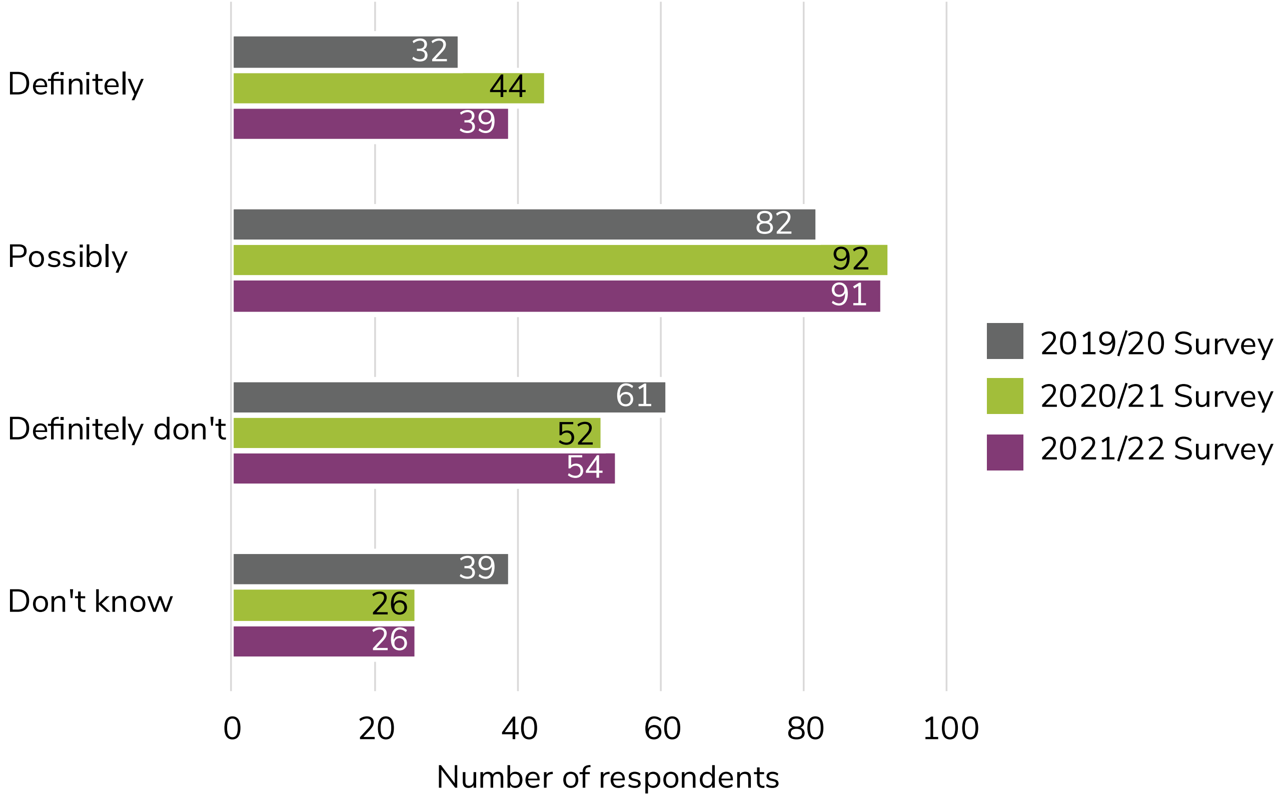

Figure 24: Do organisations hold any digital information that is inaccessible?

Organisations have taken steps to keep this information accessible (Figure 25).

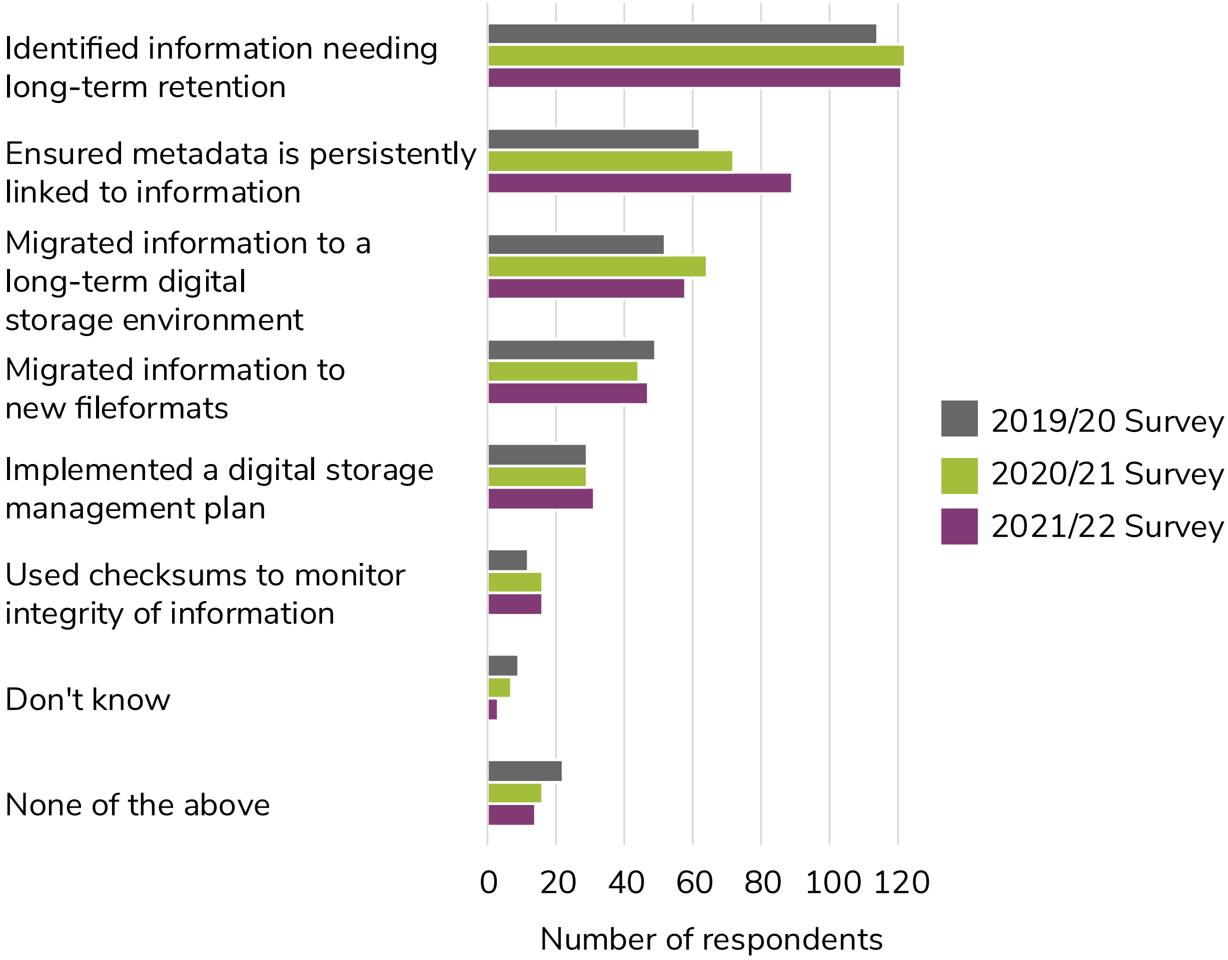

Figure 25: Actions to maintain usability in the last 12 months

The most common reasons for inaccessibility are the same as those reported in 2020/21: information being stored in personal systems, inadequate metadata and obsolete file formats (Figure 26). Please note some of these options were not available for 2019/20.

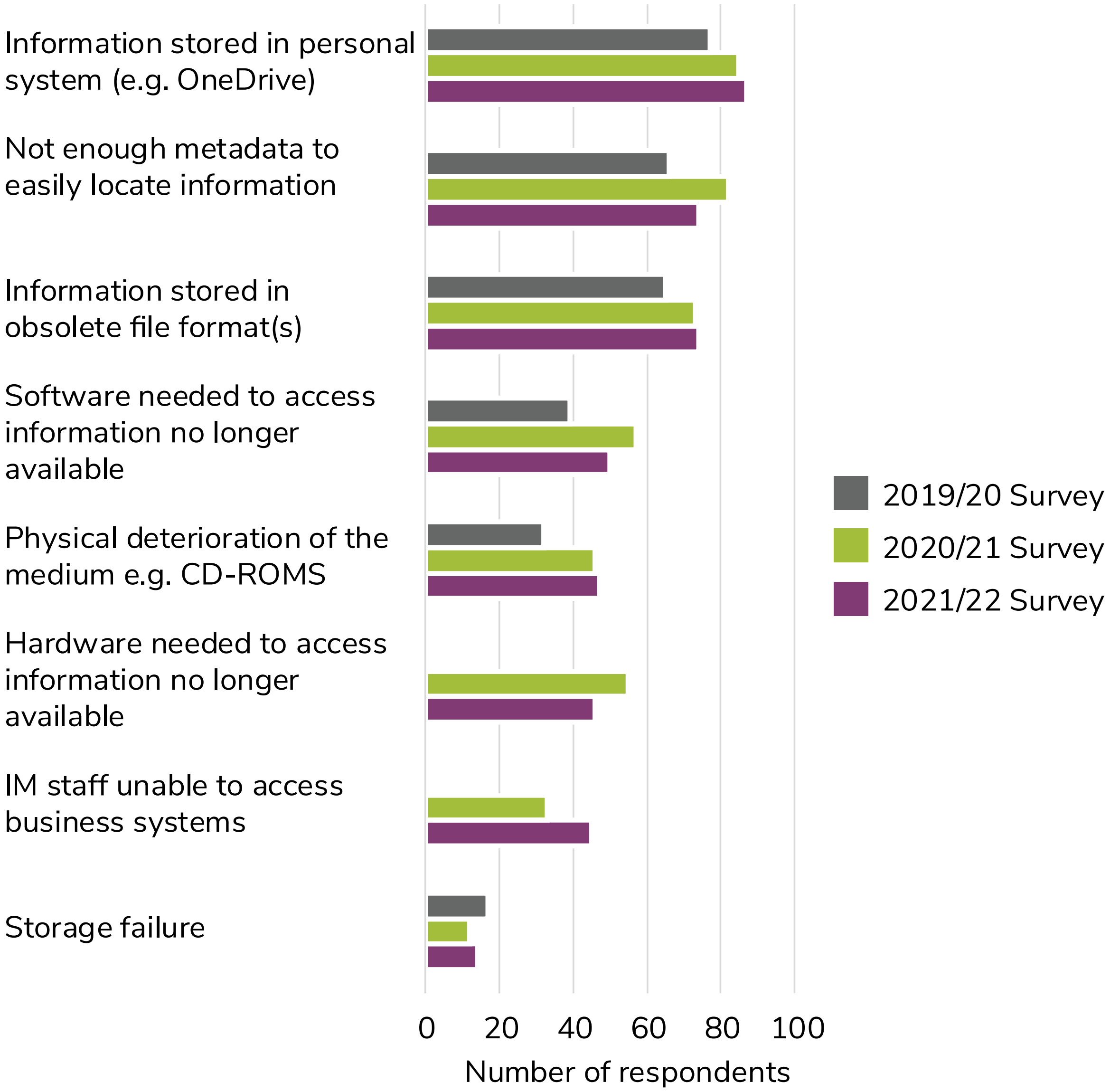

Figure 26: Reasons why digital information is inaccessible

Managing digital information during change

Q33. This question is about business changes that have implications for IM. In the last 12 months, which of these changes has occurred?

- *As part of an administrative change, received information from another organisation*
- *As part of an administrative change, transferred information to another organisation*
- *Decommissioned business information system(s)*
- *Decommissioned website*
- *Established new activity/activities within a function*
- *Established new function(s)*
- *Implemented new service offering(s)*
- *Migrated information between systems*
- *Migrated information to a new storage environment*
- *Undertook business changes in response to COVID-19*
- *None of these*

Q34. 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?

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, 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.

Survey findings

Many organisations reported undergoing organisational change during 2021/22 (Figure 27). There is a reduction of 5 percentage points in business changes because of COVID-19, which was reported to be the greatest change in the 2020/21 report[7].

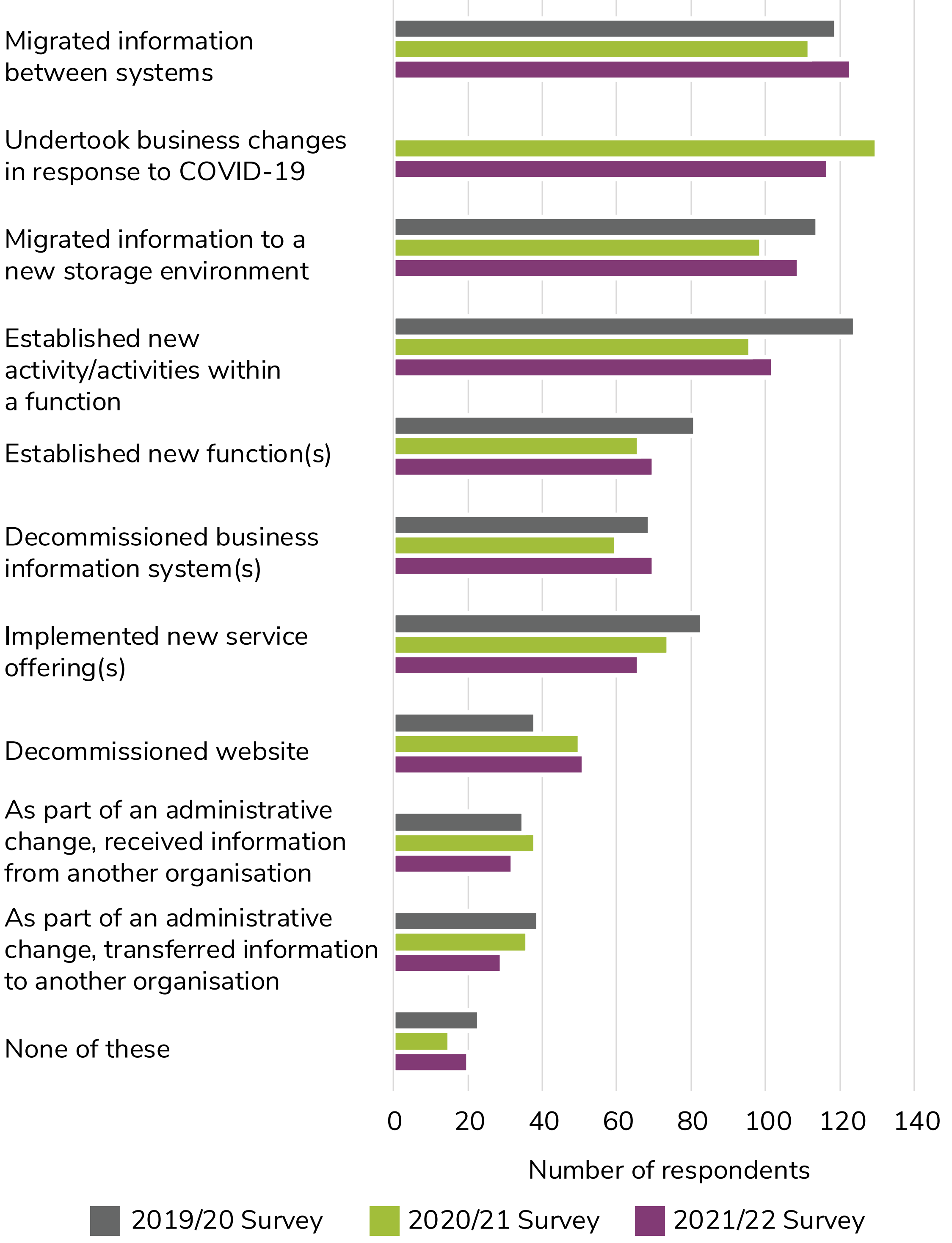

Figure 27: Organisational change in the last 12 months

[7] 'Business changes in response to COVID-19' was added during the 2020/21 survey based on our analysis of qualitative responses in 2019/20.

We surveyed the 190 respondents who reported organisational changes listed in Figure 27 and asked whether they were able to guarantee their information would not be affected by the change.

Integrity of information guaranteed?

- 56% reported ‘in every case’ of organisational change
- 41% reported ‘in some cases’ of organisational change

In 2020/21, 59% reported the integrity of information had been guaranteed in all instances of organisational change, while 37% said this had been done ‘in some cases’.

Protecting information against security risks

Q35. This question is about physical information. Which security risk(s) does your organisation take measures to protect against?

- *Unauthorised access*
- *Unauthorised alteration*
- *Unauthorised destruction*
- *Loss*
- *None of these*

Q36. This question is about storage of digital information. Which security risk(s) does your organisation take measures to protect against?

- *Unauthorised access*
- *Unauthorised alteration*
- *Unauthorised destruction*
- *Loss*
- *None of these*

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. Security breaches can undermine public trust and Ministerial confidence. We expect organisations to stay on top of security risks to protect information in all formats, wherever it is located.

Survey findings

A high proportion of respondents said that they protect both physical and digital information against loss and unauthorised alteration, destruction and access (Figure 28).

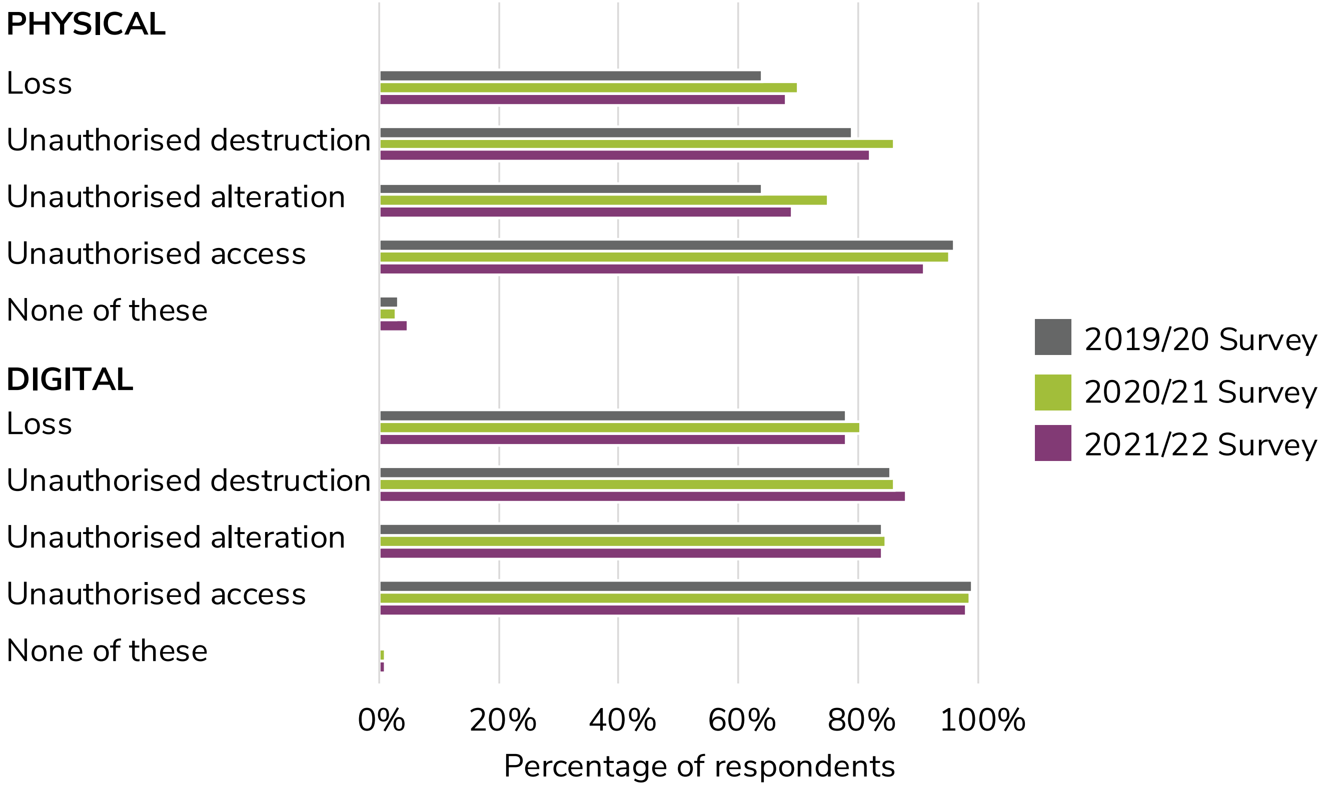

Figure 28: Number of organisations that protect physical and digital information against risk

Access classification for information over 25 years old

Q43. Does your organisation hold any information that is more than 25 years old?

Q44. How much of that information over 25 years old has been classified as either open or restricted access?

In the words of the Chief Ombudsman "It is crucial that the information on which impactful decisions are based is available to, or can be requested by, the public so the rationale for decision making is transparent and open to scrutiny by those whom the decisions affect."[8] Although public access to central and local government information is largely guided by official and personal information laws, the PRA 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).[9]

Access must 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 for inspection 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.

[8] (2022). Office of the Ombudsman. Ready or not? A report on the public sector, the OIA, and the pandemic.

[9] 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).

Survey findings

We surveyed organisations that said they hold information that is more than 25 years old. Of those organisations, the most common response we received was they did not know if they have classified information (Figure 29). This response may indicate that many organisations may not realise classifying information is something they should be doing.

75% hold information that is >25 years old

- 29% have classified 'all or almost all' of that information as open or restricted
- 28% have classified 'hardly any or no' information over the last 25 years
- 30% say they 'don't know' if they have classified information

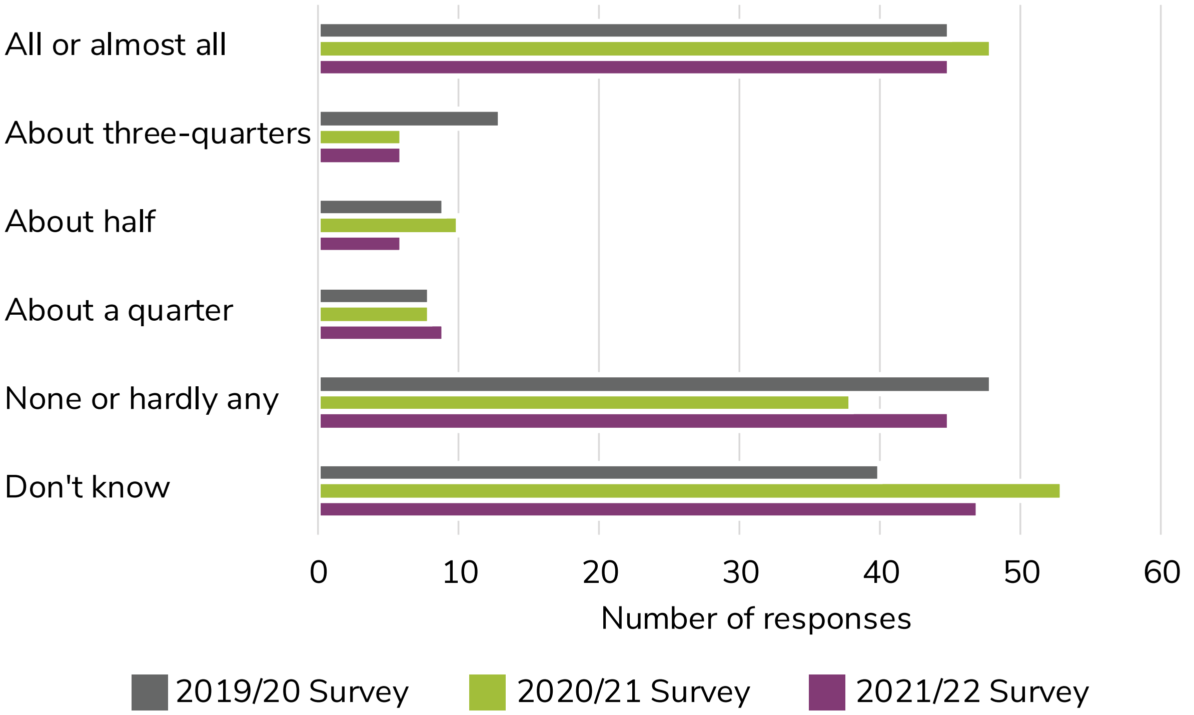

Figure 29: Proportion of information over 25 years old classified as open or restricted

4. 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.

Topics covered include:

- preparing for disposal
- doing disposal

Preparing for disposal

Q37. How much of the information held by your organisation is covered by authorised disposal authorities?

Q38. This question is about the information not covered by disposal authorities. When does your organisation plan to start improving coverage?

Q39. This question is about both physical and digital information. I the last 12 months, which action(s) has your organisation carried out in preparation for disposal?

- *Developed a disposal implementation plan*
- *Obtained approval to dispose of information from business owners*
- *Sentenced information in offsite storage*
- *Sentenced unstructured information in business information systems*
- *Sentenced unstructured information in shared drives*
- *Set-up automated disposal in Enterprise Content Management System (or similar)*
- *Used automated tools to analyse digital files in preparation for transfer (for example, DROID)*
- *Don't know*
- *None of the above*

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 or, where applicable, coverage by a functional 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.

Survey findings

We asked respondents to tell us what proportion of their information was covered by disposal authorities (Figure 30). 44% reported 'all or almost all' their information was covered by approved disposal authorities. However, in this year's survey, responses to 'none or hardly any' have increased since 2020/21.

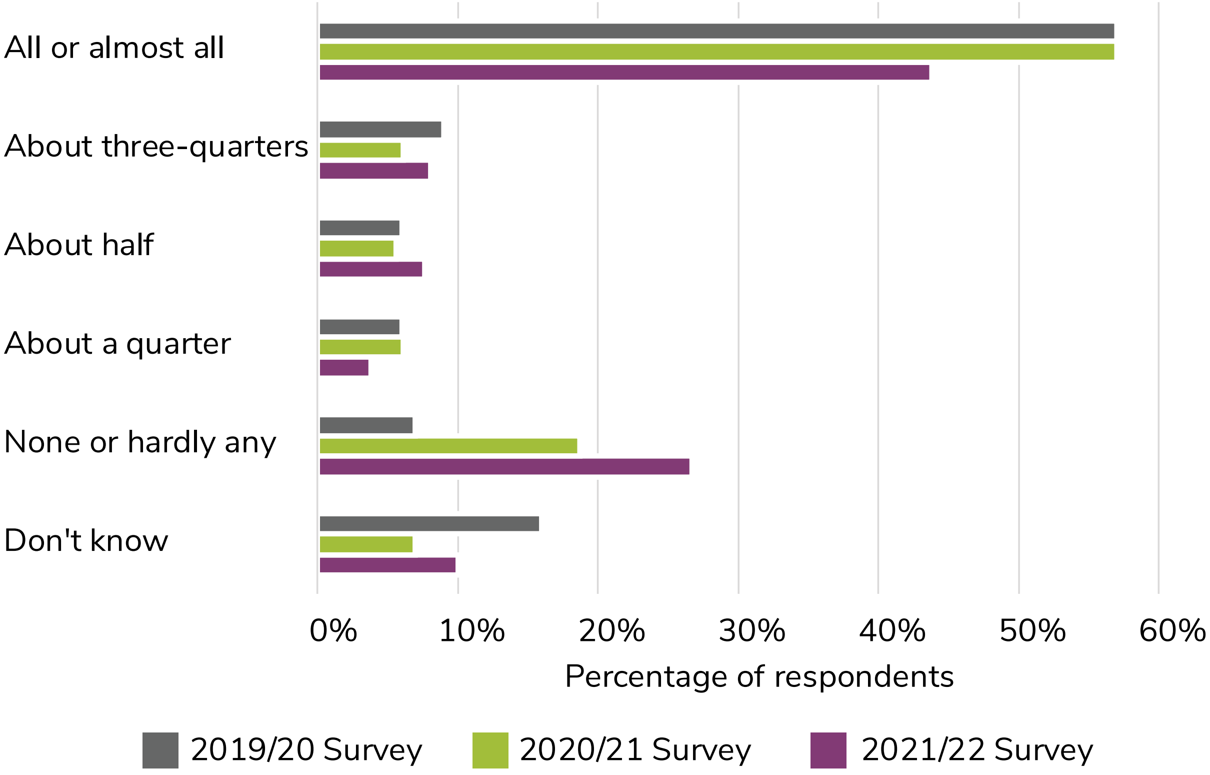

Figure 30: Proportion of information covered by disposal authorities

Of the respondents who were asked when they plan to improve coverage, 47% provided a timeframe while 40% said that appraisal to improve coverage was underway.

The most common actions to prepare for doing disposal were obtaining approval to dispose from business owners and sentencing information in offsite storage, that is, physical information (Figure 31). There is far less activity focused on preparing digital information for disposal.

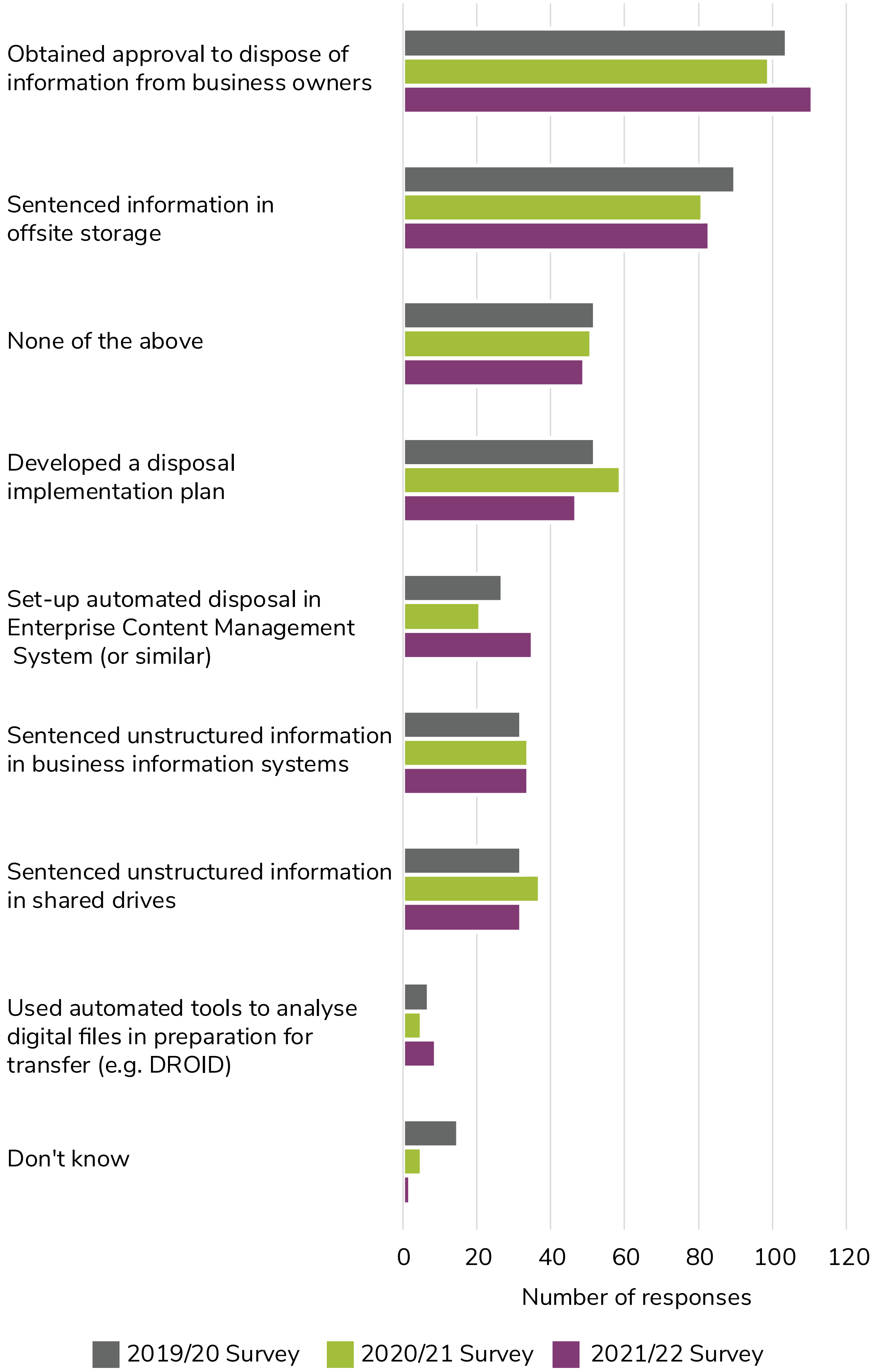

Figure 31: Actions to prepare for disposal over the last three surveys

Doing disposal

Q42. This question is about both physical and digital information. Which challenge(s) affect your organisation's ability to undertake regular authorised destruction of information?

- *A lack of confidence that sentencing has been done accurately*
- *Destruction not seen as a priority for staff*
- *Difficulty of sentencing unstructured information repositories*
- *Disposal authorities do not support automated disposal*
- *IM staff unable to access business systems*
- *Not enough resources put toward sentencing activity*
- *Systems not set up to automate regular authorised deletion*
- *The cost of secure destruction/deletion through the storage provider*
- *The difficulty of obtaining approvals*
- *Don't know*
- *None of the above*

Q45. In the next 12 months, is your organisation planning to transfer any physical information?

Q46. Where are you planning to transfer the physical information to?

Q47. Does your organisation hold physical information that is ready to transfer to Archives New Zealand's new Wellington repository when it becomes fully operational?

Q48. In the last 12 months, is your organisation planning to transfer any digital information to:

- *Archives New Zealand*
- *A local authority*
- *Neither of these*
- *Don't know*

Q49. This question is about both physical and digital information. What challenge(s) affect your organisation's ability to undertake regular transfer of information?

- *Have no information over 25 years old*
- *Archives New Zealand's Wellington repository is not taking transfers of physical information*
- *Current system is unable to export records and descriptive metadata for digital transfer*
- *Difficulty obtaining approval from senior management*
- *Difficulty understanding Archives New Zealand's processes and requirements*

- *Lack of confidence that sentencing has been done accurately*
- *Lack of resources to prepare transfer*
- *Lack of skills in doing physical transfers*
- *Lack of system support to export records and descriptive metadata for digital transfer*
- *No Local Authority archive to transfer to*
- *Not a priority for senior management*
- *Not enough resources put toward sentencing activity*
- *Don't know*

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 (for example, 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 Te Rua Mahara, but the status of their information changes to that of 'Local Authority archive' after 25 years or when no longer in current use. Te Rua Mahara Wellington repository is closed for physical transfers while new archival storage is planned and developed, 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 a project that requires special resourcing.

Survey findings

The most common challenges for doing regular authorised destruction are not enough resources, system set-up and lack of prioritisation by staff responsible for electronic deletion (Figure 32).

Other challenges mentioned in the comments in addition to those listed in Figure 32, include:

- moratorium on the disposal of records relating to a Royal Commission Inquiry
- waiting for disposal authority approval. Archive New Zealand's approval process is time demanding
- lack of staff awareness of their responsibilities
- insufficient resources-staff, funding.

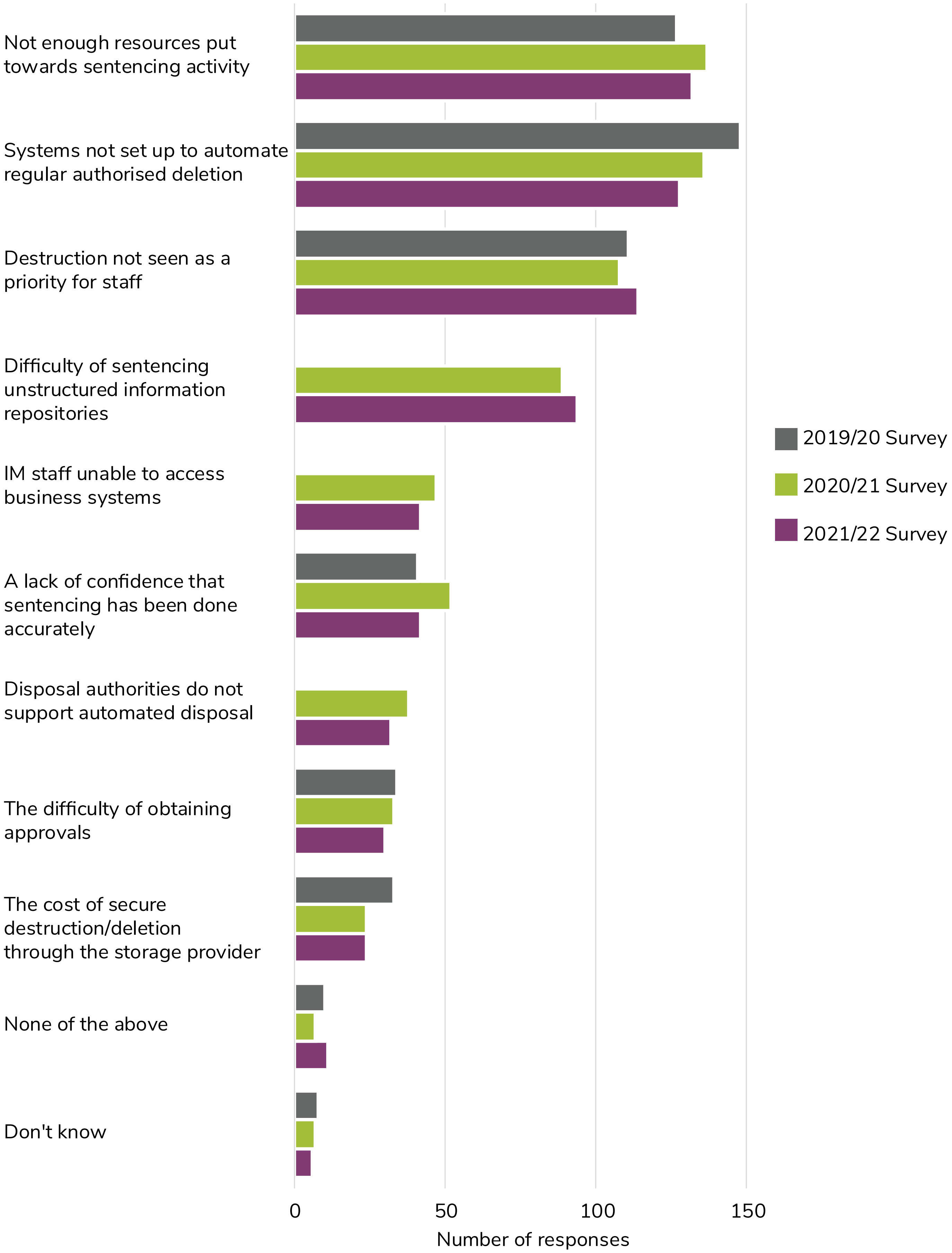

Figure 32: Challenges for doing authorised destruction of information[10]

[10] Not all categories were available for the 2019/20 survey.

A minority of respondents have plans to transfer physical (22%) or digital (15%) information in the next 12 months. Consistent with the 2020/21 survey, only 20% percent of respondents said that they hold physical information that is ready for when Wellington transfers resume.

The most common challenges for doing regular transfer are: lack of resources to prepare transfer, lack of resources for sentencing and the Wellington repository isn't taking transfers of physical information (Figure 33).

Other challenges mentioned in the comments in addition to those listed in Figure 33 include:

- waiting for disposal authority to be approved. Archive New Zealand's approval process is time intensive
- records are still needed
- legislative changes required to enable transfer of some records
- lack of resources, funding, staff capacity and (high staff turnover) capability.

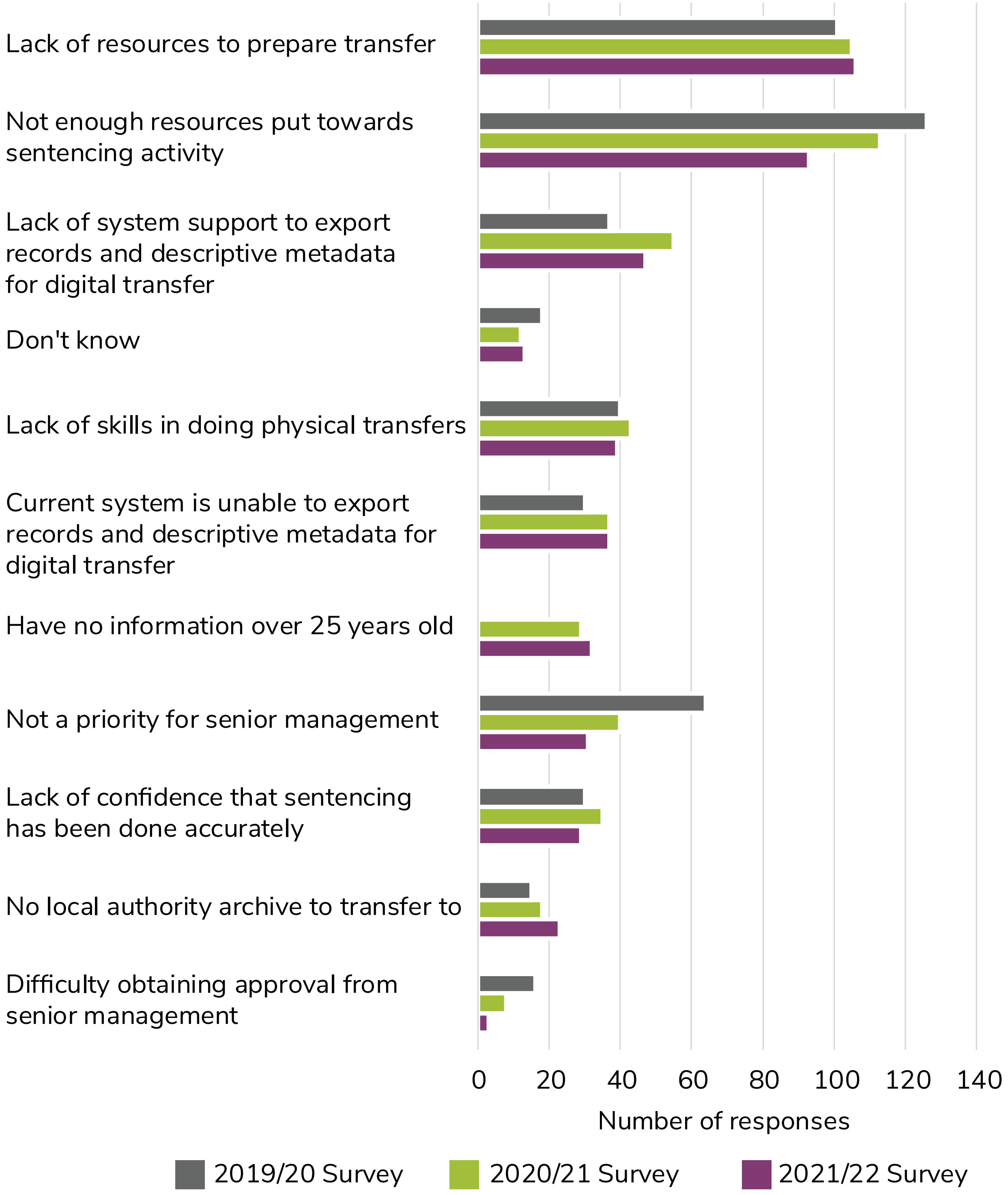

Figure 33: Challenges for transferring information

5. 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.

Topics covered include:

- Drivers, challenges and risks
- Requests for official information

Drivers, challenges and risks

Q50. What current drivers for good IM practice and processes are important to your organisation?

- *Business efficiency*
- *Risk management*
- *Customer service delivery*
- *Compliance with legislative requirements*
- *Efficient cost management*
- *In-house collaboration*
- *Collaboration with other organisations*

Q51. Below are some challenges for good IM practices and processes. In your organisation, how big a challenge are these to the organisation's IM?

- *Lack of understanding of the importance of IM*
- *IM not adequately addressed in planning phase of projects*
- *IM insufficiently resourced*
- *'Silos' – lack of communication across business groups*
- *Information incomplete, for example, not providing evidence of decisions*
- *Information not easily searchable*
- *Information is not easily accessible*

Q52. Has your organisation identified any key risks to its information?

Q53. What key risks to your organisation's information have been identified?

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 case 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.

Survey findings

The strongest drivers for IM were compliance with legislative requirements and risk management (Figure 34). 81% of respondents said that compliance was an ‘extremely important’ driver and 78% of respondents reported risk management was an ‘extremely important’ driver. In previous years, risk management was a stronger driver than compliance with legislative requirements. Most 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 34, include:

- supporting strategic goals of our organisation/sector
- information/data has high value for future research on our sector and Aotearoa
- ensuring records of care are accessible
- transparency of research

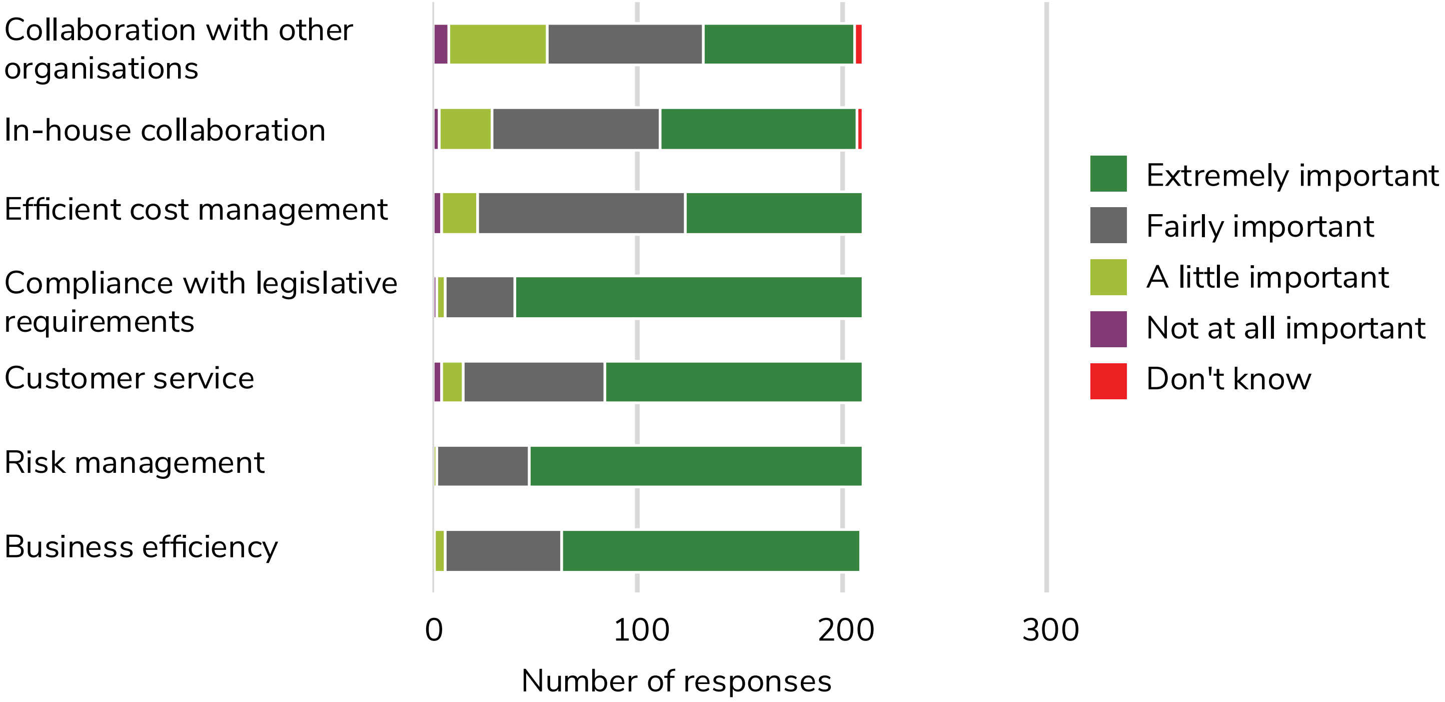

Figure 34: Drivers for good IM

The greatest challenges for good IM practice were the lack of understanding of importance of IM, IM not adequately addressed in planning phase of projects, communication across business groups and insufficient resourcing for IM (Figure 35). This is fairly consistent with our 2020/21 findings. Other challenges mentioned in the comments in addition to those listed in Figure 35, include:

- 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

- lack of knowledgeable staff and resources
- locating classified information
- IM staff training.

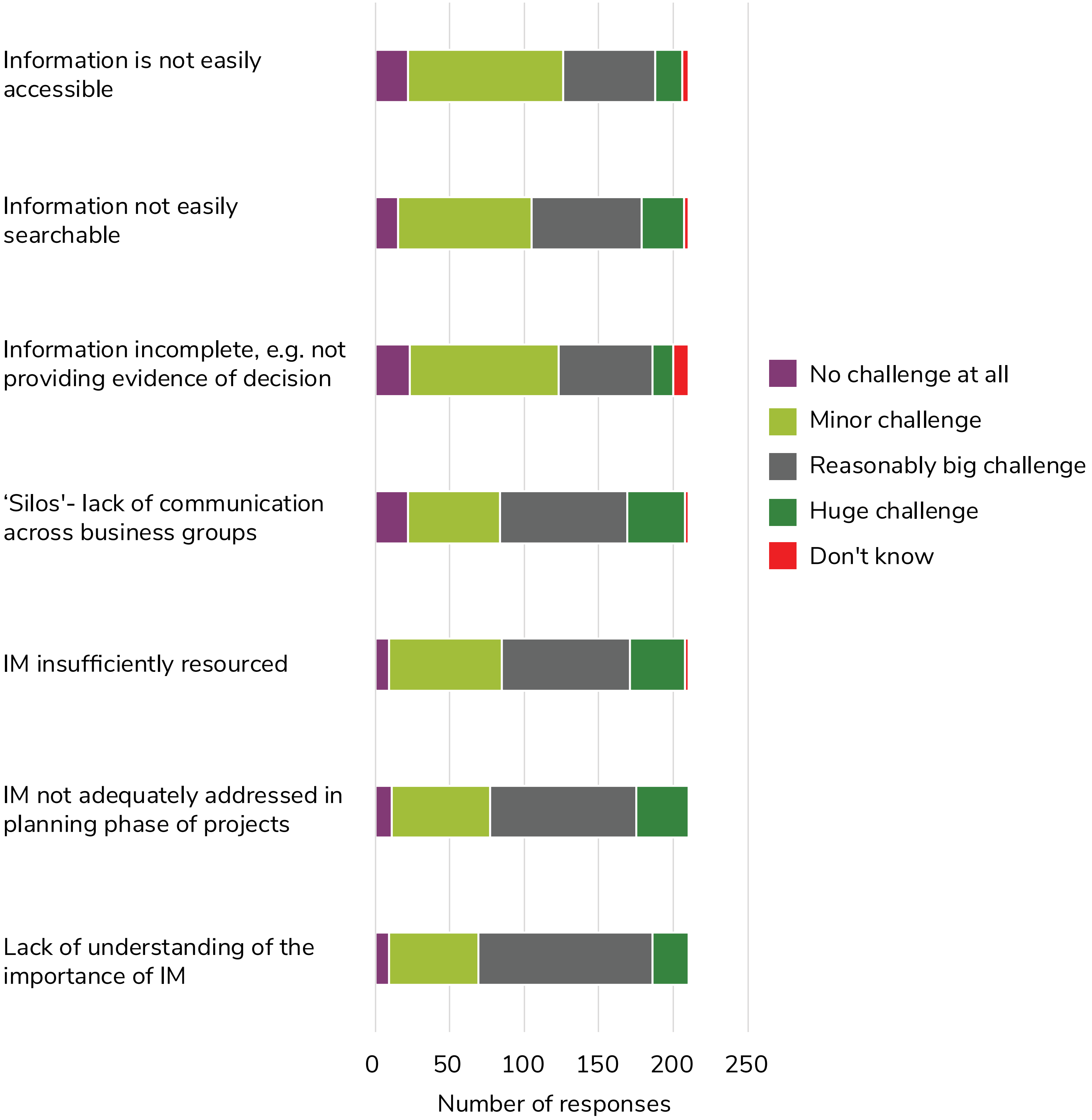

Figure 35: Challenges for good IM

Figure 36 shows that the most common risks to information are shadow IT or personal repositories, lack of contextual information and collaboration tools. Other risks mentioned in the comments in addition to those listed in Figure 36 include:

- cybersecurity threats (for example, hacking)
- information held by contractors and not accessible by the organisation
- using cloud services, one drive and email to store information
- behaviour of staff, for example, not following proper procedures
- lack of expertise in MS 365 applications
- processes do not meet legislative compliance.

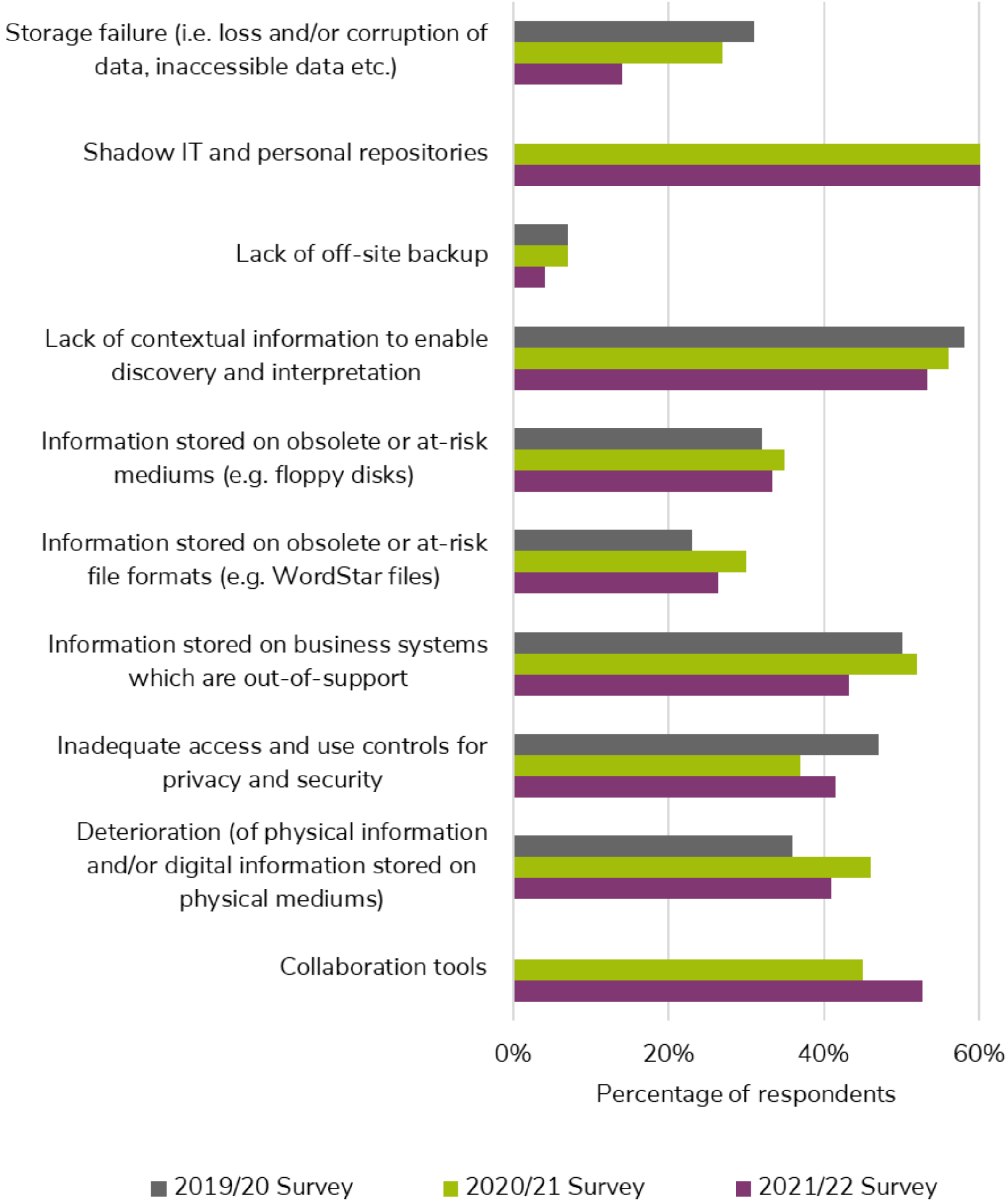

Figure 36: Risks to information[11]

[11] 'Collaboration tools' and 'shadow IT and personal repositories' were not included in the 2019/20 survey.

Requests for official information

Q54. 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?

Q55. In the last 12 months, has your organisation ever been unable to provide the official information asked for?

Q56. 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 (that is, the record has not been created)?

Q57. 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?

We are interested in the reasons for refusing official information requests because they can indicate underlying issues with IM. The PRA 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.

Survey findings

Of the respondents who received requests for official information in the last 12 months, 37% said that they were unable to provide some information requested. This number is comparable to 2020/21 survey responses (38%). Of the 37%, a combined 64% said that the reason for this was ‘rarely’ or ‘never’ because the information does not exist (Figure 37). In 2020/21, 52% reported the reason being ‘rarely’ or ‘never’ because the information does not exist. A combined 80% said the reason for this was ‘rarely’ or ‘never’ because the information cannot be found, compared to 2020/21 with 73%.

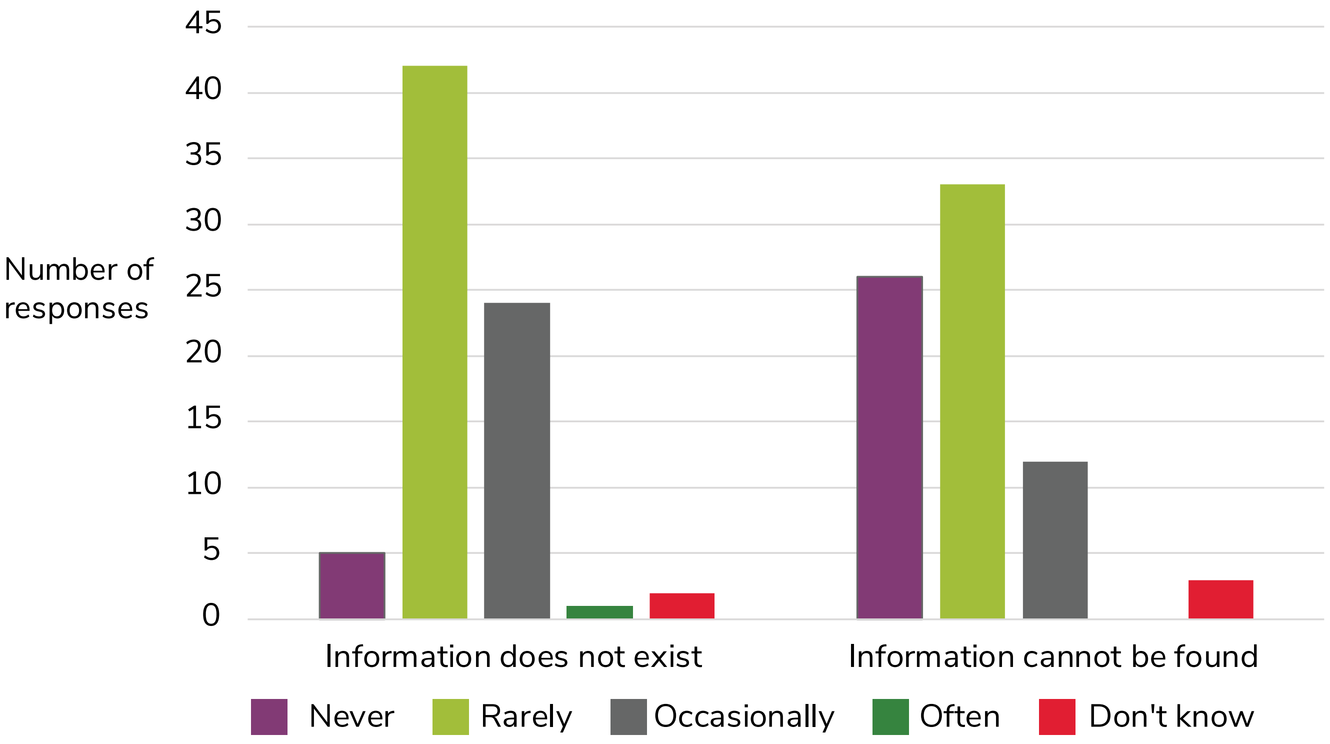

Figure 37: Frequency with which information does not exist or cannot be found

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?

Q2 What type of organisation is it?

Response options	Number	Percent
State sector	117	56%
Local government	66	31%
Other	27	13%
Total	210	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'.

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	117	56%
One office only	45	21%
More than one office, all of them in the same town city	32	15%
Offices located across more than one country	16	8%
Total	210	100.0%

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

Response options	Number	Percent
None	1	0%
Less than 100	60	29%
100 to 299	54	25.7%
300 to 499	30	14.3%
500 to 2999	47	22%
3000 to 5999	13	6%
More than 6000	5	2%
Total	210	100.0%

Q5 Does your organisation have a formal governance group which:

Response options	Number	Percent
Has IM oversight as part of its mandate	101	48%
Is dedicated to IM	27	13%
Neither of the above	82	39%
Total	210	100.0%

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

Response options	Number	Percent
Yes	119	93%
No	8	6%
Don’t know	1	1%
Total	128	100%

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

Response options	Number	Percent
Yes	108	84%
No	20	16%
Total	128	100%

Q8 Does your organisation have documented IM policy?

Response options	Number	Percent
Yes	183	87%
No	24	11%
Don’t know	3	1%
Total	210	100%

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

Response options	Number	Percent
Yes	82	39%
No	87	41%
Don’t hold any	15	7%
Don’t know	26	12%
Total	210	100%

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

Response options	Number	Percent
Yes, please specify	42	51%
No	31	38%
Don’t know	9	11%
Total	82	100%

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=82)

Response options	Number	Percent
Documented IM implications from Te Tiriti o Waitangi agreements	13	16%
Improved access	42	51%
Improved discoverability for example, improved metadata	43	52%
Improved levels of care	28	34%
Involved IM staff in negotiating agreements with Māori	7	9%
Worked with Māori to change IM practices	25	31%
No action taken	7	9%
Total	210	100.0%

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=82). Similarly, the percents do not add to 100%.

Q12 In the last 12 months, has your organisation done any self-monitoring of its compliance with: (tick all that apply) (N=210)

Response options	Number	Percent
Archives New Zealand's requirements	145	69%
This organisation's own IM policy	119	57%
Neither of these	33	16%

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=210). Similarly, the percents do not add to 100%.

Q13 What method(s) were used for that self-monitoring? (tick all that apply) (N=177)

Response options	Number	Percent
Assessment by a third party	62	30%
Bench-marking exercise	8	4%
Internal audit	72	34%
Maturity assessment	89	42%
Review of processes	115	55%

Response options	Number	Percent
Risk Assessment	63	16%

Q14 As a result of that self-monitoring, is your organisation developing or has it developed an action plan? (tick all that apply) (N=177)

Response options	Number	Percent
Developing an action plan	100	56%
Developed an action plan	55	31%
Deferring action	10	6%
None of these	12	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=177). Similarly, the percents do not add to 100%.

Q15 As a result of that self-monitoring, is your organisation implementing or implemented an action plan?

Response options	Number	Percent
Implementing an action plan	50	91%
Implemented an action plan	3	5%
Deferred implementation of action plan	2	4%
None of these	0	0%

Note for Q15: Excluded one response.

Q16: 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	49	23%
1 IM FTE or less	51	24%
More than 1 up to 3 IM FTE	44	21%
More than 3 up to 6 IM FTE	32	15%
More than 6 up to 10 IM FTE	23	11%
More than 10 IM FTE	11	5%
Total	210	100%
Total FTE of dedicated IM staff across all 210 organisations	677	

Note for Q16: Respondents were asked to enter an exact number. Their responses have been classified into the options presented in the table.

Q17 In the last 12 months, which of the following has any dedicated IM staff member(s) done? (tick all that apply) (N=162)

Response options	Number	Percent
Attended an IM conference (or similar event)	83	51%
Attended an IM training course (face-to-face and or/online)	108	67%
Had an IM-relevant secondment	18	11%
Presented at an IM conference (or similar event)	15	9%
Studied towards a recognised IM qualification	17	10%
None of these	31	10%

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=162). Similarly, the percentages do not add to 100%.

Q18 Which of the groups below does your organisation inform about their IM responsibilities (tick all that apply) (N=210)

Response options	Number	Percent
Staff at all levels	200	95%
Contractors	123	59%
Consultants	99	47%
None of these	10	5%

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=210). Similarly, the percentages do not add to 100%.

Q19 In which way(s) are the groups that you ticked in the previous question informed about their IM responsibilities? (tick all that apply) (N=200)

Response options	Number	Percent
Code of Conduct	111	56%
Contracts	92	46%
Induction training (face-to-face and/or online)	173	87%
Job descriptions	80	40%
Performance development plans /agreements	33	17%
Refresher training (face-to-face and/or online)	111	56%
Don’t know	0	0.0%
None of the above	2	1%

Note for Q19: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=200). Similarly, the percents do not add to 100%.

Q20 Has your organisation identified its most important high value/high risk information?

Response options	Number	Percent
Yes	76	36%
In progress	108	51%
No	20	10%
Don’t know	6	3%
Total	210	100%

Q21 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=210)

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	68	32%
Implemented a new business information system to mitigate risks to information	79	38%

Response options	Number	Percent
Implemented back-up capability	91	43%
Redeveloped systems to improve long-term accessibility of information	82	39%
Tested its business continuity plan	66	31%
Don’t know	11	5%

Note for Q21: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%.

Q22 Does your organisation have an information asset register (or similar way of recording information assets)?

Response options	Number	Percent
Yes	59	28%
In development	66	31%
Work started but deferred	28	13%
No	57	27%
Total	210	100.0%

Q23 Is that register:

Response options	Number	Percent
Up-to-date?	44	75%
Being used?	38	64%
Neither of these	4	7%
Total	86	100.0%

Q24 Is your organisation planning to have an information asset register (or similar)?

Response options	Number	Percent
Yes	33	58%
No	12	21%
Don’t know	12	21%
Total	57	100.0%

Q25. 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	146	70%
No	59	28%
Don't know	5	2%
Total	210	100.0%

Q26. Is a process for managing information through its lifecycle built into those new business information system(s)?

Response options	Number	Percent
Yes	88	60%
No	42	29%
Don't know	16	11%
Total	146	100.0%

Q27 Which challenge(s) affect your organisation's ability to integrate IM requirements into new or upgraded business information systems? (tick all that apply) (N=210)

Response options	Number	Percent
Age of business system(s)	86	41%
IM requirements are not specified in the procurement process	85	40%
IM requirements considered 'nice-to-have' or de-scoped	59	28%
IM staff are not consulted enough	89	42%
Internal staff are not fully aware of the requirement	123	59%
Not enough management support	41	20%
Speed of implementation/upgrade	72	34%
The number of systems in use	94	45%
Don't know	7	3%
None	22	10%

Note for Q27: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%.

Q28 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	Number	Percent
All systems do	42	20%
Some systems do	144	69%
No systems do	5	2%
Don’t know	19	9%
Total	210	100%

Q29 Does your organisation have any digital information of long-term value (that is, required for more than 10 years)?

Response options	Number	Percent
Yes	180	86%
No	21	10%
Don’t know	9	4%
Total	210	100.0%

Q30 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=180)

Response options	Number	Percent
Ensured metadata is persistently linked to information	89	49%
Identified information needing long-term retention	121	67%
Implemented a digital storage management plan	31	17%
Migrated information to a long-term digital storage environment	58	32%
Migrated information to new file formats	47	26%
Used checksums to monitor integrity of information	16	9%
Don’t know	3	2%
None of the above	14	8%

Note for Q30: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=180). Similarly, the percents do not add to 100%.

Q31 Does your organisation have any digital information that is inaccessible (that is, cannot be located, retrieved or used)?

Response options	Number	Percent
Don’t know	26	12%
Definitely don’t	54	26%
Possibly	91	43%
Definitely	39	19%

Q32 What are the reasons your organisation is unable to access that digital information? (tick all that apply) (N=130)

Response options	Number	Percent
Hardware needed to access information no longer available	46	35%
IM staff unable to access business systems	45	35%
Information stored in obsolete file format(s)	74	57%
Information stored in personal system (for example, OneDrive)	87	67%
Not enough metadata to easily locate information	74	57%
Physical deterioration of the medium (for example, CD-ROMS)	47	36%
Software needed to access information no longer available	50	39%
Storage failure	14	11%

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=130). Similarly, the percents do not add to 100%.

Q33 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=210)

Response options	Number	Percent
As part of an administrative change, received information from another organisation	32	15%
As part of an administrative change, transferred information to another organisation	29	14%
Decommissioned business information system(s)	70	33%
Decommissioned website	51	24%
Established new activity/activities within a function	102	49%

Response options	Number	Percent
Established new function(s)	70	33%
Implemented new service offering(s)	66	31%
Migrated information between systems	123	59%
Migrated information to a new storage environment	109	52%
Undertook business changes in response to COVID-19	117	56%
None of these	20	10%

Note for Q33: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%.

Q34 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	106	41%
In some cases	78	56%
Don't know	4	2%
Never	2	1%
Total	190	100.0%

Q35 This question is about physical information. Which security risk(s) does your organisation take measures to protect against? (tick all that apply) (N=210)

Response options	Number	Percent
Unauthorised access	191	91%
Unauthorised alteration	145	69%
Unauthorised destruction	173	82%
Loss	143	68%
None of these	10	5%

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=210). Similarly, the percents do not add to 100%.

Table: Q36. 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=210)

Response options	Number	Percent
Unauthorised access	206	98%
Unauthorised alteration	176	84%
Unauthorised destruction	184	88%
Loss	164	78%
None of these	2	1%

Note for Q36: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%

Q37 How much of the information held by your organisation is covered by authorised disposal authorities?

Response options	Number	Percent
None or hardly any	56	27%
About a quarter of it	8	4%
About half of it	16	8%
About three-quarters of it	17	8%
All or almost all	92	44%
Don’t know	21	10%
Total	210	100.0%

Q38 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	47	40%
In less than 12 months	21	18%
In the next 1-3 years	34	29%
In the next 4-5 years	0	0
Don’t know	16	14%
Total	118	100.0%

Q39 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=210)

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	47	22%
Obtained approval to dispose of information from business owners	111	53%
Sentenced information in offsite storage	83	40%
Sentenced unstructured information in business information systems	34	16%
Sentenced unstructured information in shared drives	32	15%
Set-up automated disposal in Enterprise Content Management System (or similar)	35	17%
Used automated tools to analyse digital files in preparation for transfer (for example, DROID)	9	4%
Don't know	2	1%
None of the above	49	23%

Note for Q39: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%.

Q40 In the last 12 months, has your organisation carried out authorised destruction of physical information?

Response options	Number	Percent
Yes	107	51%
No	97	46%
Don't know	6	3%
Total	210	100.0%

Q41 In the last 12 months, has your organisation carried out authorised destruction of digital information?

Response options	Number	Percent
Yes	71	34%
No	134	64%
Don't know	5	2%
Total	210	100.0%

Q42 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=210)

Response options	Number	Percent
A lack of confidence that sentencing has been done accurately	42	20%
Destruction not seen as a priority for staff	114	54%
Difficulty of sentencing unstructured information repositories	94	45%
Disposal authorities do not support automated disposal	32	15%
IM staff unable to access business systems	42	20%
Not enough resources put towards sentencing activity	132	63%
Systems not set up to automate regular authorised deletion	128	61%
The cost of secure destruction/deletion through the storage provider	24	11%
The difficulty of obtaining approvals	30	14%
Don't know	6	3%
None of the above	11	5%

Note for Q42: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%.

Q43 Does your organisation hold any information that is more than 25 years old?

Response options	Number	Percent
Yes	158	75%
No	45	21%
Don't know	7	3%
Total	210	100.0%

Q44 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	45	28%
About a quarter of it	9	6%
About half of it	6	4%
About three quarters of it	6	4%
All or almost all	45	29%
Don’t know	47	30%
Total	158	100.0%

Q45 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	46	22%
No	136	65%
Don’t know	28	13%
Total	210	100.0%

Q46 Where are you planning to transfer the physical information to?

Response options	Number	Percent
A Local Authority archive	19	41%
Archives New Zealand’s Auckland repository	9	20%
Archives New Zealand’s Christchurch repository	5	11%
An approved repository, please specify	10	22%
Archive NZ’s Dunedin repository	0	0
Don’t know	3	7%
Total	46	100.0%

Q47 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	43	20%
No	116	55%
Not applicable, Local Authorities select this option	51	24%
Total	210	100.0%

Q48 In the next 12 months, is your organisation planning to transfer any digital information to:

Response options	Number	Percent
Archives New Zealand	17	8%
A Local Authority archive	14	7%
Neither of these	146	70%
Don't know	33	16%
Total	210	100.0%

Q49 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=210)

Response options	Number	Percent
Have no information over 25 years old	32	15%
Archives New Zealand s Wellington repository is not taking transfers of physical information	73	35%
Current system is unable to export records and descriptive metadata for digital transfer	37	18%
Difficulty obtaining approval from senior management	3	1%

Response options	Number	Percent
Difficulty understanding Archives New Zealand's processes and requirements	36	17%
Lack of confidence that sentencing has been done accurately	29	14%
Lack of resources to prepare transfer	106	50%
Lack of skills in doing physical transfers	39	19%
Lack of system support to export records and descriptive metadata for digital transfer	47	22%
No Local Authority archive to transfer to	23	11%
Not a priority for senior management	31	15%
Not enough resources put towards sentencing activity	93	44%
Don't know	13	6%

Note for Q49: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=210). Similarly, the percents do not add to 100%.

Q50 What current drivers for good IM practice and processes are important to your organisation? (N=210)

Response options	Not important	A little important	Fairly important	Extremely important	Don't know
Business efficiency	1	5	57	146	1
Risk management	0	2	45	163	0
Customer service delivery	4	11	69	126	0
Compliance with legislative requirements	2	4	34	170	0
Efficient cost management	4	18	101	87	0
In-house collaboration	3	26	82	96	3
Collaboration with other organisations	8	48	76	74	4

Q51 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=210)

Response options	No challenge at all	Minor challenge	Reasonably big challenge	Huge challenge	Don't know
Lack of understanding of the importance of IM	9	60	117	24	0
IM not adequately addressed in planning phase of projects	11	66	98	35	0
IM insufficiently resourced	9	76	86	37	2
'Silos' - lack of communication across business groups	22	62	85	39	2
Information incomplete, for example, not providing evidence of decisions	23	100	63	14	10
Information not easily searchable	15	90	74	28	3
Information is not easily accessible	22	104	62	18	4

Q52 Has your organisation identified any key risks to its information?

Response options	Number	Percent
Yes	171	81%
No	32	15%
Don't know	7	3%
Total	210	100.0%

Q53 What key risks to your organisation's information have been identified? (tick all that apply) (N=171)

Response options	Number	Percent
Collaboration tools	90	53%
Deterioration (of physical information and/or digital information stored on physical mediums)	70	41%
Inadequate access and use controls for privacy and security	71	42%

Response options	Number	Percent
Information stored on business systems which are out-of-support	74	43%
Information stored on obsolete or at-risk file formats (for example, WordStar files)	45	26%
Information stored on obsolete or at-risk mediums (for example, floppy disks)	57	33%
Lack of contextual information to enable discovery and interpretation	91	53%
Lack of off-site backup	7	4%
Shadow IT and personal repositories	117	68%
Storage failure (that is, loss and/or corruption of data, inaccessible data etc.)	24	28%

Note for Q53: Respondents may select multiple options so the number of responses will not add to the total number of people who answered this question (N=171). Similarly, the percents do not add to 100%.

Q54 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	199	95%
No	11	5%
Don’t know	0	0
Total	210	100.0%

Q55 In the last 12 months, has your organisation ever been unable to provide the official information asked for?

Response options	Number	Percent
Yes	74	37%
No	105	53%
Don’t know	20	10%
Total	199	100%

Q56 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 (that is, the record has not been created)?

Response options	Number	Percent
Often	1	1%
Occasionally	24	32%
Rarely	42	57%
Never	5	7%
Don't know	2	3%
Total	74	100.0%

Q57 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	26	35%
Rarely	33	45%
Occasionally	12	16%
Often	0	0.0%
Don't know	3	4%
Total	74	100.0%

Appendix 2

IM Maturity Assessment Topics

Categories		Topic
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.
Governance	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.
Governance	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.
Governance	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.

Categories		Topic
Governance	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.
Governance	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
Capability	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.

Categories		Topic
Creation	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.
Management	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.
Management	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.
Management	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 predefined 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.

Categories		Topic
Storage	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.
Access	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.
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.
Disposal	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.
Disposal	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 nonrespondents (A–Z)

Organisation name	Response
Abuse in Care Royal Commission of Inquiry	Complete
Accident Compensation Corporation	Complete
Accreditation Council	Complete
AgResearch Limited	Complete
Airways Corporation of New Zealand Limited	Complete
Animal Control Products Limited	Complete
Arts Council of New Zealand Toi Aotearoa	Complete
Ashburton District Council	Complete
AsureQuality Limited	Complete
Auckland Council	Complete
Auckland University of Technology	Complete
Bay of Plenty Regional Council	Complete
Broadcasting Commission	Complete
Broadcasting Standards Authority	Complete
Buller District Council	Complete
Callaghan Innovation	Complete
Canterbury Regional Council	Complete
Carterton District Council	Complete
Central Hawke's Bay District Council	Complete
Central Otago District Council	Complete
Chatham Islands Council	Complete
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
Controller and Auditor-General	Complete
Courts of New Zealand	Complete
Criminal Cases Review Commission	Complete
Crown Irrigation Investments Limited	Complete

Organisation name	Response
Crown Law Office	Complete
Department of Conservation	Complete
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
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	Complete
Government Communications Security Bureau	Complete
Government Superannuation Fund Authority	Complete
Greater Wellington Regional Council	Complete
Grey District Council	No response
Guardians of New Zealand Superannuation	Complete
Hamilton City Council	Complete
Hastings District Council	Complete
Hauraki District Council	Complete
Hawke’s Bay Regional Council	Complete
Health and Disability Commissioner	Complete
Health Promotion Agency	Complete

Organisation name	Response
Health Quality and Safety Commission	Complete
Health Research Council of New Zealand	Complete
Heritage New Zealand Pouhere Taonga	Complete
Horizons Regional Council	Complete
Horowhenua District Council	Complete
Human Rights Commission	Complete
Hurunui District Council	Complete
Hutt City Council	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
Invercargill City Council	Complete
Kaikōura District Council	Complete
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
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
Manawatu District Council[12]	No response
Maritime New Zealand	Complete
Marlborough District Council	Complete
Massey University	Complete

[12] We acknowledge that the Manawatu District Council engaged with us following the closure of the survey outlining the reasons they were unable to complete the survey this year. We thank the Council for that advice and their good will.

Organisation name	Response
Masterton District Council	Complete
Matamata-Piako District Council	No response
Mental Health and Wellbeing Commission	Complete
Meteorological Service of New Zealand Limited	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	No response
National Institute of Water and Atmospheric Research Limited	Complete
National Pacific Radio Trust	Complete
Nelson City Council	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
New Zealand Cadet Forces	Complete
New Zealand Customs Service	Complete
New Zealand Defence Force	Complete
New Zealand Film Commission	Complete
New Zealand Fish and Game Council	Complete

Organisation name	Response
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	Complete
New Zealand Police	Complete
New Zealand Post Limited	Complete
New Zealand Productivity Commission	Complete
New Zealand Qualifications Authority	Complete
New Zealand Security Intelligence Service	Complete
New Zealand Symphony Orchestra	Complete
New Zealand Tourism Board	Complete
New Zealand Trade and Enterprise	Complete
New Zealand Transport Agency	Complete
New Zealand Walking Access Commission	Complete
Northland Regional Council	No response
Office for Māori Crown Relations - Te Arawhiti	Complete
Office of the Clerk of the House of Representatives	Complete
Office of the Ombudsman	Complete
Opotiki District Council	Complete
Oranga Tamariki - Ministry for Children	Complete
Otago Regional Council	Complete
Otorohanga District Council	Complete
Palmerston North City Council	Complete
Parliamentary Commissioner for the Environment	Complete
Parliamentary Counsel Office	Complete
Parliamentary Service/Parliamentary Service Commission/ Parliamentary Corporation	Complete
Pharmaceutical Management Agency	Complete
Porirua City Council	Complete
Privacy Commissioner	Complete
Public Service Commission	Complete

Organisation name	Response
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	Complete
Rotorua Lakes Council	Complete
Ruapehu District Council	Complete
SCION	No response
Selwyn District Council	Incomplete
Serious Fraud Office	Complete
Social Workers Registration Board	Complete
South Taranaki District Council	Complete
South Waikato District Council	Complete
South Wairarapa District Council	Complete
Southland District Council	No response
Sport and Recreation New Zealand	Complete
Statistics New Zealand	Complete
Stratford District Council	Complete
Takeovers Panel	Complete
Taranaki Regional Council	Complete
Tararua District Council	Complete
Tasman District Council	Complete
Taumata Arowai	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

Organisation name	Response
Te Whare Wānanga o Awanuiārangi	Complete
Television New Zealand Limited	Complete
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	No response
Transport Accident Investigation Commission	Complete
Transpower New Zealand 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 Regional Council	Complete
Waimakariri District Council	Complete
Waimate District Council	Complete
Waipa District Council	Complete
Wairoa District Council	No response
Waitaki District Council	No response
Waitomo District Council	Complete
Wellington City Council	Complete
West Coast Regional Council	Complete
Western Bay of Plenty District Council	Complete
Westland District Council	Complete
Whakatāne District Council	No response
Whanganui District Council	Complete
Whangarei District Council	Complete
WorkSafe New Zealand	Complete

Te Rua Mahara o te Kāwanatanga
archives
NEW ZEALAND

archives.govt.nz