

# Report on the 2013 digital recordkeeping survey

## 1 Executive summary

Between February and March 2013 a survey was conducted with 279 public offices to measure compliance with the *Standard on digital recordkeeping* and more broadly to assess the implementation of digital recordkeeping within the NSW public sector.

The basis of the survey was provided by section 12(4) of the *State Records Act 1998* which requires each public office to report on its records management program in accordance with arrangements made with State Records.

The trends and issues highlighted by the survey results indicate that government business is transitioning to the digital environment and some public offices are doing excellent work in progressing their organisations into this new environment with appropriate digital recordkeeping.

However for the bulk of the NSW public sector this is not the case. Many organisations are grappling with the challenges of the digital environment. The absence of appropriate governance frameworks and identification of high risk business processes, is also making the transition more difficult and adding a level of risk to government business. Without the necessary frameworks and understanding of high risk business and critical processes, decisions will be made during the transition which could expose organisations to significant information loss and impair the delivery of services.

It is clear from the results of the survey that further work will be needed in the area from NSW public sector organisations in order to provide the necessary certainty that digital recordkeeping is fit for purpose. In addition, State Records will need to continue to develop, review and promote guidance to assist organisations with this transition.

## 2 Survey

### 2.1 Standard on digital recordkeeping

The *Standard on digital recordkeeping* was issued in September 2008, with minimum compliance requirements commencing from 30 June 2009.

Requirements within the Standard were phased in so that public offices had sufficient time to implement requirements. The Compliance timetable, issued with the Standard in 2008 (available from State Records' website), identifies the three tiers of requirements to be introduced from 30 June 2009 to 30 June 2012:

1. From 30 June 2009 public offices need to define digital records for any new system acquired or built after this date, ensure recordkeeping requirements are built into new systems and metadata mappings of new systems are made. Additionally all public offices were reminded that from the date of the issue of the Standard, the disposal of recordkeeping metadata should be in accordance with the requirements of the State Records Act 1998.
2. From 30 June 2011 public offices need to define digital records for high risk business processes supported by existing systems.
3. From 30 June 2012 public offices need to be able to demonstrate existing systems which capture and manage records of high risk business processes meet the requirements of a digital recordkeeping system as specified in the Standard and that metadata mappings of such systems are complete.

A survey was conducted in 2010 to assess the first phase of requirements of the Standard and progress with the implementation of the second phase of requirements.

The 2013 survey builds on this earlier work; seeking information on compliance with the Standard, the framework for digital recordkeeping and the implementation of digital recordkeeping in public offices. By looking at the framework, implementation and management of digital recordkeeping, we are able to assess the pace of transition to the digital environment and whether fundamental requirements were being implemented.

## **2.2 Survey pool**

279 public offices were surveyed, including

- 112 NSW Government agencies / authorities / state owned corporations (40% of survey pool)
- 141 local government organisations (51% of survey pool)
- 16 Local Health Districts (6% of survey pool), and
- 10 universities (3% of survey pool).

A number of public offices were excused from the survey process; including very small public offices (with less than 20 FTE staff), public offices which had been affected by natural disasters in NSW in early 2103, or those public offices who were involved in major organisational change. State Records believes that the results of the survey with 279 public offices can be extrapolated across all public offices and is indicative of the challenges that the NSW public sector is facing as it transitions to a digital environment.

The response rate for the survey was 100% with responses received from 279 public offices.

In the following discussion of survey results, percentages are used. For a complete statistical report on each question of the survey, please see **Appendix A**. For results by type of public office, please see **Appendix B**.

## **2.3 Survey questionnaire**

The survey questionnaire was divided into two sections: Management frameworks for digital recordkeeping and Implementing digital recordkeeping.

The first section allowed us to explore whether public offices have put frameworks in place to manage digital recordkeeping and ensure that requirements for digital recordkeeping have been incorporated into policy and procedure. The second section explored how public offices are managing records in a digital environment: the creation, management, accessibility, and disposal of digital records through assessing practices and processes for managing digital records in a range of systems, applications and environments.

The survey results are quantitative and will be used to report on compliance with the Standard and the broader implementation of digital recordkeeping in State Records' Annual Report. This information will also be applied to State Records' work in assisting public offices in implementing good digital recordkeeping practices.

## **2.4 Verification of survey responses**

State Records undertook a major process to verify survey responses. Public offices were advised in the survey questionnaire that as part of the assessment, they may be contacted and requested to provide documentation to support and validate survey responses.

Prior to the commencement of the survey, State Records selected three questions for the verification process (Questions 8, 9, and 29). It was also determined that only large, very large, or mega sized public offices who answered 'yes' to any of these questions would be contacted and asked to provide documentation to validate their response/s.

As a result of answering 'YES' to one or more of the pre-defined validation questions, 94 public offices were contacted and asked for documentation. As a result of our request, 11

public offices changed one or more answers from 'YES' to 'NO'. A total of 81 public offices provided documentation to verify their survey responses. This documentation confirmed responses and provided State Records with an opportunity to see how requirements and advice are being translated into practice. We thank public offices for their cooperation with the verification of survey responses.

### **3 Issues and trends in digital recordkeeping**

The discussion of responses to the survey below indicates that the NSW public sector is gradually making the transition to digital recordkeeping, however there are many challenges with moving from a paper paradigm to the digital environment and the implementation of sound digital recordkeeping.

One of the key risks to Government during the transition to the digital environment is the loss of information. Without appropriate information governance and management, Government risks losing business intelligence, opportunities for better service delivery, decision-making and accountability through digital recordkeeping.

Public offices will need to adopt better information governance and management practices and identify which of the organisation's business processes are high risk in order to implement appropriate digital recordkeeping and ensure that there are adequate records to support the organisation's high risk business.

In addition, it is important that all NSW Government agencies in particular are able to manage information assets adequately and within the requirements of the Government's ICT Strategy and the developing Information Management Framework. Projects coming out of the ICT Strategy are still ongoing and will support organisational transitioning to digital ways of working, managing and sharing information and building competencies. The policies and guidelines that come out of the Government's ICT Strategy will also be a resource that other sectors such as the universities and local councils can use and benefit from, where appropriate.

The survey findings provide a great deal of valuable information on the areas in which more work is needed to achieve better digital recordkeeping outcomes across the NSW public sector. At the end of each section, we have identified priorities for State Records and for public offices.

#### **3.1 Frameworks for digital recordkeeping (Questions 1–5, 11–14)**

The questionnaire assessed if public offices have been developing frameworks for the governance of digital recordkeeping. Good information governance and management ensures that roles, requirements, processes and monitoring are in place to ensure that an organisation is achieving effective and efficient use of its information. With digital environments, information governance becomes increasingly important, because if requirements, processes and monitoring are not implemented, there is a lack of accountability and a real risk of information loss for the organisation.

It was pleasing to learn that most public offices (84%) have assigned responsibility for digital information and digital records to a senior or executive level officer. A challenging area for organisations is the setting of policy and recordkeeping rules for a range of social media applications. While use varies across the public sector the following was reported:

- 23% have policy and recordkeeping rules for Facebook
- 18% have policy and recordkeeping rules for Twitter
- 11% have policy and recordkeeping rules for Blogs
- 6% have policy and recordkeeping rules for Wikis
- 5% have policy and recordkeeping rules for Yammer.

The survey identified that many public offices do not use Blogs, Wikis or Yammer.

It is a similar story for the setting policy and recordkeeping rules for a range of business applications and devices:

- 55% have policy and recordkeeping rules for shared network drives
- 49% have policy and recordkeeping rules for websites
- 45% have policy and recordkeeping rules for the intranet.
- 36% have policy and recordkeeping rules for mobile devices
- 32% have policy and recordkeeping rules for portable storage
- 13% have policy and recordkeeping rules for instant messaging
- 13% have policy and recordkeeping rules for SharePoint.

Setting policy and recordkeeping rules for the use of shared network drives, web sites, applications and devices within an organisation is important and sets the basis for good recordkeeping and information management practices. Without policy and rules, staff do not know what is expected and what to do, and recordkeeping is likely to suffer.

Email was one area where we were pleased to see that frameworks have been established: 85% of public offices reported that they had set policy and recordkeeping rules for the use of email while 87% have policy and procedures for the capture of business-related email into the organisation's recordkeeping system. A significant number of public offices provided some form of training for staff in their responsibilities to capture business related emails (80%). While public offices have invested resources in developing frameworks for managing email, only 27% of public offices monitor conformity with these requirements and 24% monitor only some key or high level staff or high risk business processes. Pleasingly, 78% of public offices report that they can identify and retrieve emails when required.

Email is widely used in the NSW public sector as the driver of the vast majority of high level business decisions and to perform a large number of business transactions internally and externally. Policy, coordination, senior management and governance processes use email as their dominant business system. Significant evidence of corporate decision making is therefore likely to be captured in email messages, and messages are therefore likely to have ongoing value to organisations (both to support current business and as evidence that may be required beyond the immediate business needs for the information). Good email management, by capturing emails of business activity, ensures that the emails are available to facilitate business decisions and to provide evidence of decision-making.

While many public offices identified that they do not use shared services or outsource functions, the requirement to include recordkeeping requirements / rules in contractual arrangements is starting to gain some momentum with 26% of public offices including requirements in shared services agreements and 35% including requirements in outsourcing arrangements. Of concern here is that there are public offices entering shared services (24%) and outsourced arrangements (21%) without specifying recordkeeping requirements. As Government enters into more shared services arrangements or outsources functions to other providers, it is critically important that recordkeeping is addressed as part of these arrangements so as to ensure that accountability for the delivery of services, in the form of reliable records, is available for scrutiny.

A pleasing result in the development of the framework is the emphasis that public offices are placing on ensuring all staff and contractors are aware of their responsibilities to create and capture records. 72% of public offices provide training to ensure that staff and contractors are aware of their responsibilities to create and capture digital records.

---

### **Priorities for State Records**

---

Review and promote email management guidance  
Issue and promote guidance on social media and information management strategies  
Promote the Information Management Framework being developed within NSW Government

### **Priorities for public offices**

Develop business rules and identify recordkeeping requirements for the different business tools and systems used  
Promote awareness in staff, contractors and service providers of business rules and recordkeeping requirements for key business processes

## **3.2 Defining the digital records required by your organisation (Questions 6–8, 15, 21-22, and 44)**

The survey examined the implementation of requirements from the Standard to ensure that recordkeeping requirements were built into business systems (for new systems only) and that digital records for high risk business processes were defined (for new systems and systems implemented prior to June 2012).

39% of public offices have policies and procedures which require that digital recordkeeping functionality is incorporated into any new business systems design. However, 40% answered that they did not have policies or procedures in place. This requirement is fundamental to ensuring that new business systems acquired by organisations are able to create and maintain records of the business that is being undertaken. In analysing this question, it is clear that all types of public offices are struggling to implement this requirement.

47% of public offices reported that they have identified their high risk business processes and the digital records that need to be created and retained to support these processes (33% have partly done this and 20% reported that they had not done this). Understanding the high risk business processes of the organisation is fundamental to taking a planned, risk based approach, to ensuring that the public office has digital records of the most critical and high risk aspects of its business. Without such records, public offices are unlikely to be able to withstand scrutiny of these high risk business processes.

From our analysis, we found that local health districts (56%) and universities (50%) have been predominately undertaking this work, while to a lesser extent agencies / authorities / state owned corporations (47%) and councils (45%) have identified high risk business processes and the records that are required to be created and retained to support these processes.

Of the organisations that have identified their high risk business processes, a pleasing 62% undertake internal auditing or monitoring of high risk business processes to ensure that digital records are made and captured. This means that 138 organisations are actively ensuring that they have adequate records for their high risk business processes, but ultimately this is only 49% of the public offices who were surveyed.

Public offices were able to identify that they are managing particular types of digital records:

- 88% reported that they are scanning/digitising some incoming paper correspondence
- 80% scan/digitise existing paper files to improve accessibility
- 64% are creating and managing complex records such as 3D engineering records, CAD files etc.

Another aspect to defining digital records, is to be aware of the different technologies and storage repositories that are being used for digital recordkeeping. 79% of public offices reported that they are still using shared drives for storing digital records. This means that a proportion of an organisation's digital records are on the network outside of the corporate recordkeeping system. This poses issues for the organisation in identifying and accessing all digital records when required, and also raises issues concerning the security and possible unauthorised alteration or deletion of digital records. The legacy of digital records on shared network drives is one that many public offices will need to proactively manage over the next few years.

#### **Priorities for State Records**

Develop and promote further guidance / templates for identifying high risk business processes

#### **Priorities for public offices**

Identifying high risk business processes

Monitor high risk business processes to ensure digital records are made and captured

### **3.3 Digital disposal (Questions 16–20)**

The survey results indicate that there is very little disposal of digital records in EDRMS or designated recordkeeping systems:

- 11% disposed of digital records in EDRMS in the last 6 months
- 4% disposed of digital records in EDRMS in the last year
- 8% disposed of digital records in EDRMS in the last 2 years, and
- 77% have not disposed of digital records held in the EDRMS

Based on feedback provided in the survey, some of the reasons public offices do not dispose of digital records are:

- records in the EDRMS have not yet reached the end of their retention period
- EDRMS has only been implemented in the last 7 years
- the organisation has not implemented retention and disposal authorities into the system due to system issues
- no retention and disposal authority for the organisation
- decision by organisation to retain all records, particularly as there is 'no imperative to dispose of digital records as there is adequate storage capacity', and
- limited resources to implement digital disposal

For a number of organisations, aspects of recordkeeping is still a paper-based activity and there are no digital records in the EDRMS. This is concerning because these organisations have not yet commenced the transition to digital recordkeeping.

The issue of disposal of records in business systems is just as concerning. Only 46% of public offices identify retention periods for digital records when developing requirements for new business systems and 22% reported this is done only sometimes. For existing business systems, only 28% know which digital records in *all* systems will need to be kept for 5 or more years, while 49% know which digital records in *some* systems will need to be kept for 5 or more years. We can not be sure of the reason for this situation – and it may be that some organisations are taking a risk based approach and only identifying retention requirements in systems that support high risk business. However, this is unlikely to be the situation in all cases.

In asking public offices how they dispose of digital records in business systems, we were concerned by the results:

- 38% will address disposal of digital records in business systems in the future
- 30% don't dispose of any digital records in business systems
- 21% are likely to keep all digital records in business systems
- 19% will dispose as part of system migrations
- 17% will dispose as part of system decommissioning, and
- 5% don't know how the organisation disposes of digital records in business systems.

Overall, these results make it clear that disposal of digital records in an EDRMS or designated recordkeeping systems or business systems is not occurring and there is inadequate planning for disposal. This poses a range of issues for Government including:

- increasing data storage costs as more organisations store more data in systems
- system inefficiencies as there is no disposal of data and systems have to process more and more data
- increasing migration costs as more data is migrated forward rather than using the migration process as an opportunity to identify and dispose of data
- increase of poorly controlled and managed data retained sitting in legacy systems, and
- more data means slower retrieval or ineffective retrieval of the data required by users.

Organisations should also be aware that any information held in systems are subject to GIPA requests and legal discovery. These requirements apply to backup tapes, personal mobile devices that are also used for business purposes, government social media accounts and offline storage systems.

For State Records, understanding the challenges and obstacles for disposal in the digital environment will assist in providing more practical advice in this area.

<b>Priorities for State Records</b>
-------------------------------------

Develop and promote guidance on undertaking disposal in the digital environment
---

<b>Priorities for public offices</b>
--------------------------------------

Plan and undertake disposal in the digital environment
--

### **3.4 Migrating digital records (Questions 9–10, 19-20, 41-43)**

In a digital environment, a key or the primary means of keeping records accessible for as long as they are required to meet ongoing business and accountability requirements is to migrate the records to the next version of software or application. It is important that such critical work is underpinned by policies and procedures.

Only 25% of public offices have policies or procedures for migrating digital records. Given that migration is such primary means of ensuring accessibility to digital records, this is a particularly concerning result. Of the 70 organisations who have established requirements for migrating digital records, a pleasing 79% include the migration of metadata from one system or another and identify the disposal process for digital records that are not migrated forward.

The migration of digital records is a time of risk for digital records and their metadata. The sustainability of long term government business information and the maintenance of

digital archives into the future will be reliant on the success of migration projects. The lack of proactive migration consideration and planning at present is a risk to information sustainability and a potential risk to Government business. State Records will be looking at how it can provide clearer advice about core migration principles and requirements, to help organisations plan for strategic information migration.

State Records is aware that some public offices are undertaking regular migrations of systems which include the disposal of records. 19% of public offices identified that this was one of the strategies that they were undertaking to dispose of records from business systems. Pleasingly, all public offices that do undertake disposal as part of system migrations are confirming the quality and success of a migration before destroying the source records.

Fundamental to the migration of digital records is understanding the configuration of the business systems. Documenting systems configuration has some way to go. 50% of public offices have documented the configuration of key business systems. 26% of public offices (74 organisations) use SAP and 31 organisations (42%) have documented the configuration of SAP; 36% of public offices (101 organisations) use SharePoint and 69 (68%) have documented the configuration of SharePoint.

It is important that all public offices develop the proper frameworks for the migration of digital records and metadata in order to ensure that the risks associated with migration are minimised.

The management and successful execution of migrations is essential to ensure the continuity of digital information for as long as it is needed. As more information – about customers, service provision, infrastructure, financial management, land management and so on – is created and managed digitally, then ensuring that adequate digital continuity strategies are in place is essential. These strategies and approaches provide assurance and certainty that digital records will remain useable and accessible for as long as it is required.

#### **Priorities for State Records**

Develop and promote further information on migrating digital records

Sample policy or procedures on migrating digital records

#### **Priorities for public offices**

Adequately plan for the migration of high risk business and long-term records

### **3.5 Recordkeeping and business systems (Questions 23–27)**

Questions 23 to 27 of the survey questionnaire examined how public offices are managing recordkeeping in business systems. The results in this section are interesting because they reveal that many public offices have yet to grapple with governance issues and information management requirements in business systems.

36% of public offices have identified all the owners of the business systems which hold records of high risk business, 21% have a partial listing and 15% are planning to do this in 2013/2014 as part of information asset inventory. As this work is fundamental to the governance of these systems and their ongoing management we would encourage all public offices to progress this work as a priority.

Of those public offices who have a complete or partial listing or are planning to do this work, we sought to find out if the listing of systems would be more than an information asset inventory and include information about whether the system was creating and capturing record and had recordkeeping functionality. 48% of respondents have done such work, whereas 42% of respondents do not have such listings which incorporate recordkeeping information.

We were also interested to find out how many organisations had integrated business systems with an EDRMS as a strategy for ensuring that records were captured and maintained:

- 55% have integrated 1- 4 business systems
- 8% have integrated 5 – 10 business systems
- 2% have integrated more than 10 business systems, and
- 35% have not integrated any system.

Perhaps the most poorly understood questions in the survey were Questions 26 and 27. Question 26 required organisations to identify 3 key business systems which perform recordkeeping processes and to identify whether the systems capture recordkeeping process metadata with the digital record. Most public offices identified key business systems, but many were unable to advise if the metadata was captured with the record.

Question 27 required organisations to identify 3 business systems which support high risk business processes which have records of long-term value (to be retained for more than 20 years) or State archives. Many organisations could not answer this question as they haven't identified high risk business processes nor have they assessed which systems hold long term records.

Information on systems in use in public offices provided in response to Questions 26 and 27 will be used by State Records to underpin the development of further guidance on identifying high risk business processes.

The lack of work in this area by public offices is perhaps underpinned by a lack of understanding of the need to ensure that business systems are able to manage records or integrate with other systems that can manage records. The responsibility to ensure that digital business processes are adequately supported by digital records able to provide evidence of and accountability for decisions and actions is a business issue, not just an ICT matter.

#### **Priorities for State Records**

Develop and promote further guidance / templates for identifying high risk business processes

#### **Priorities for public offices**

Identify which business systems support high risk business processes

### **3.6 Recordkeeping in the cloud (Questions 28–33)**

With Government increasingly using cloud based services, we were interested to know what types of services were being used by public offices:

- 32% use cloud based applications
- 20% use cloud based services
- 15% use data storage in the cloud
- 13% use cloud based business operations.

Interestingly, 53% of public offices report that they do not use cloud based services at all.

Of those public offices that do use the cloud, 53% reported that they have undertaken a risk assessment of business and recordkeeping risks before using cloud-based services. Further analysis identified that 60% of universities have undertaken risk assessments, whereas only 26% of government agencies/state owned corporations have done this work.

72% reported that the services used have export functionality which would allow for the retrieval or return of records to the organisation. 45% reported that they haven't tried to bring digital records back into corporate systems, while 24% didn't have any issues with bringing digital records back into corporate systems during or at the end of the contract period.

### **Social media**

Key government business processes including policy development, community engagement, emergency management, business collaboration and project management are increasingly moving to social media channels which are hosted by third party organisations in the cloud. The NSW ICT Strategy is encouraging the widespread use of social media for government business.

State Records is aware that maintaining important information in these environments can be very challenging. We found that only 11% of public offices have strategies for making and keeping digital records that support the organisation's key social media activities. Of those organisations who do have strategies, we found that 14% use maintaining tweets of high risk business activities in Twitter as their strategy (the default option and not really a management strategy) and 7% capture these types of tweets into 3<sup>rd</sup> party software and then into their EDRMS. Interestingly, 39% of organisations with strategies noted that they don't tweet in relation to high risk business activities.

The responses to the questions on social media indicate that information management frameworks within public offices are not transitioning to incorporate records created in social media. As Government moves to new business environments and uses new technologies to do business, there is a real risk of information and business intelligence being lost unless the necessary frameworks are put in place.

#### **Priorities for State Records**

Issue and promote guidance on social media and information management strategies  
Develop and promote further guidance on recordkeeping and cloud-based services

#### **Priorities for public offices**

Undertake assessments of business activities conducted in or through these environments (social media, cloud services) and develop recordkeeping strategies based on business risk and information risks

### **3.7 Managing digital records over time (Questions 34-40)**

The last section of the survey questionnaire looked at the management of digital records over time and included questions about legacy or older business systems and how they are currently managed, accessibility of data in legacy or older systems, how organisations are managing longer term retention of digital records, identification of State archives in systems and intentions to transfer these records to State Records as digital archives in the near future.

58% of public offices have legacy systems or older business systems which they are currently managing. Interestingly, most local health districts have legacy or older systems, whereas 58% of councils, 54% of agencies/state owned corporations, and 50% of universities identified that they were managing legacy or older business systems.

162 public offices are using a range of strategies to manage these systems and it is clear from responses that public offices are deploying multiple strategies to manage these digital records:

- 65% migrate the digital records in legacy or older systems to new systems

- 62% retire legacy and older systems, retain the system and maintain the digital records within the system
- 10% have assessed legacy and older systems as low risk and the systems have been turned off, and
- 7% retire legacy and older systems, do not retain systems, and records are not migrated or accessible.

Of the public offices who have legacy or older systems that have not been migrated, 88% are able to access the data held in these systems.

It is clear that public offices are starting to consider how they manage the long term retention of digital records in key business systems, with 99% of public offices providing a response to this question. Responses included IT solutions such as backups and digital archiving, disposal of records from systems using authorised disposal and retention authorities, and some public offices were aware but unsure what they should do manage their digital records into the long term. We have concerns that public offices see backups as an appropriate response for the long term retention of digital records. While this is an appropriate disaster management strategy, it is not an appropriate long term management strategy. Digital records held on backup tapes will likely be only accessible for 2–3 years, which is not ideal if the record is required to be kept for longer than 20 years or permanently as a digital State archive.

53% of public offices have also started to identify digital State archives in their EDRMS systems and key business systems. 87% of public offices provided a response to the types of systems that hold these digital State archives, however in most cases, public offices only nominated their EDRMS and did not include any other business systems in use within their organisations. At this stage only 7% are planning to transfer these digital State archives in the next 12 months. We anticipate that the intention/planning to transfer response will increase once the Digital State archives project is fully operational.

#### **Priorities for State Records**

Work to deliver a fully functional Digital State archive for public offices

Develop and promote guidance on migrating State archives to the Digital State archives

#### **Priorities for public offices**

Identify long term digital records and implement appropriate preservation strategies to ensure that the records remain accessible, including migration to Digital State archives.

## **4 In conclusion**

The trends and issues highlighted by the survey results indicate that NSW public sector organisation are transitioning their business processes to the digital environment and some public offices are doing excellent work in progressing their organisations into this new environment with appropriate digital recordkeeping.

However for many of the NSW public sector this is not the case. Many organisations are grappling with the challenges of the digital environment. The absence of appropriate governance frameworks and the failure to identify high risk business processes, is also making the transition more difficult and adding a level of risk to government business. Without the necessary frameworks and understanding of high risk business and critical processes, decisions will be made during the transition which could expose organisations to significant information loss and impair the delivery of services.

It is clear from the results of the survey that further work will be needed in a number of areas from both State Records and the NSW public sector to provide the necessary certainty that digital recordkeeping is fit for purpose.

*Priorities for State Records include:*

- Review and promote email management guidance
- Issue and promote guidance on social media and information management strategies
- Promote the Information Management Framework being developed within NSW Government
- Develop and promote further guidance / templates for identifying high risk business processes
- Develop and promote guidance on undertaking disposal in the digital environment
- Develop and promote further information on migrating digital records
- Sample policy or procedures on migrating digital records
- Develop and promote further guidance on recordkeeping and cloud-based services
- Work to deliver a fully functional Digital State archive for public offices
- Develop and promote guidance on migrating State archives to the Digital State archives.
- Advise Department of Finance and Services' Strategic Policy of findings of the survey
- Work with Department of Finance and Services' Strategic Policy to improve digital recordkeeping in public offices

*Priorities for public offices include:*

- Develop business rules and identify recordkeeping requirements for the different business tools and systems used
- Promote awareness in staff, contractors and service providers of business rules and recordkeeping requirements for key business processes
- Identifying high risk business processes
- Identify which business systems support high risk business processes
- Monitor high risk business processes to ensure digital records are made and captured
- Plan and undertake disposal in the digital environment
- Adequately plan for the migration of high risk business and long-term records
- Undertake assessments of business activities conducted in or through these environments (social media, cloud services) and develop recordkeeping strategies based on business risk and information risks
- Identify long term digital records and implement appropriate preservation strategies to ensure that the records remain accessible, including migration to Digital State archives.

## **Appendix A: Survey statistics**

*What type of public office is your organisation?*

- 40% NSW Government agencies / authorities / state owned corporations
- 51% local government organisations
- 6% local health districts, and
- 3% universities.

*What size is your organisation?*

- 20% are small (20 – 80 FTE)
- 33% are medium sized (80 – 250 FTE)
- 26% are large (250 – 1000 FTE)
- 19% are very large (1000 – 10, 000 FTE)
- 2% are mega (10,000+ FTE)

*Is your organisation using a shared services arrangement for the delivery of records management services and operations?*

- 17% responded YES
- 79% responded NO
- 4% responded that planning is in place to transition to shared services in 2013 which will likely include records services

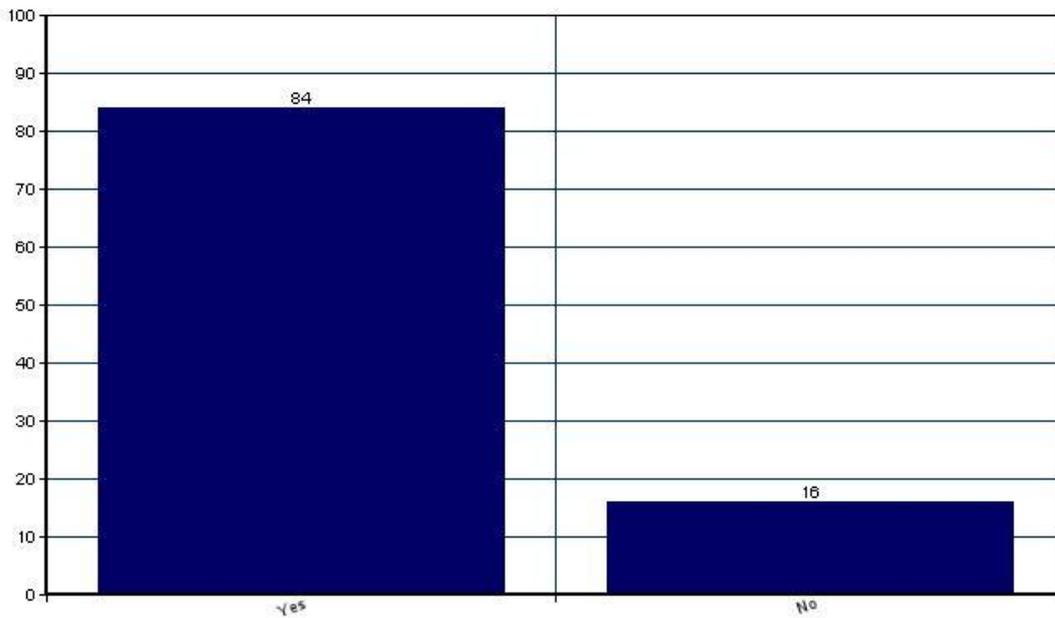
*Does your organisation have access to strategic whole-of-organisation records and information management advice and knowledge?*

- 64% responded Yes, we have access to an in-house fulltime records management resource
- 16% responded Yes, we have access to an in-house part time records management resource
- 10% responded Yes, we have access to strategic records and information management advice and knowledge but don't have a resource on staff
- 10% responded No, we don't have access to strategic records and information management advice and knowledge.

**In the following graphs, all results are in percentages.**

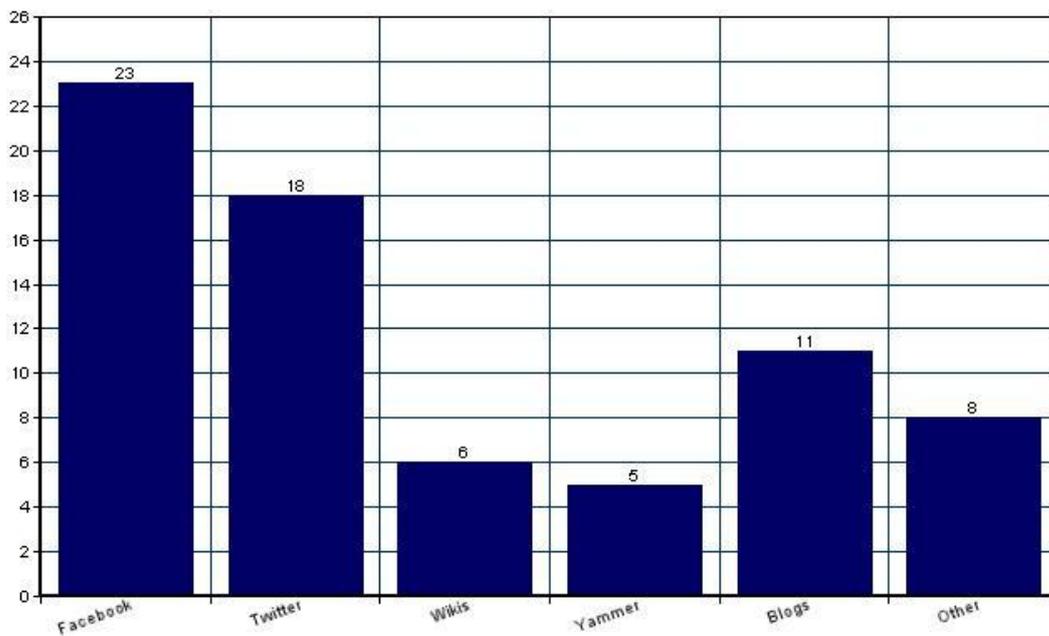
**Question 1: Does your organisation assign responsibility for digital information and digital records to a senior or executive level officer?**

Question 1



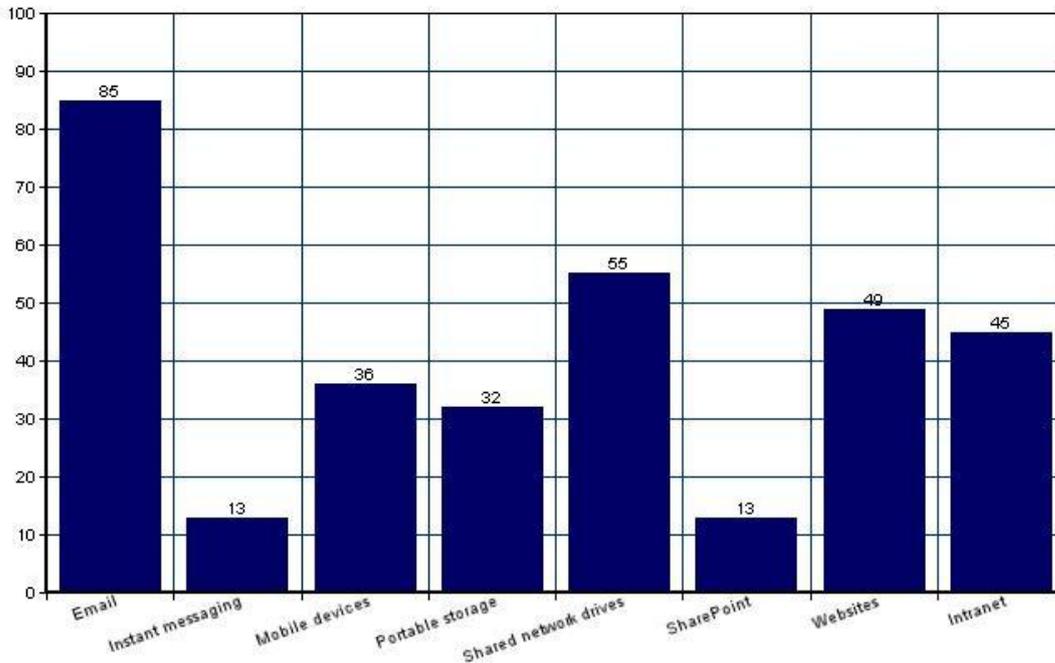
**Question 2: Has the organisation set its policy and recordkeeping rules for the use of the following social media applications?**

Question 2



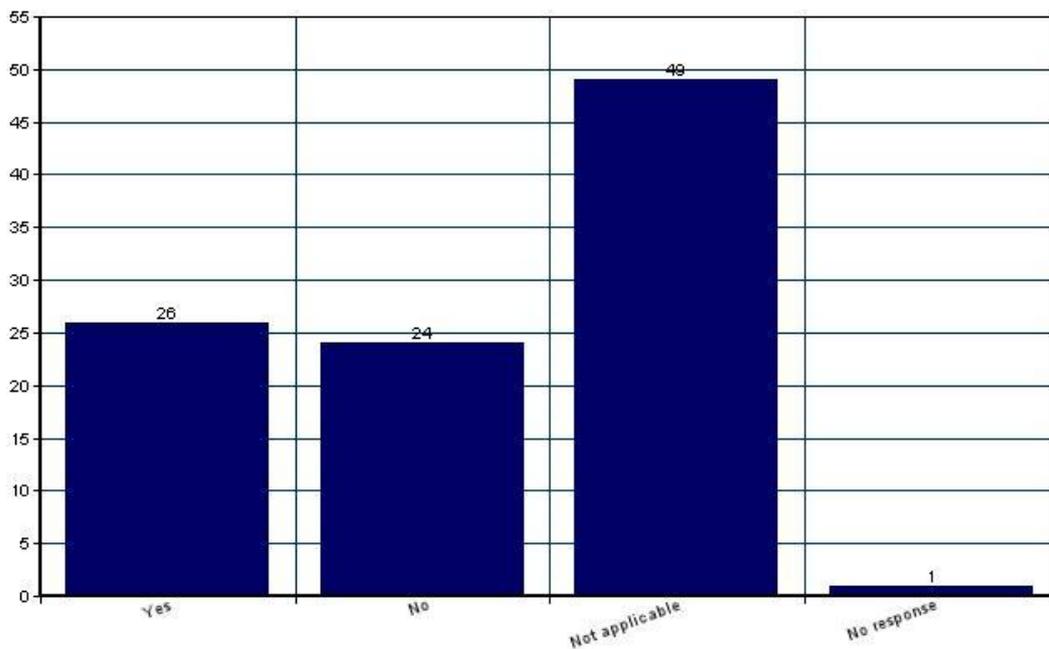
**Question 3: Has the organisation set its policy and recordkeeping rules for the use of the following devices and business applications?**

Question 3



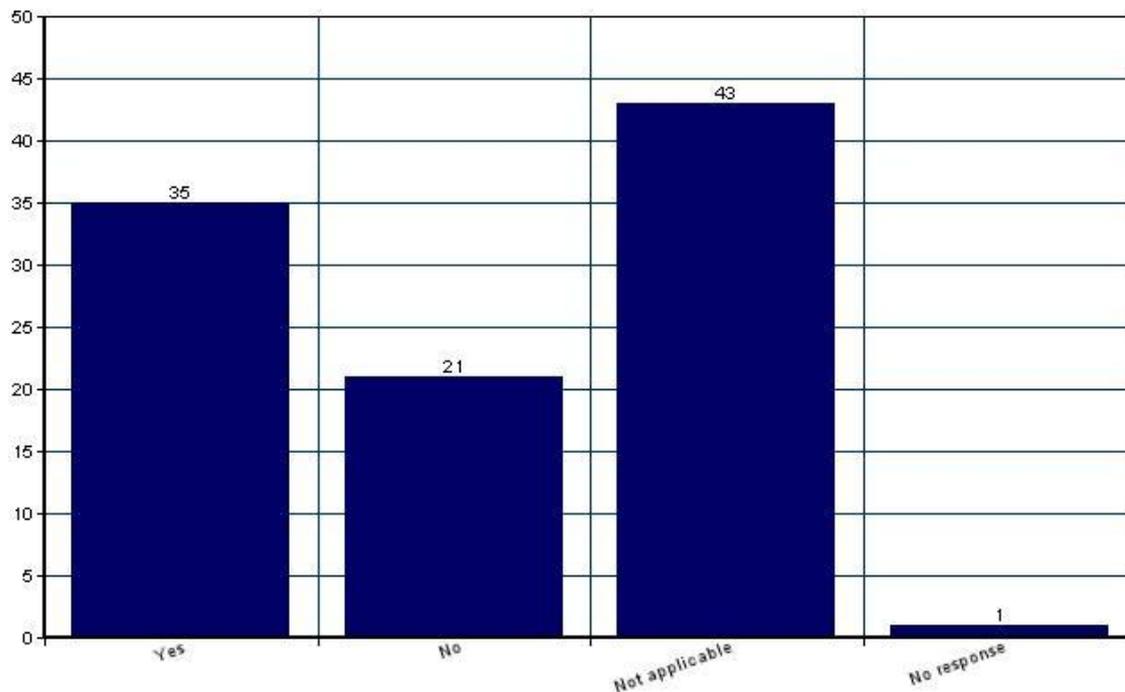
**Question 4: Are recordkeeping requirements included in shared service or in-sourcing arrangements?**

Question 4



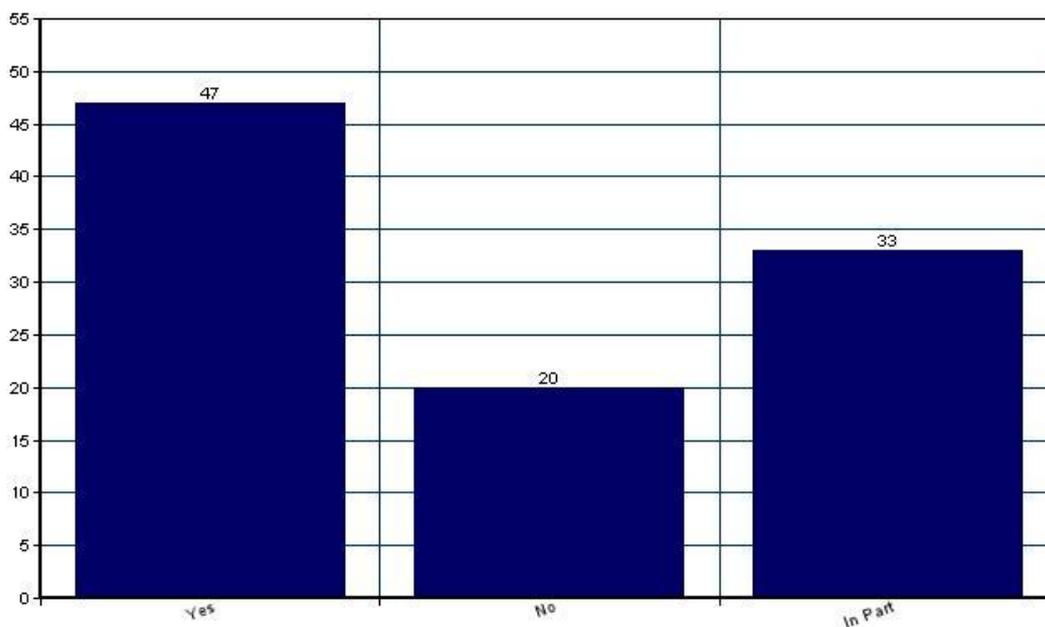
**Question 5: Are recordkeeping requirements included in outsourced arrangements?**

Question 5



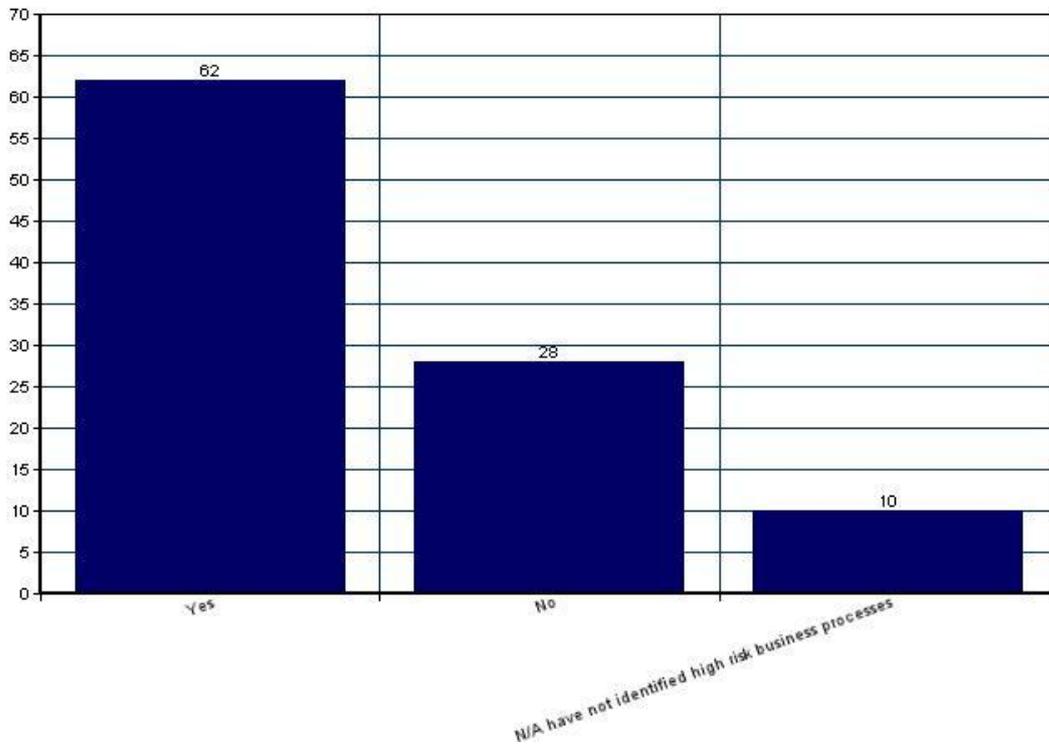
**Question 6: Has the organisation identified its high risk business processes and the digital records that it needs to create and retain in support of these processes?**

Question 6



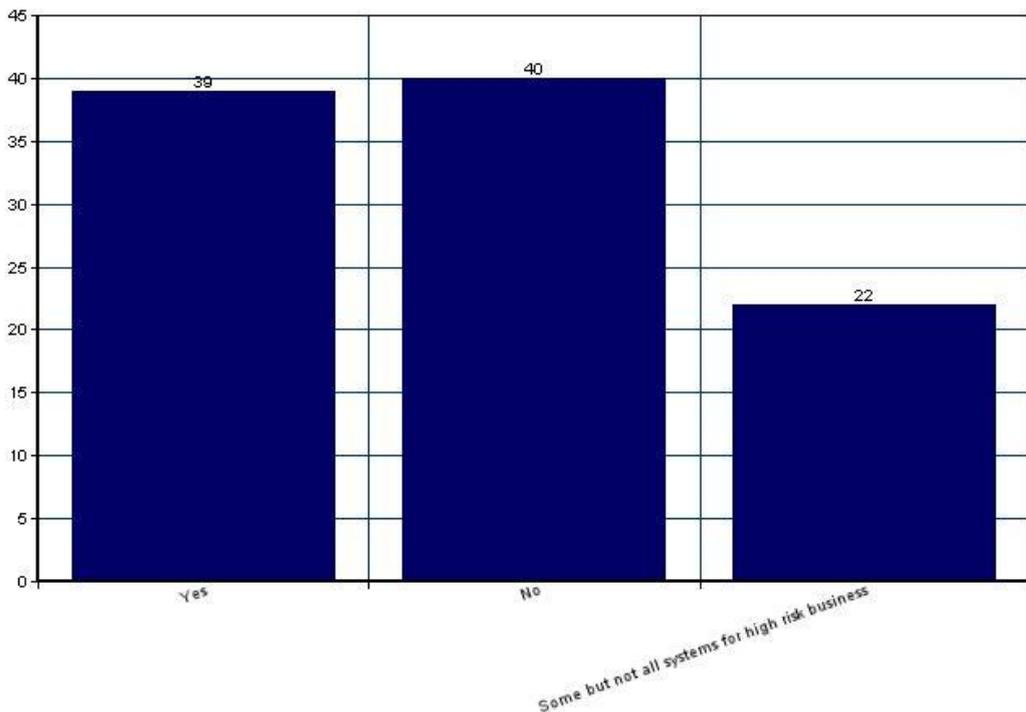
**Question 7: Does your organisation undertake internal auditing or monitoring of high risk business processes to ensure that digital records are made and captured?** *Question answered by 223 public offices; question skipped by 56 public offices*

Question 7



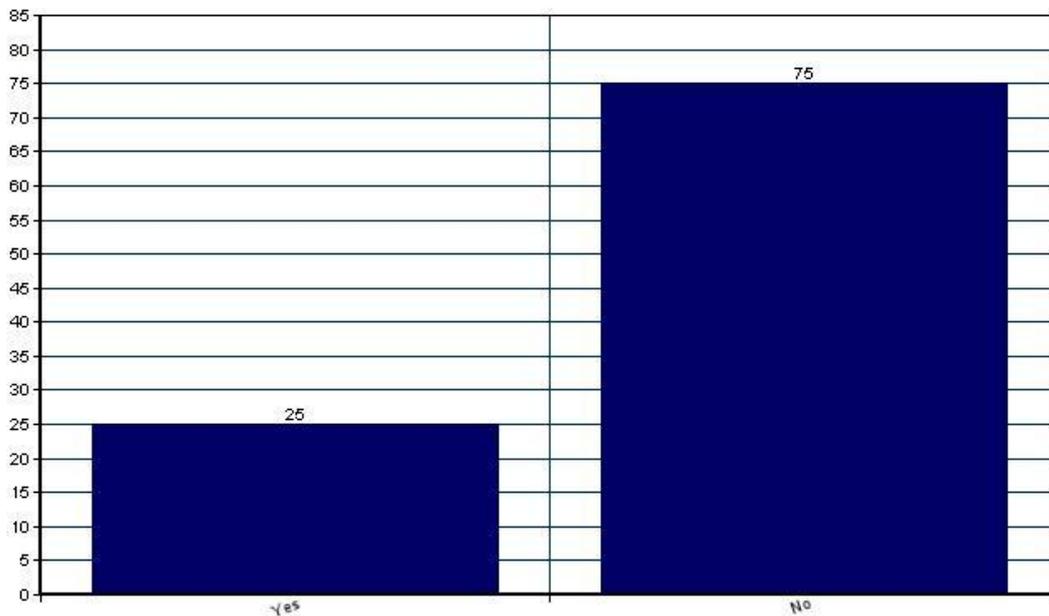
**Question 8: Does your organisation have policies or procedures which require that digital recordkeeping functionality is incorporated into any new business systems design?**

Question 8



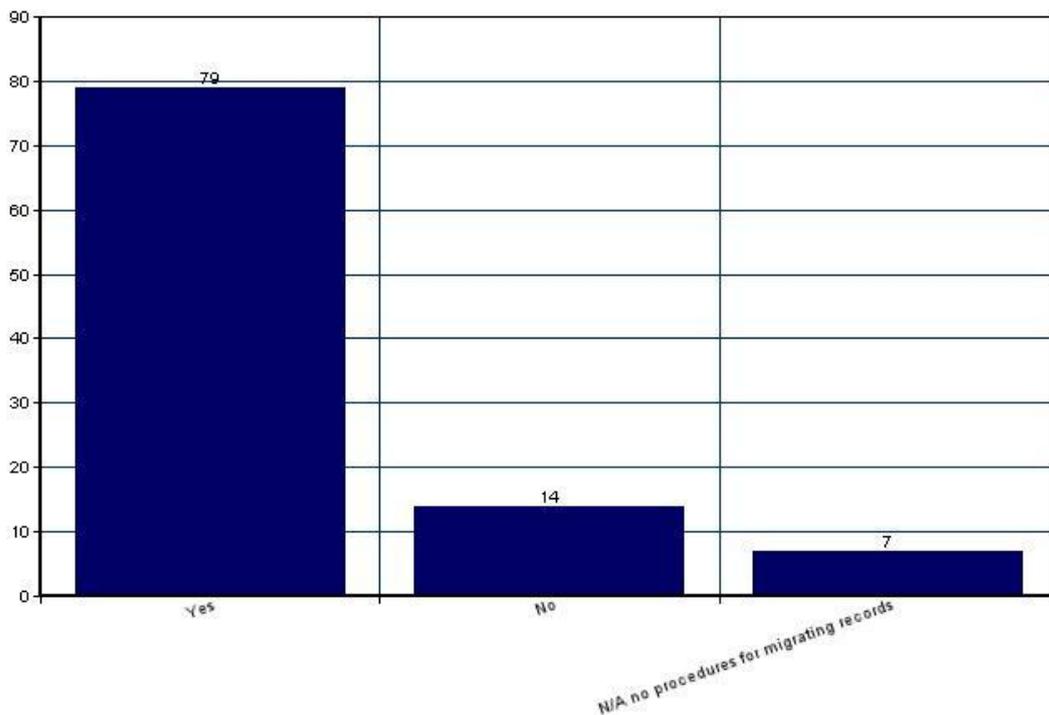
**Question 9: Does your organisation have policy or procedures for migrating digital records?**

Question 9



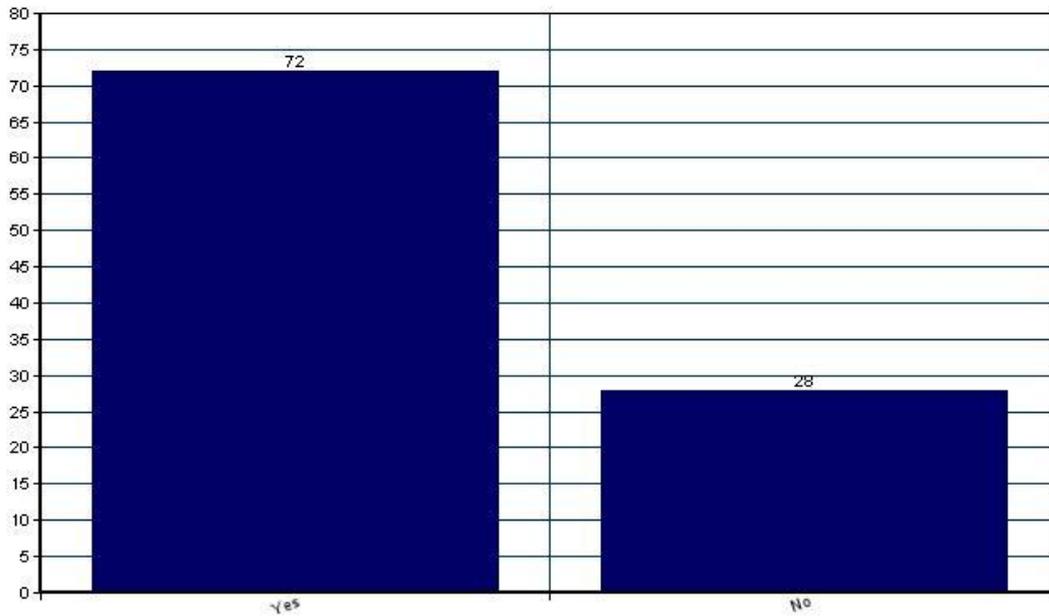
**Question 10: Does the policy or procedures include the migration of metadata from one system to another and identify the disposal process for digital records not migrated forward?** *Question answered by 70 public offices; question skipped by 279 public offices*

Question 10



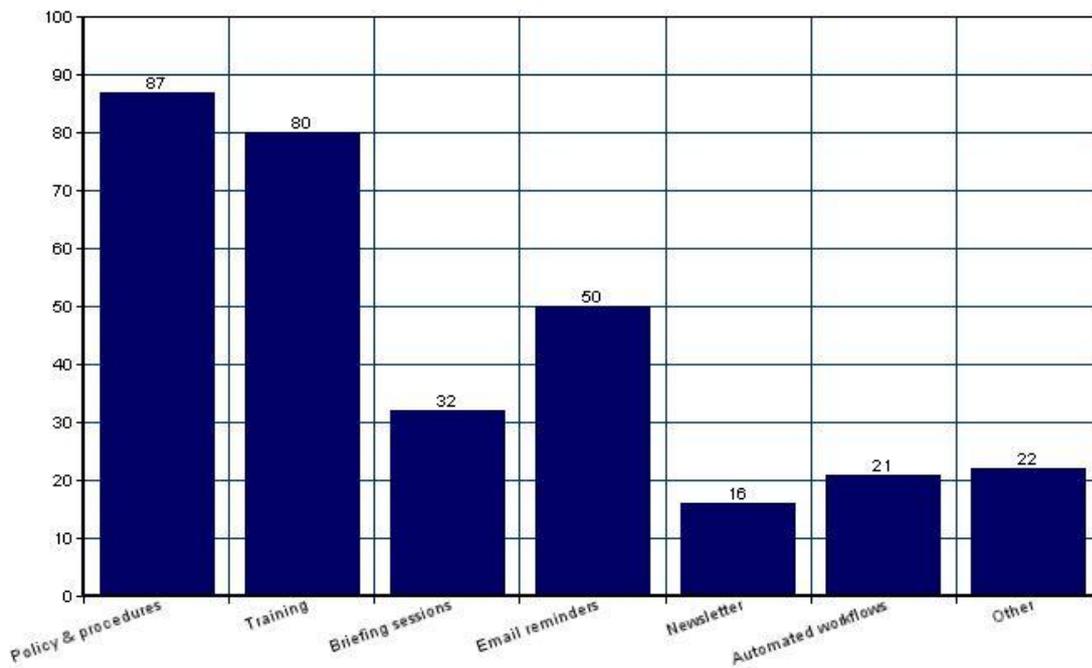
**Question 11: Does your organisation provide training to all staff and contractors on meeting their responsibilities to create and capture full and accurate digital records?**

Question 11



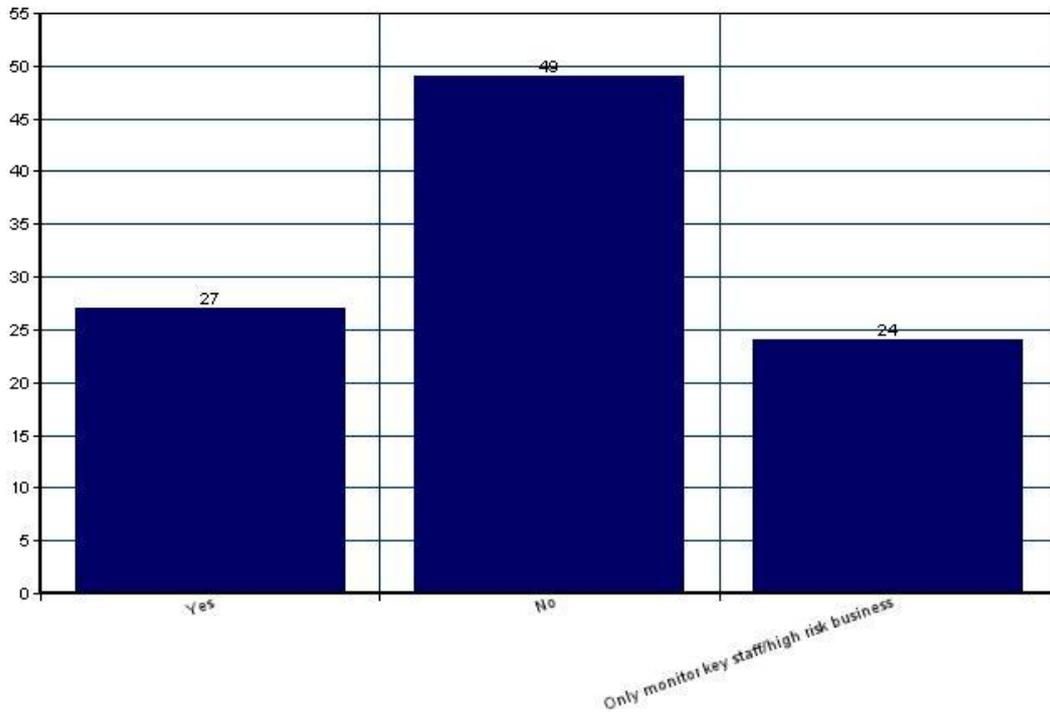
**Question 12 How does your organisation inform staff of their responsibility to capture business-related email into the organisation's recordkeeping system (e.g. into EDRMS or designated recordkeeping system)? Respondents could tick as many options as apply**

Question 12



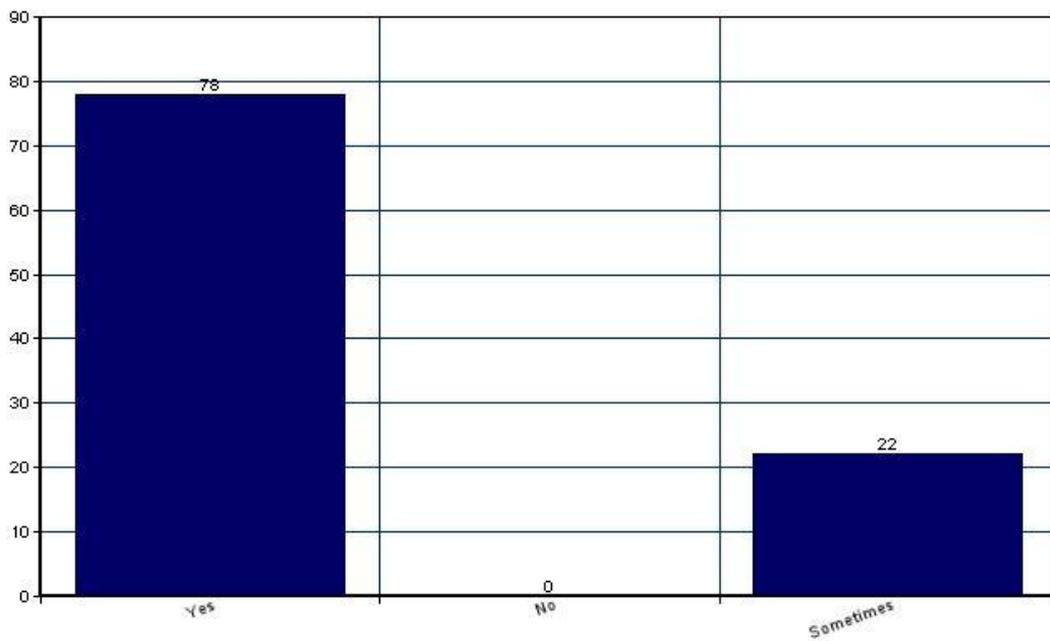
**Question 13 Does your organisation monitor compliance with requirements to capture business-related emails into the organisation's recordkeeping system (e.g. into EDRMS or designated recordkeeping system)?**

Question 13



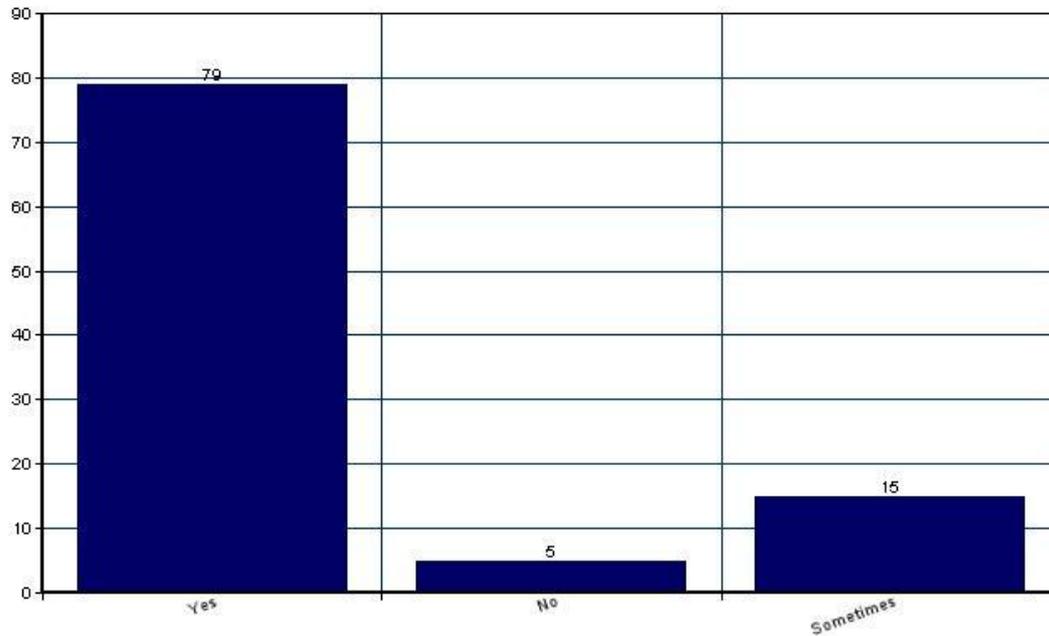
**Question 14 Are you or other staff able to identify and retrieve emails when required?**

Question 14



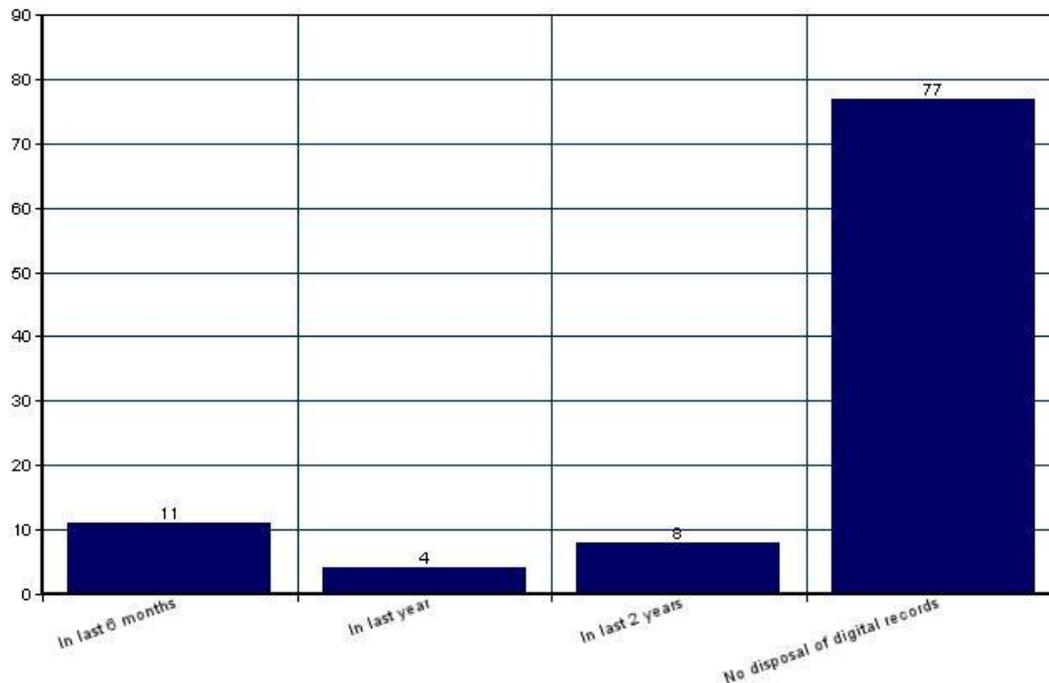
**Question 15: Does your organisation use shared drives for storing digital records?**

Question 15



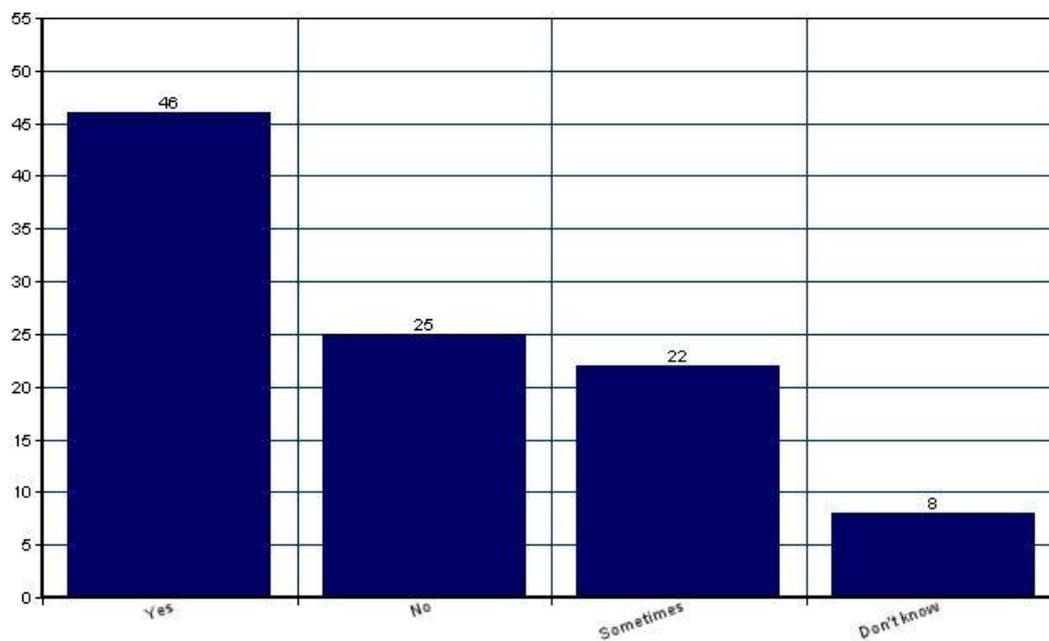
**Question 16: Has your organisation disposed of digital records held in the organisation's designated recordkeeping system and/or EDRMS?**

Question 16



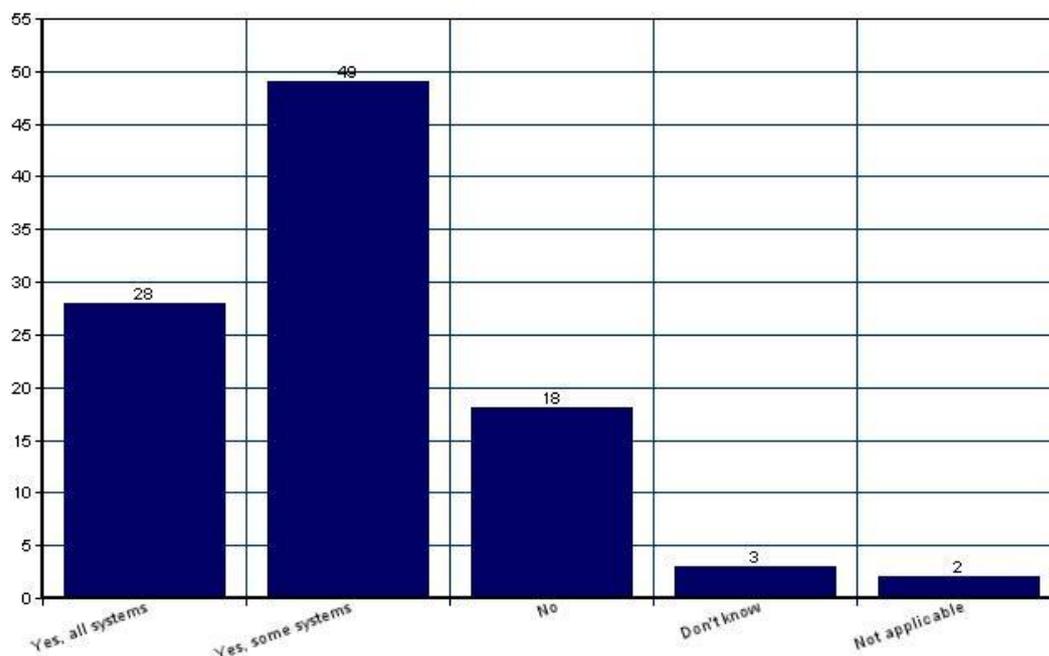
**Question 17: When developing requirements for new business systems, does the organisation consider and address retention periods for digital records?**

Question 17



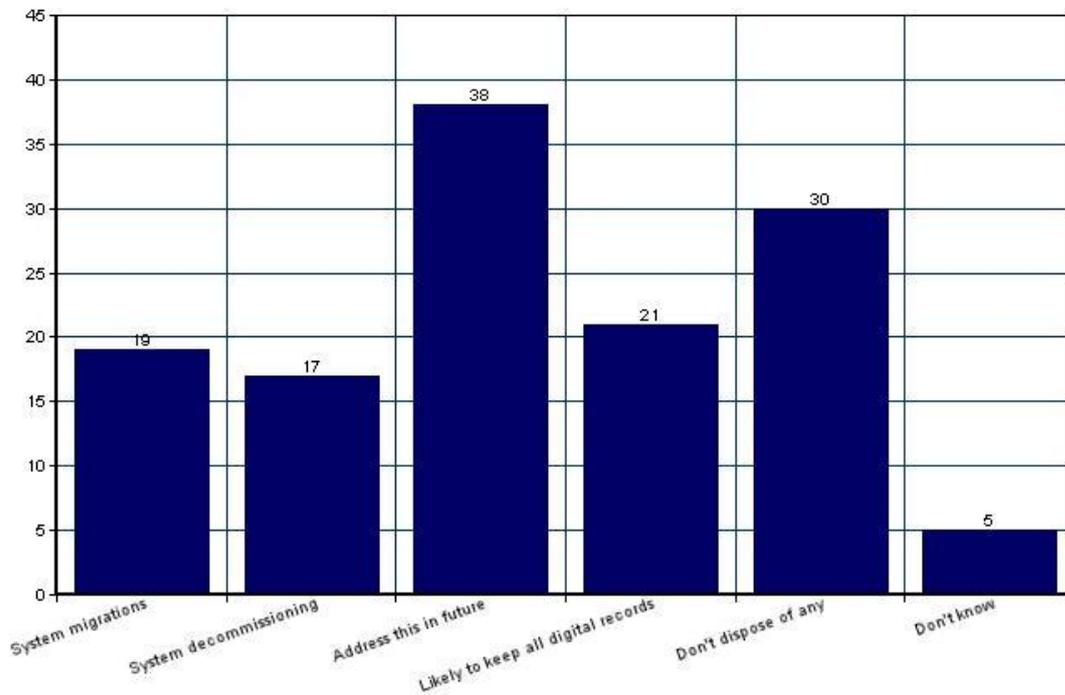
**Question 18: Does your organisation know which digital records in its business systems will need to be kept for 5 or more years?**

Question 18



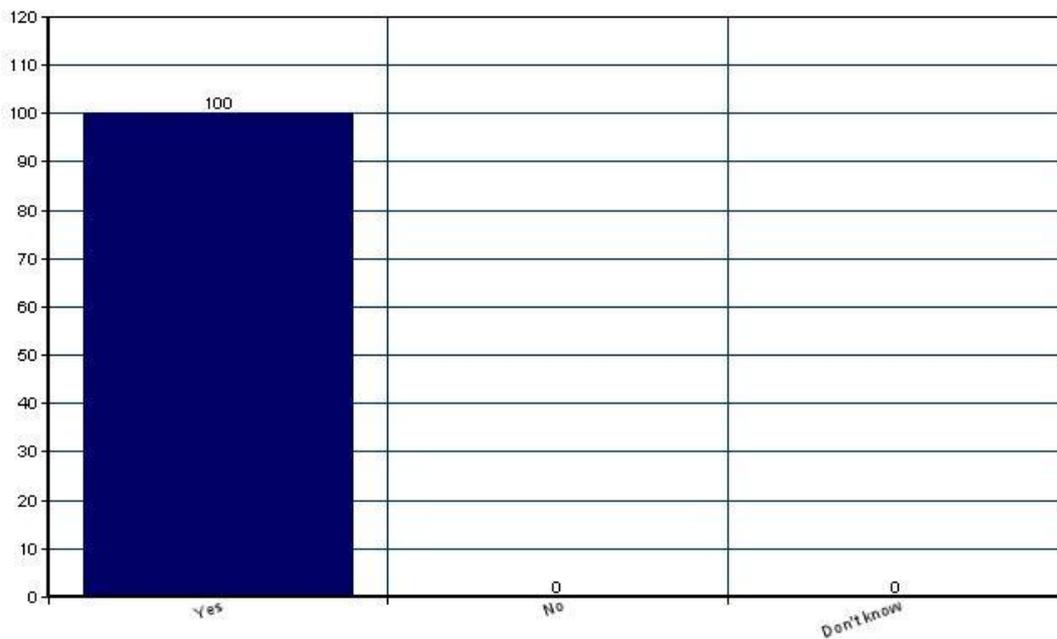
**Question 19: How do you dispose of digital records in business systems?** Respondents could tick as many options as apply

Question 19



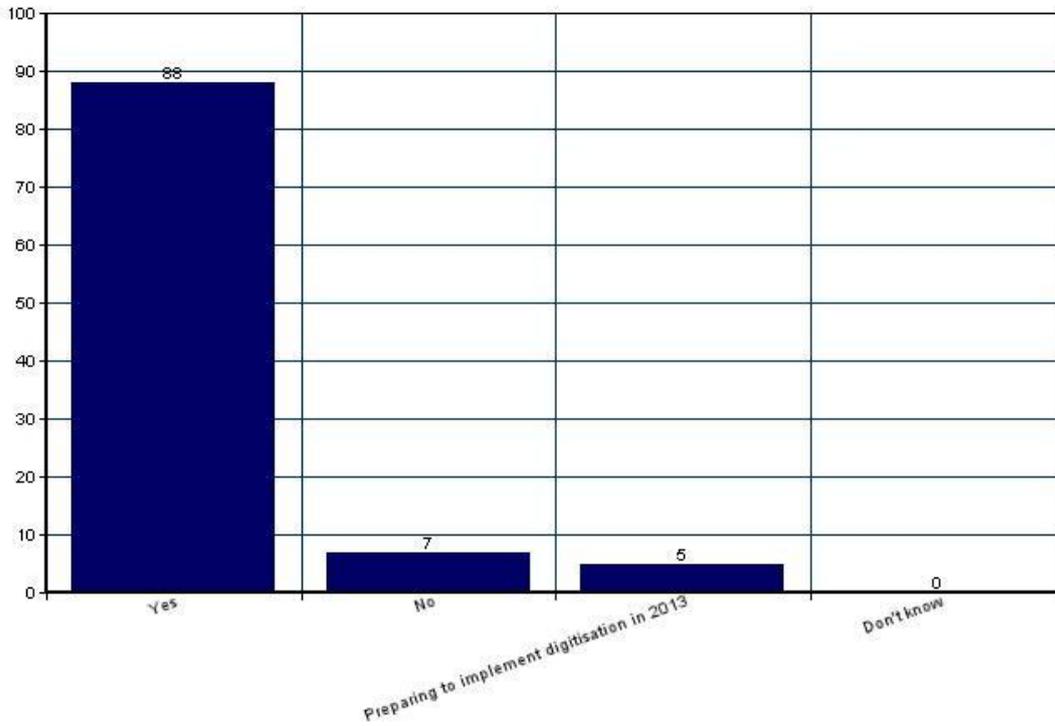
**Question 20: Does your organisation confirm the quality and success of a migration before destroying the source records?** Question answered by 59 public offices; question skipped by 220 public offices

Question 20



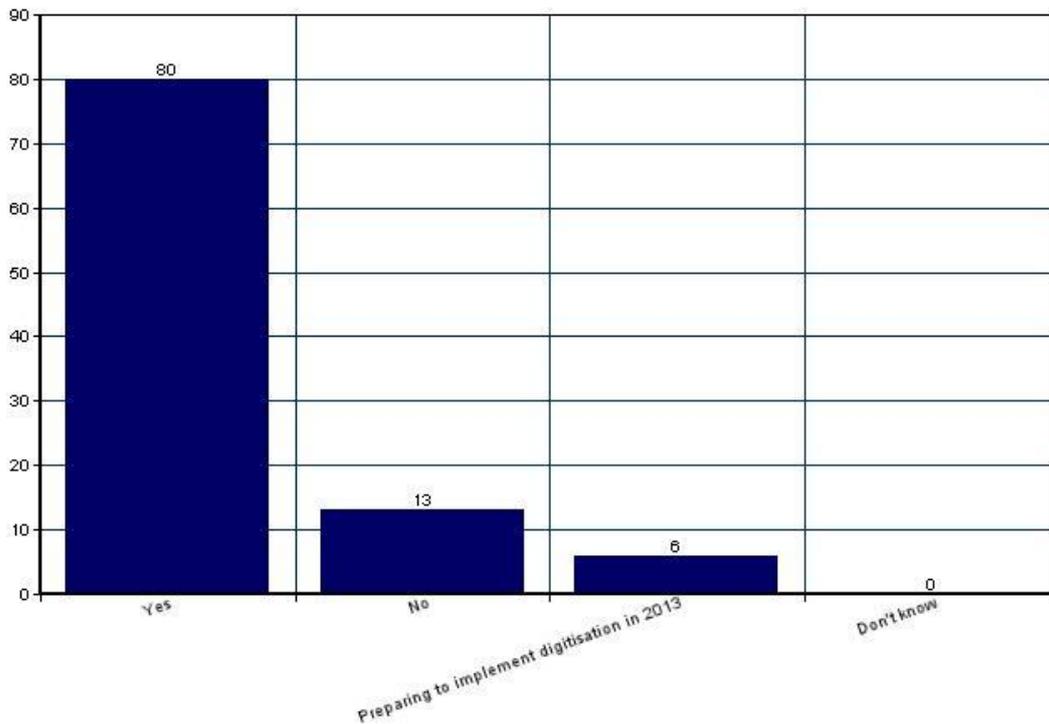
**Question 21: Does your organisation scan/digitise some incoming paper correspondence?**

Question 21



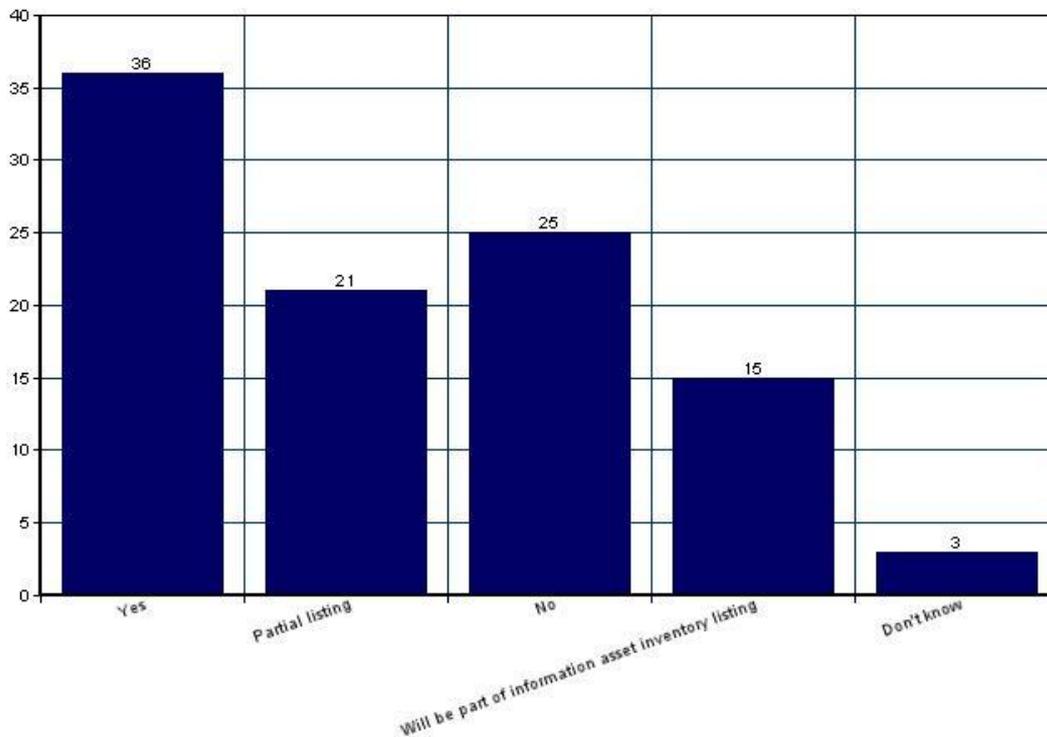
**Question 22: Does your organisation scan/digitise some existing paper files to improve accessibility?**

Question 22



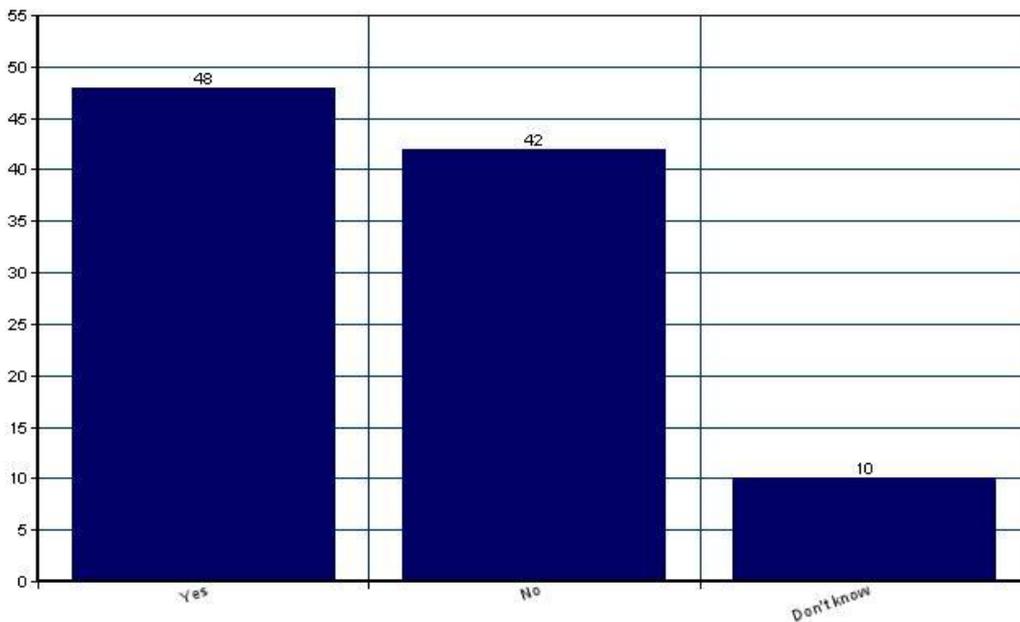
**Question 23: Has your organisation identified all the owners of business systems which hold records of high risk business? In undertaking this work, you may have created an inventory or listing of systems and business owners.**

Question 23



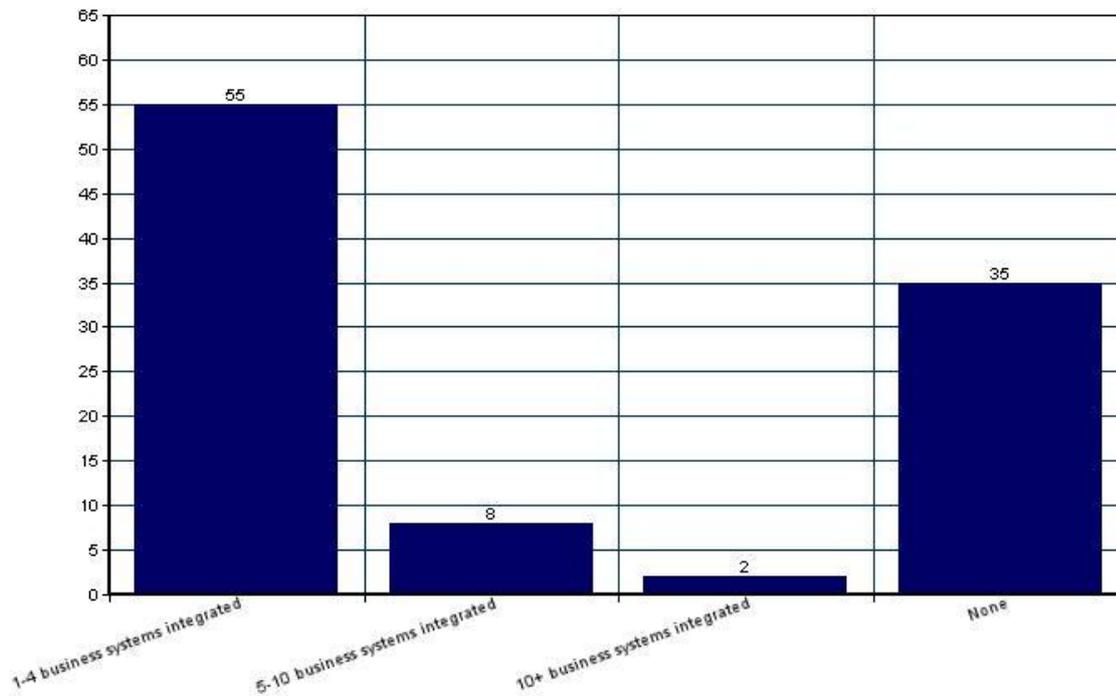
**Question 24: Does your listing identify if the systems are creating and capturing records and have appropriate recordkeeping functionality?** *Question answered by 199 public offices; question skipped by 80 public offices*

Question 24



**Question 25: What number of business systems are integrated with or linked to the organisation's EDRMS or designated recordkeeping system?**

Question 25

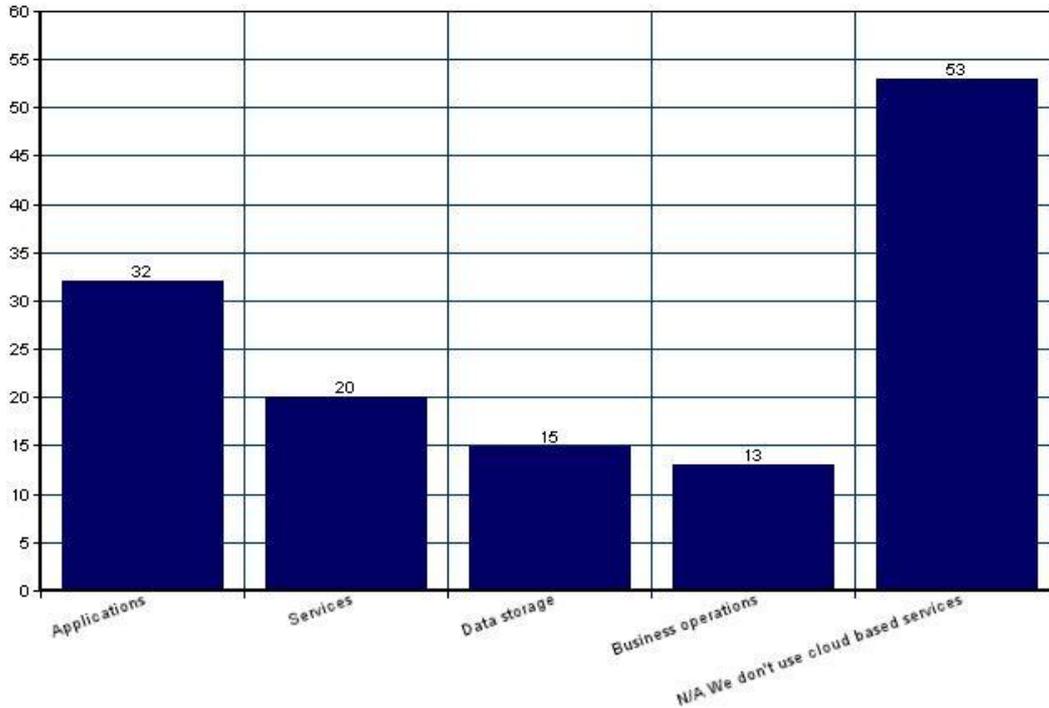


**Question 26: Consider 3 key business systems in your organisation within which recordkeeping processes are performed. Do these business systems (and/or linked EDRMS) capture recordkeeping process metadata about the digital record?** *Text responses to this question*

**Question 27: Identify 3 business systems which support high risk business processes in your organisation that have digital record of long-term value (required for 20 years or more) or digital State archives in them.** *Text responses to this question*

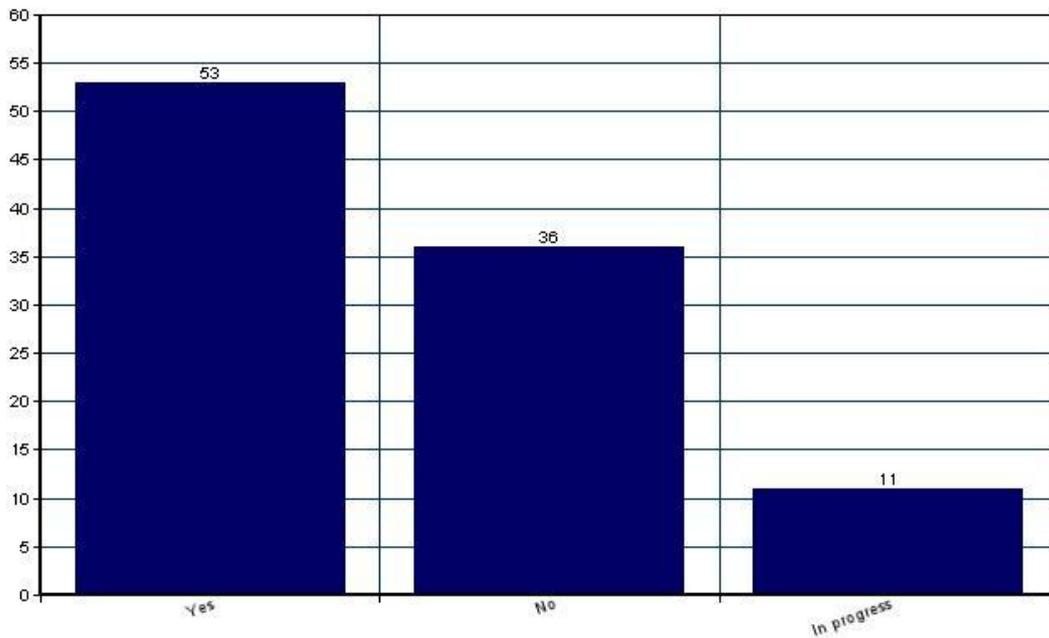
**Question 28: What types of cloud based services does your organisation use?**

Question 28



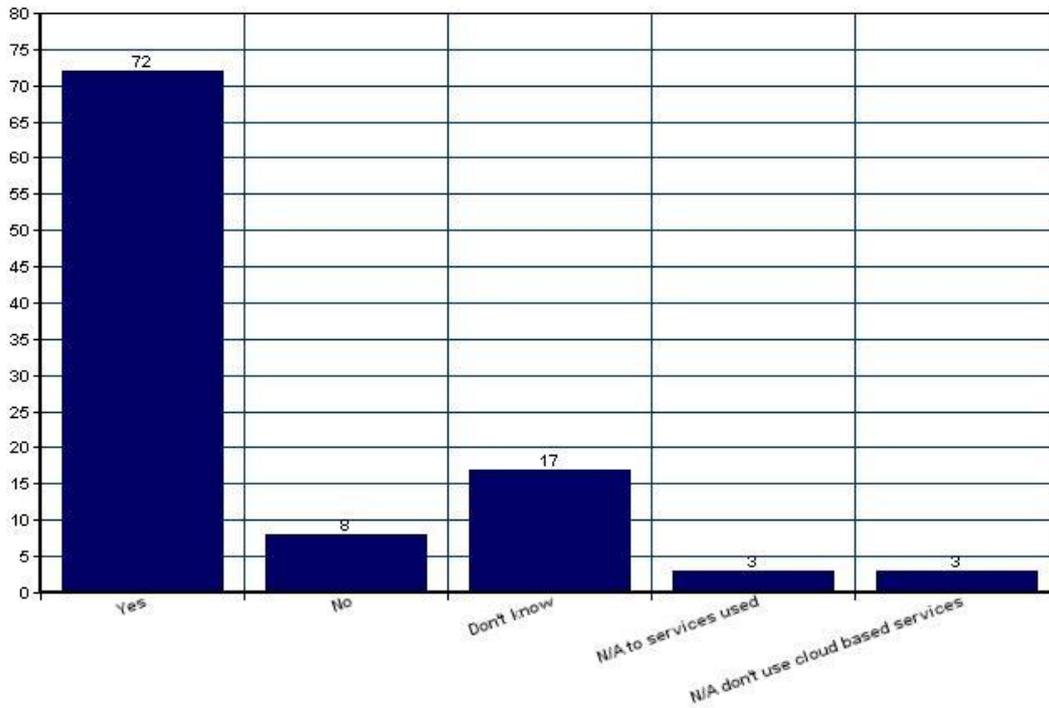
**Question 29: Has your organisation undertaken a risk assessment of business and recordkeeping risks before using cloud-based services?** *Question answered by 128 public offices; question skipped by 151 public offices*

Question 29



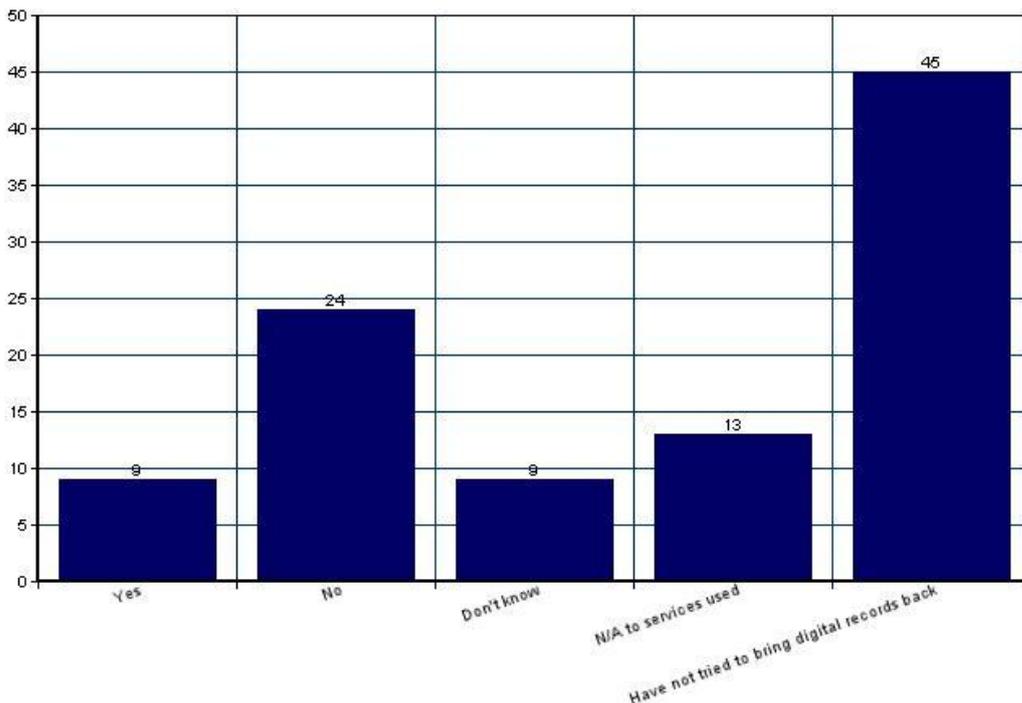
**Question 30: Do cloud-based services used by your organisation have export functionality?** *Question answered by 126 public offices; question skipped by 149 public offices*

Question 30



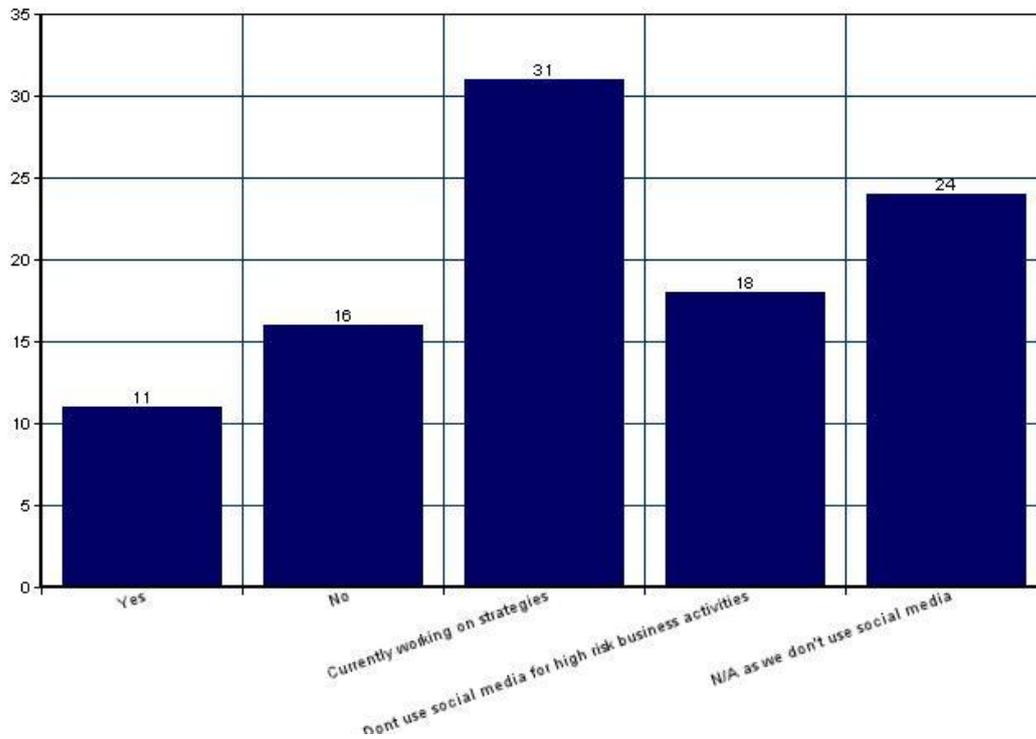
**Question 31: If your organisation has used a cloud-based service, did your organisation have any issues with bringing digital records back into corporate systems or other problems during the contract or at the end of a contract?** *Question answered by 128 public offices; question skipped by 151 public offices*

Question 31



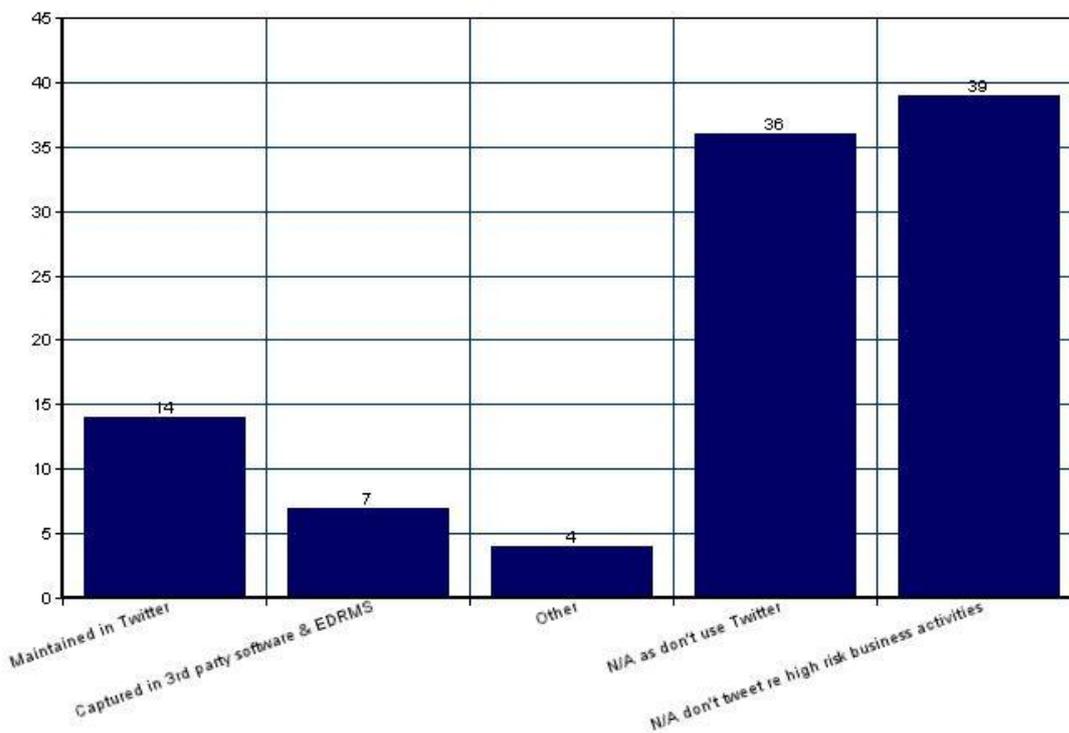
**Question 32: Have you determined strategies for making and keeping digital records that support your organisation's key social media activities?**

Question 32



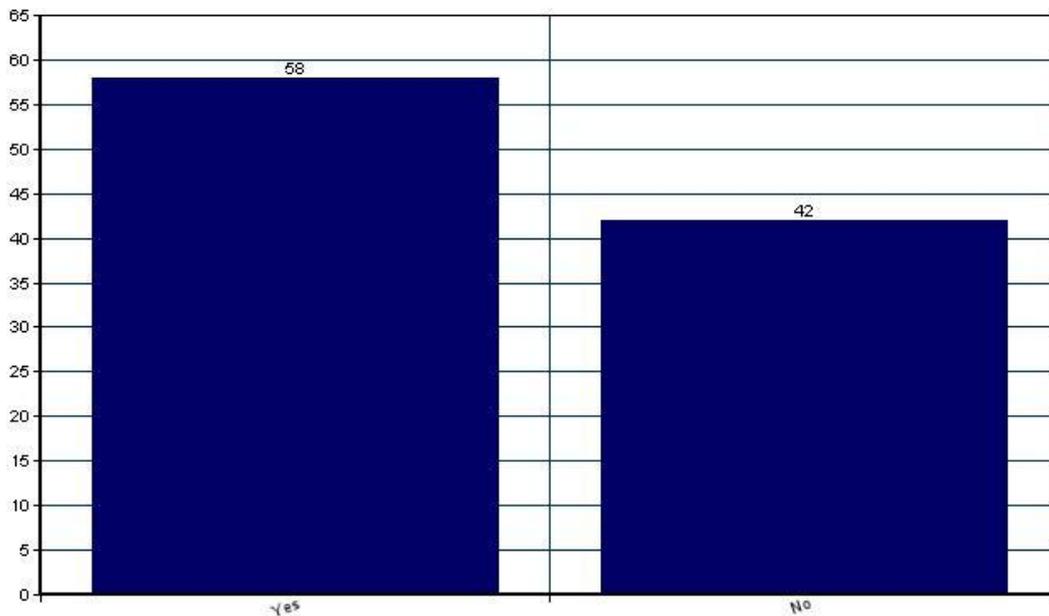
**Question 33: How do you capture tweets of high risk business activities?** *Question answered by 225 public offices; question skipped by 54 public offices*

Question 33



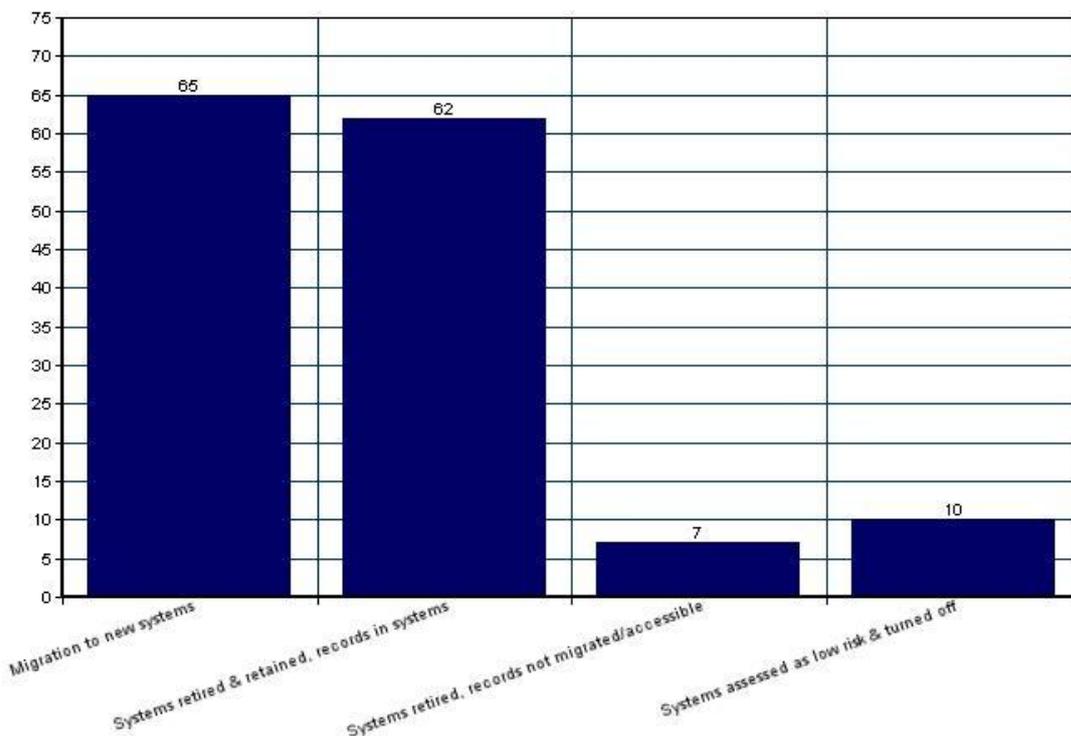
**Question 34: Does your organisation have legacy systems or older business systems which it is managing?**

Question 34



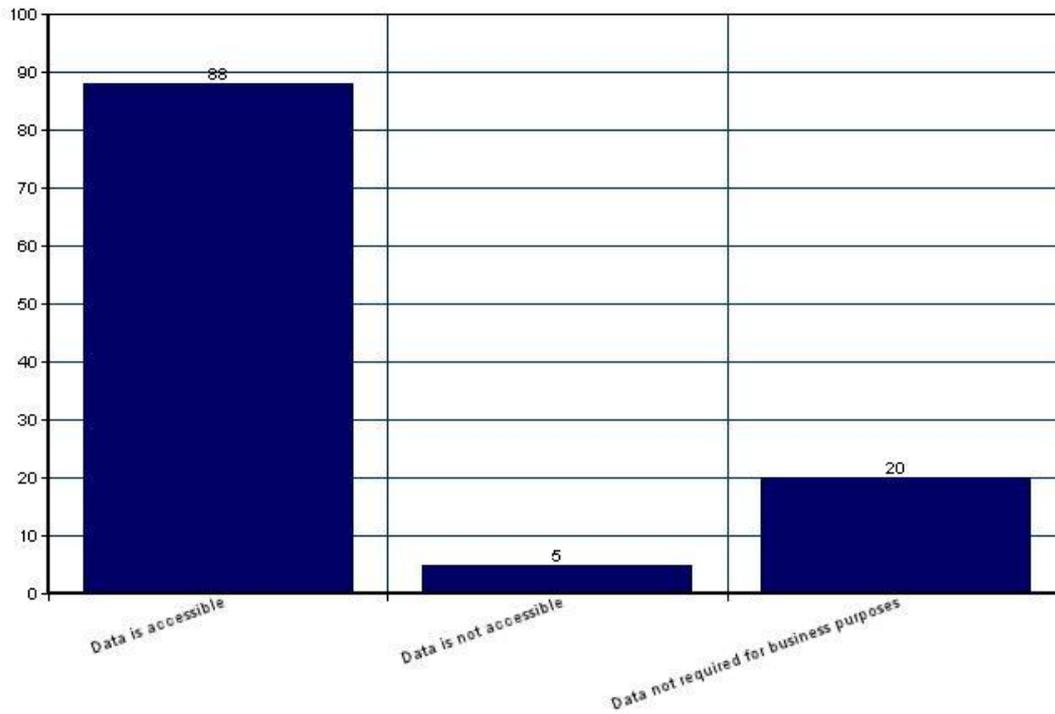
**Question 35: How are legacy systems or older business systems that contain digital records currently managed?** *Question answered by 162 public offices; question skipped by 117 public offices. Respondents could tick as many options as apply*

Question 35



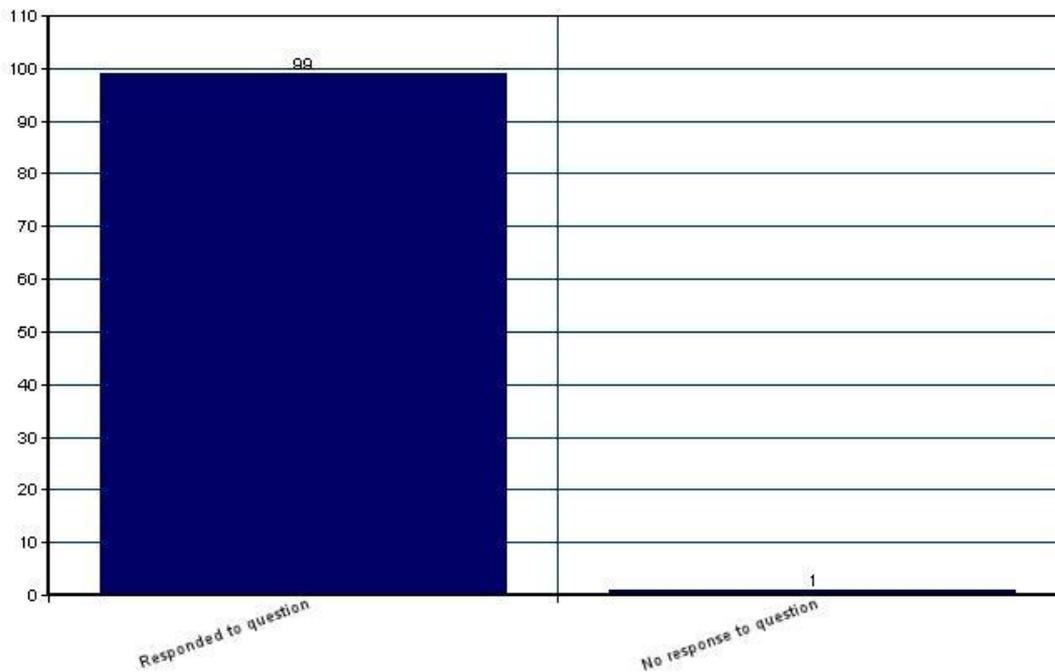
**Question 36: Is there any data held in these legacy or older systems required for business purposes but which is not currently accessible?** *Question answered by 115 public offices; question skipped by 164 public offices. Respondents could tick as many options as apply*

Question 36



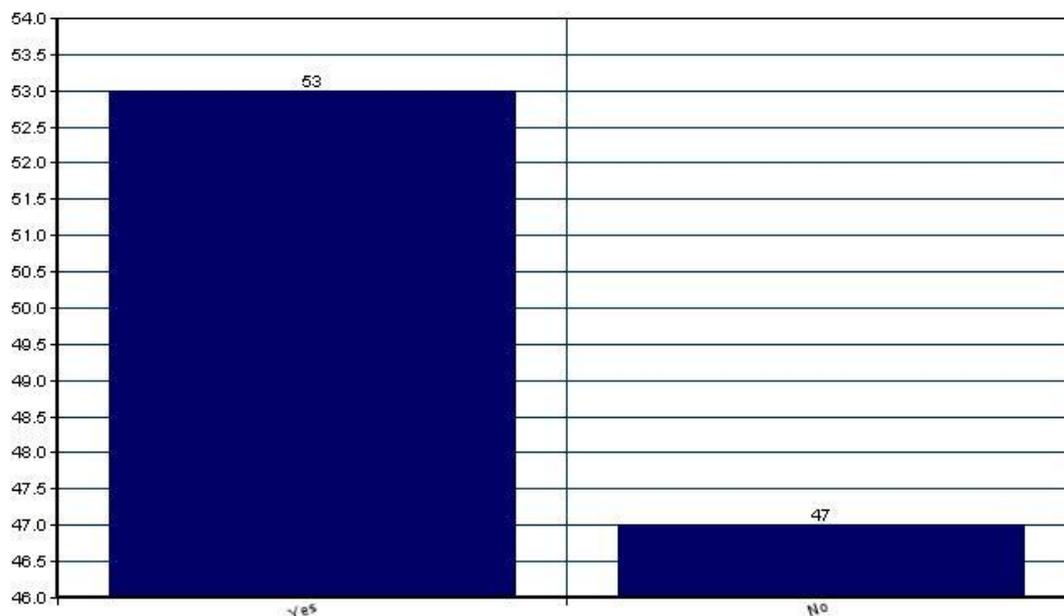
**Question 37: How is your organisation managing the long term retention of digital records in key business systems?** *Text responses to this question*

Question 37



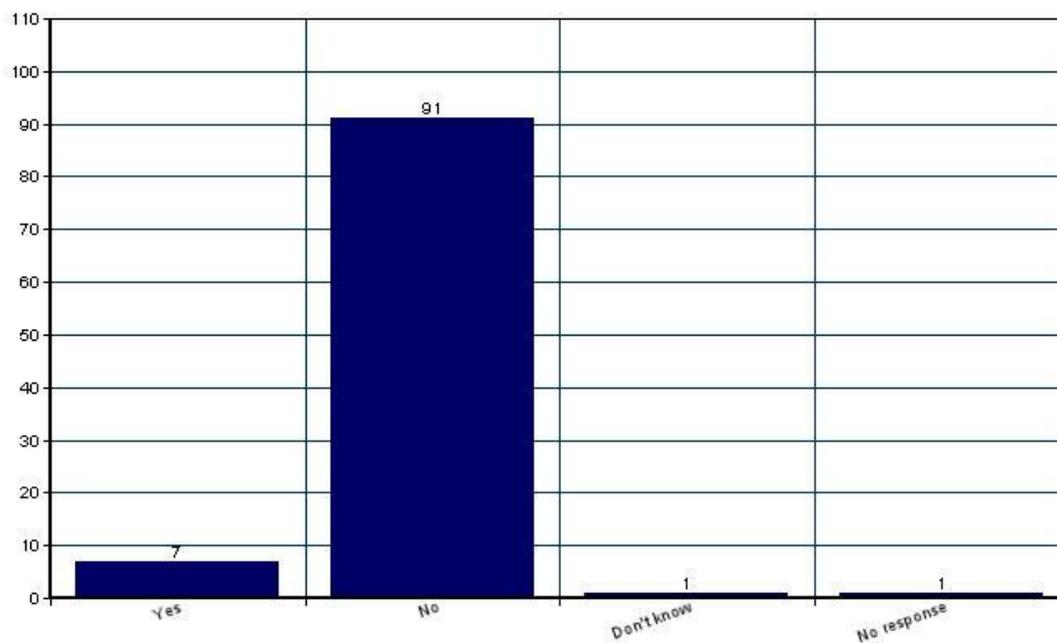
**Question 38: Has your organisation identified digital State archives in its EDRMS or key business systems?**

Question 38



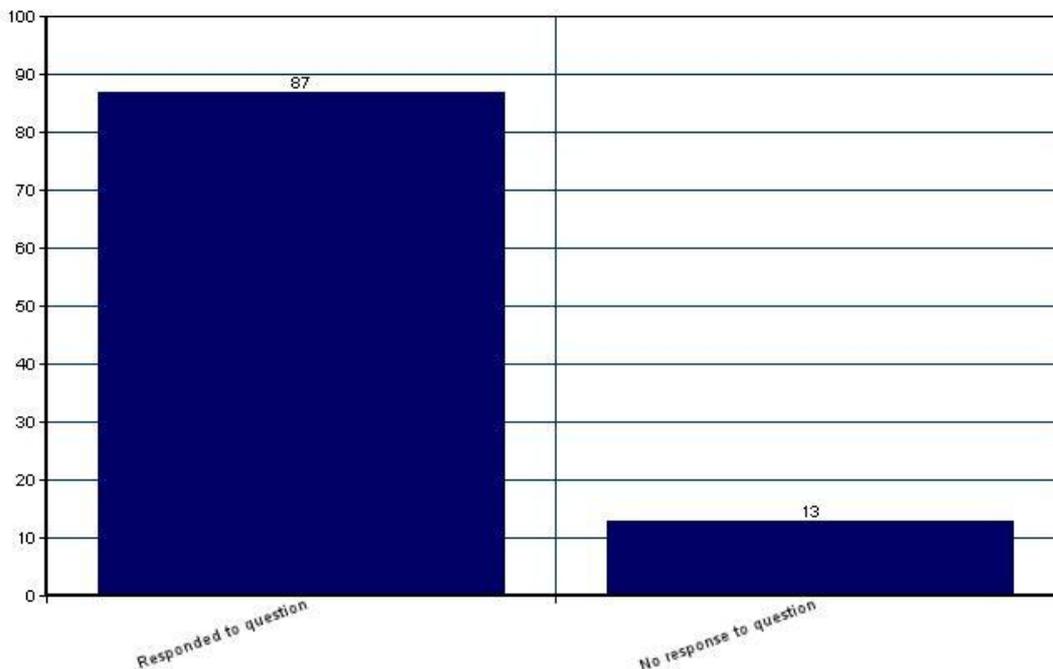
**Question 39: Does your organisation plan to transfer digital State archives to State Records NSW in the next 12 months?**

Question 39



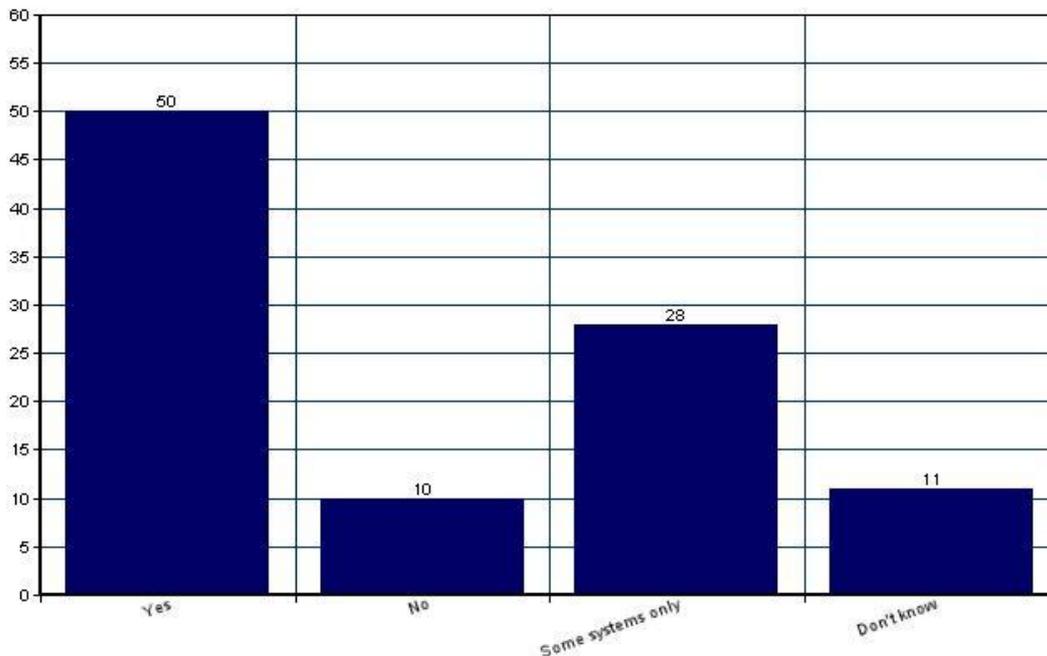
**Question 40: What types of systems hold these State archives?** *Text responses to this question*

Question 40



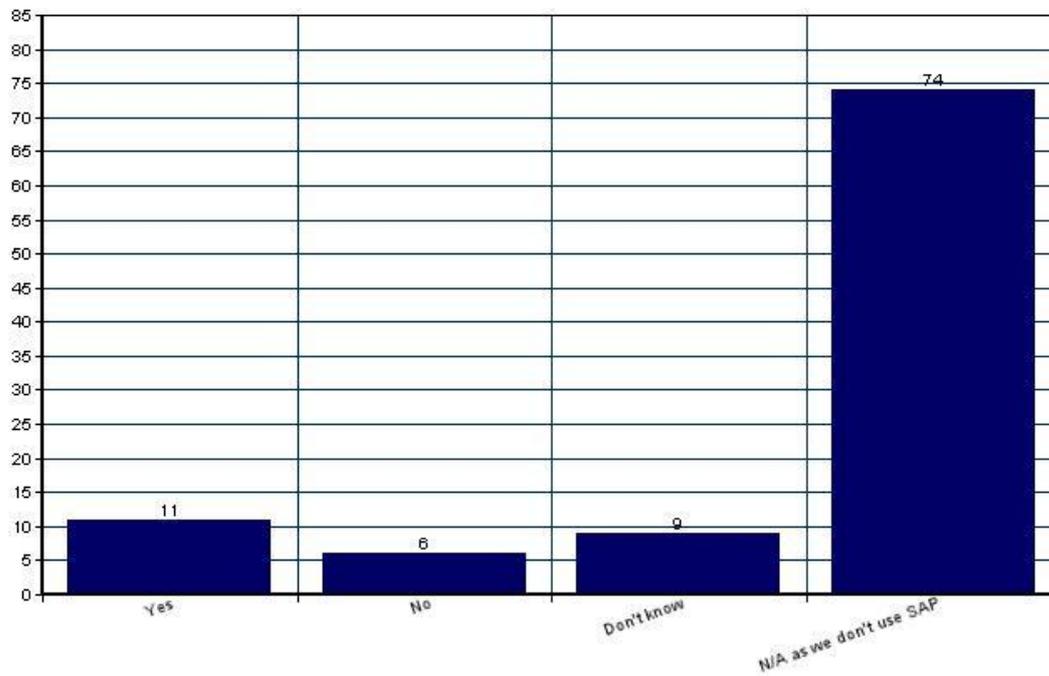
**Question 41: Does your organisation document the system configuration of key business systems?**

Question 41



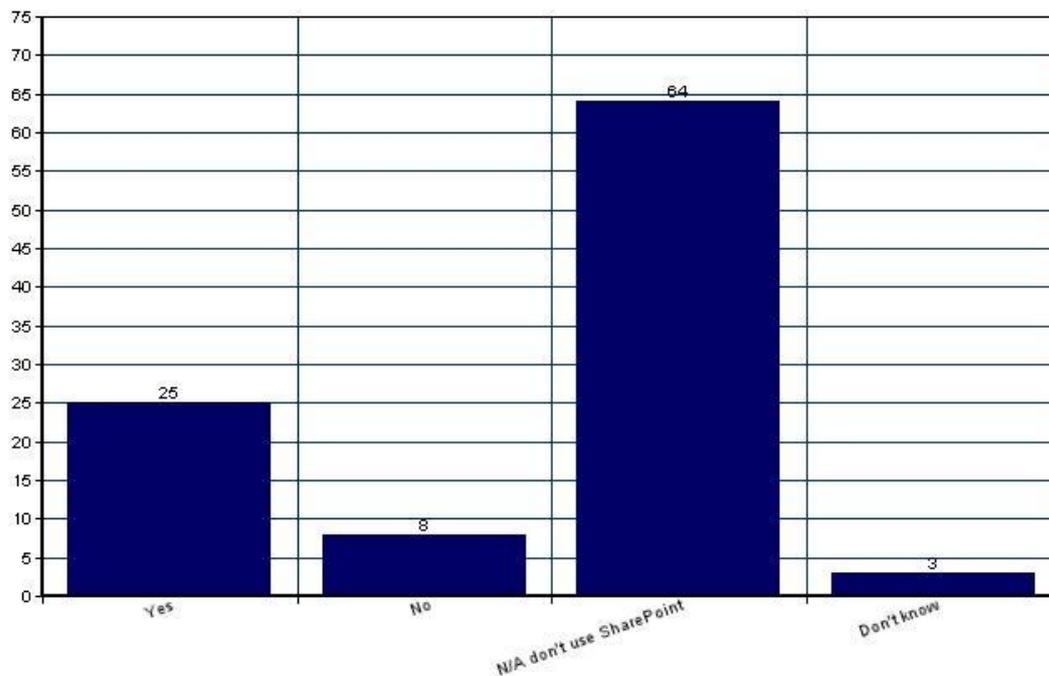
**Question 42: If your organisation uses SAP, has your organisation documented the configuration?**

Question 42



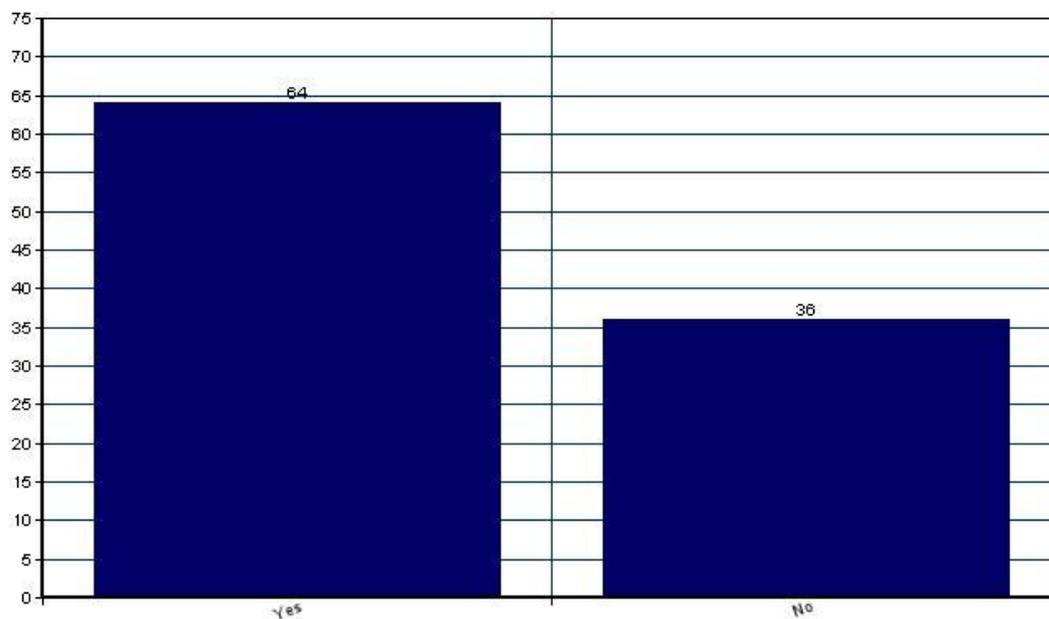
**Question 43: If your organisation uses SharePoint, has your organisation documented the configuration?**

Question 43



**Question 44: Is your organisation creating and managing complex records such as 3D engineering records, CAD files etc.?**

Question 44



## **Appendix B: Results by sector**

Please see separate document