

# GOVERNANCE AND COMPLIANCE IN 2017:

*A Real World View*



## About the Research

As the non-profit association dedicated to nurturing, growing and supporting the information management community, AIIM is proud to provide this research at no charge to our members. In this way, the entire community can leverage the education, thought leadership and direction provided by our work. We would like these research findings to be as widely distributed as possible. Feel free to use individual elements of this research in presentations and publications with the attribution – “© AIIM 2017, [www.aiim.org](http://www.aiim.org)”. Permission is **not** given for other aggregators to host this report on their own website.

Rather than redistribute a copy of this report to your colleagues or clients, we would prefer that you direct them to [www.aiim.org/research](http://www.aiim.org/research) for a download of their own. Our ability to deliver such high-quality research is partially made possible by underwriters, without whom we would have to use a paid subscription model. For that, we hope you will join us in thanking our underwriter, who are:

### opentext™

OpenText  
275 Frank Tompa Drive  
Waterloo, Ontario  
Canada, N2L 0A1  
☎ +1 800 499 6544  
🏠 [www.opentext.com](http://www.opentext.com)

# TABLE OF CONTENTS



ABOUT THE RESEARCH .....	2
PROCESS USED AND SURVEY DEMOGRAPHICS .....	4
<i>ABOUT THE AUTHOR</i> .....	4
<i>ABOUT AIIM</i> .....	4
INTRODUCTION .....	5
<i>KEY FINDINGS</i> .....	6
PERCEPTIONS OF INFORMATION GOVERNANCE .....	8
<i>OVERVIEW</i> .....	8
INFORMATION GOVERNANCE POLICIES .....	14
STORAGE REDUCTION .....	18
AUTO CLASSIFICATION .....	21
TECHNICAL REQUIREMENTS .....	22
CLOUD .....	25
LEGAL HOLD AND EDISCOVERY .....	28
OPINIONS AND SPEND .....	30
CONCLUSIONS & RECOMMENDATIONS .....	32
<i>RECOMMENDATIONS</i> .....	32
APPENDIX 1: SURVEY DEMOGRAPHICS .....	34
<i>ORGANIZATIONAL SIZE</i> .....	34
<i>GEOGRAPHY</i> .....	30
<i>INDUSTRY SECTOR</i> .....	34
<i>DEPARTMENTS</i> .....	35
<i>JOB ROLES</i> .....	35
APPENDIX 2: OPEN-ENDED COMMENTS .....	36
DEVELOPED IN PARTNERSHIP WITH: .....	37
<i>OpenText</i> .....	37

## AIIM Market Intelligence Research

Tap into vendor-neutral industry research through AIIM. Learn about industry trends, benchmark your organization's progress, and understand important next steps to move your organization forward.

As the non-profit association dedicated to nurturing, growing and supporting the information management community, AIIM is proud to provide this research at no charge to our members. In this way, the entire community can leverage the education, thought leadership and direction provided by our work. We would like these research findings to be as widely distributed as possible. Permission is not given for other aggregators to host this report on their own website.

Rather than redistribute a copy of this report to your colleagues or clients, we would prefer that you direct them to [www.aiim.org/research](http://www.aiim.org/research) for a download of their own.

Our ability to deliver such high-quality research is partially made possible by underwriters, without whom we would have to use a paid subscription model. For that, we hope you will join us in thanking our underwriters.

# PROCESS USED AND SURVEY DEMOGRAPHICS

## Process Used and Survey Demographics

While we appreciate the support of these sponsors, we also greatly value our objectivity and independence as a non-profit industry association. The results of the survey and the market commentary made in this report are independent of any bias from the vendor community.

The survey was taken using a web-based tool collecting responses from 218 individual members of the AIIM community during the month of June of 2017. Invitations to take the survey were sent via email to a selection of the AIIM community members and through various social media outlets. Survey demographics can be found in Appendix 1.

## About AIIM



AIIM has been an advocate and supporter of information professionals for over 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators and consultants.



## About the author

**Bob Larrivee**

*Vice President and Chief Analyst  
of Market Intelligence, AIIM*

Bob Larrivee is Vice President and Chief Analyst of AIIM Market Intelligence. Internationally recognized as a subject matter expert, and thought leader with over thirty years of experience in the fields of information and process management, Bob is an avid techie with a focus on process improvement, and applying advanced technologies to solve business problems, improve business processes, and automate business operations.

© 2017

AIIM  
1100 Wayne Avenue, Suite 1100  
Silver Spring, MD 20910  
+1 301 587-8202  
[www.aiim.org](http://www.aiim.org)



## Introduction

The emphasis on data security, and the risk of data loss have all become sharpened focal points for businesses. Regulations are getting stricter, demanding greater need to adhere to regulatory, legal, and industry operating guidelines to secure and protect corporate and customer information. This requires businesses to implement more focused and stricter information governance (IG) policies, practices, and enforcement efforts.

Yet, in this study, only three percent of our respondents cite their IG policies as being outstanding with seventeen percent of respondents rating the maturity level of their companies' IG policies as extremely poor. When asked about data loss or challenges in finding information in the past twelve months, ten percent of respondents report data loss due to staff negligence or bad practices while eight percent say they could not find the records they required for litigation.

Given these challenges, one might think the importance placed on IG would be fairly high, yet, when we asked, only twenty-four percent of respondents reported that IG and data security is high on the agenda for senior management, with twenty-seven percent reporting they have plans in place to investigate and audit their information ecosystems. We also found that thirty-eight percent cite their biggest challenges in IG are getting anyone to be interested (38%), and getting senior management endorsement (35%).

So it is no surprise to learn that with such a low number placing high focus on IG, that thirty-four percent of respondents say their companies do not offer them IG training at all, and fifteen percent say IG training is provided only at induction to the workforce. Could this be the reason there is data loss due to staff negligence and bad practices?

Organizations in all industries must come to realize the importance of ensuring that their data assets are managed and shared in a sensible and secure manner. This study explores how organizations are addressing their governance and compliance challenges by looking at:

- The business case for a governance and compliance framework for security, privacy, and protection
- Automating governance and compliance components (Metadata, Security, etc.)
- Identifying the locations of greatest risk for breaches – internally and across the firewall
- Collection, retention, management, and defensible destruction of information
- A look ahead at the next five years to understand where businesses are focusing their efforts and funding

### Terms used:

<b>IM:</b> Information Management	<b>IG:</b> Information Governance
<b>ECM:</b> Enterprise Content Management	<b>DM:</b> Document Management
<b>ERM:</b> Electronic Records Management	<b>CA:</b> Content Analytics
<b>DAM:</b> Digital Asset Management	<b>DT:</b> Digital Transformation
<b>BI:</b> Business Intelligence	<b>BPI:</b> Business Process Improvement
<b>BPM:</b> Business Process Management	<b>IT:</b> Information Technology
<b>EFSS:</b> Enterprise file-sync-and-share	

### Personas used include:

- **Trailblazer** – Exceptional capabilities; ahead of the pack in respective market space or among peer groups
- **Citizen** – Citizen – Average capabilities; on an equal level compared to competition and peer groups
- **Outlander** – Below average capabilities, behind the times, typically waiting until the last minute to implement change

## Key Findings

### In General

- Seventeen percent of respondents report the maturity level of their companies' information governance policies as extremely poor. Three percent say their IG policies are outstanding.
- In the past 12 months, ten percent of respondents report data loss due to staff negligence or bad practices. Eight percent say they could not find records required for litigation.
- Twenty-four percent of respondents indicate that IG and data security is high on the agenda for their senior management. Twenty-seven percent have plans in place to investigate and audit their information ecosystems.
- Thirty-four percent of respondents say their companies do not offer them IG training at all. Fifteen percent say IG training is provided only at induction to the workforce.
- For those who do have training, fifty-four percent say it is delivered online. Twenty-six percent get their IG training from their employee manuals.
- Regarding what their training consists of, ninety-one percent report their IG training includes policies and practices with eighty percent indicating compliance requirements as well. Fifty-six percent report they also receive technology training.

### Information Governance Policies

- When it comes to IG helping to prevent data loss, twenty-six percent of respondents see themselves as Trailblazers. Forty percent indicate they are Outlanders when it comes to defensible deletion.
- Nearly half of our respondents report having an IG committee of some sort. Twenty-four percent report having little in the way of any policies at all.
- Information retention is part of the IG policy portfolio for sixty-seven percent of respondents, and for sixty-six percent, access and confidentiality also top the list. For sixty-one percent, data protection and personally identifiable information (PII) are high on the list.

### Storage Reduction

- From a strategic perspective, twenty-eight percent of respondents say they are consolidating their storage into larger data centers. Twenty-six percent are moving to a cloud model for content and records and the same number are also implementing EFSS, ECM, or ERM systems to replace their file-shares.
- When asked how their strategies are working, twenty-nine percent of respondents say that volumes and costs are increasing. Nineteen percent indicate they are holding their own.
- With indications that volumes and costs are increasing, the sense is deletion should be the focus. Yet twenty-seven percent of respondents say most things are never deleted. Fourteen percent say they have no defined retention periods.

### Legal Hold and eDiscovery

- When looking at the legal hold and ediscovery, thirty-six percent of respondents indicate only some of the legal department understand the policies and mechanisms while thirty-two percent say the entire legal department understands. For fifty-six percent of respondents it is believed the records managers fully understand.





# PERCEPTIONS

of

## Information Governance



# PERCEPTIONS OF INFORMATION GOVERNANCE

## Overview

There are many real world changes and challenges driving the need for better and tighter information governance, though some businesses may not readily see the need and are willing to take a risk, the need is clearly there. Reports of data loss and security breaches are at an all time high yet not all are the result of external hacking and in fact the result of internal staff, whether intentionally or unintentionally, exposing data beyond corporate walls to those who do not have the right to access it.

From a compliance perspective, there are internationally recognized regulations, and there are many regional, local, and industry regulations that must be addressed as part of transacting business within those regions and industries. For example there are the laws of the European Union (EU) like the General Data Protection Regulation (GDPR), Switzerland (like Data Protection, etc.) and of Public Administration, Norwegian petroleum Law, Canadian Radio-television and Telecommunications Commission Act, Florida State Records Laws & Regulations, Ontario Personal Health Information Protection Act, South Africa – Protection of Personal Information Act, Dutch regulatory statutes for financials and pensions, and New Zealand government regulations, in particular the Privacy Act and Electronic Transactions Act.

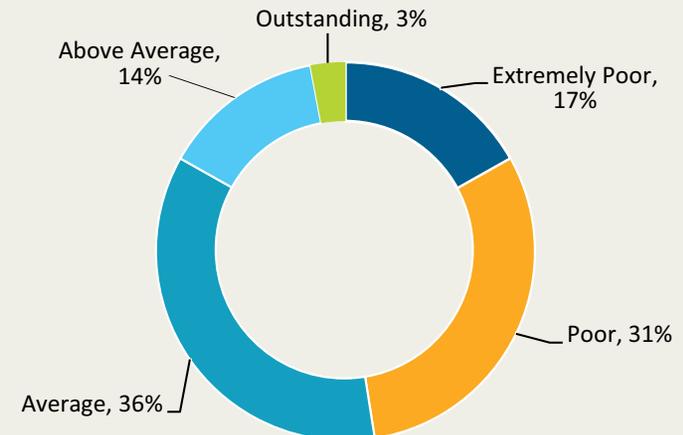
As you read through this report, take time to reflect on how this information applies to you in both your personal and business life. Try to position yourself in terms of where you and your business fit within these statistics and among your peers.

## Perceptions of Information Governance

Information governance must be viewed as an on-going commitment of continuous change and improvement, maturing to new levels in meeting the stringent regulatory requirements placed on today's businesses. We asked our respondents to rate the maturity of their company's IG policies and provide us with their assessment on a scale of one to five with five being outstanding and one being extremely poor. Only three percent see themselves as being outstanding in this area while seventeen percent see their companies as having extremely poor IG policies and an additional thirty-one percent as poor. (Figure 1)

Given the lack of support indicated in some of the feedback we've received, and will see further on in this report, it is of little surprise that we are seeing such low ratings and so much opportunity to improve.

Figure 1: On a scale of 1 to 5 (1 being poor and 5 being outstanding) how would you rate the maturity of your company's information governance (IG) policies?

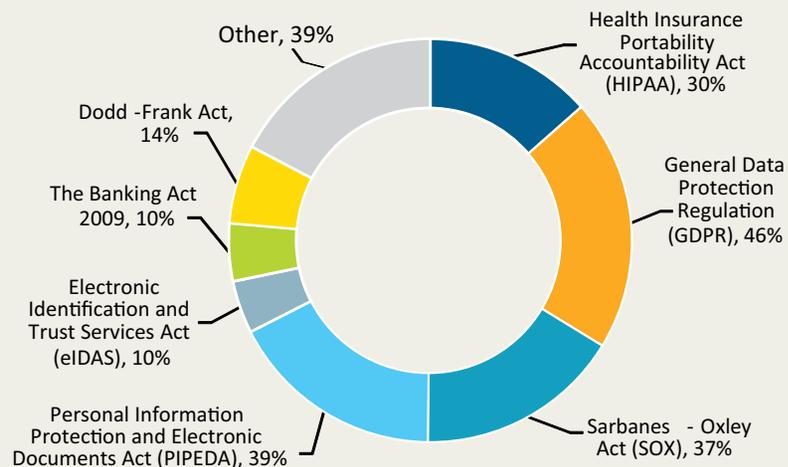


As presented in the introduction, there are many regulations driving the need for IG and certainly regulatory compliance that IG supports. We asked our respondents to identify all of the readily identifiable international regulations they must comply with and list those we did not identify, resulting in the list we presented earlier. Forty-six percent of our respondents say they operate under the European Union (EU) General Data Protection Regulation (GDPR) passed in May 2016 and scheduled to be enforced in May 2018. Interestingly, in the AIIM study titled "Understanding GDPR Readiness in 2017", we found the majority of businesses are not prepared to comply with this regulation.

The Canadian regulation Personal Information Protection and Electronic Documents Act (PIPEDA) is the top of the list for thirty-nine percent of our respondents while thirty-seven percent operate under the guidelines of the Sarbanes-Oxley Act of the United States. (Figure 2) One thing to note here is that while these may be cited as national or regional regulations, they are in fact, regulations that impact any and every business that operates within their borders and that means regardless of where a business is headquartered. If they operate in Canada, they must abide by Canadian regulations, the same as they would in the United States, the United Kingdom, or the European Union.

# PERCEPTIONS OF INFORMATION GOVERNANCE

Figure 2: Which Regulatory Statutes does your organization operate under?

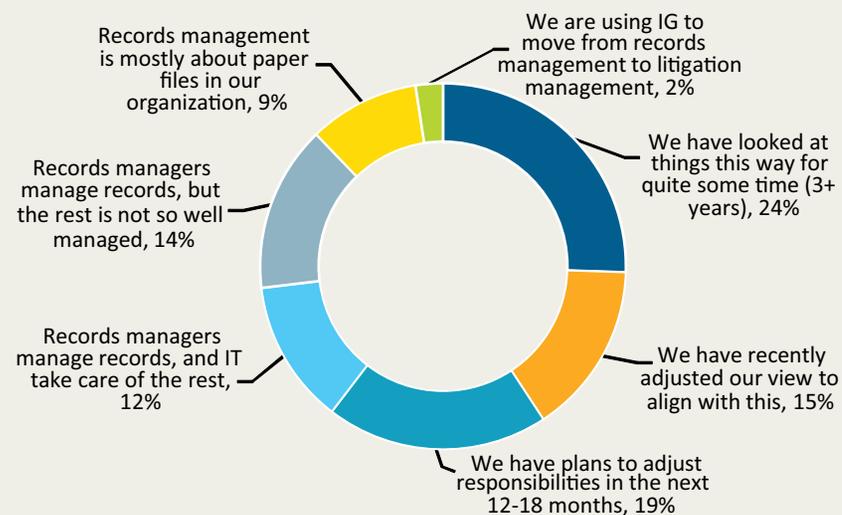


Perceptions of IG have long been centered on records and not inclusive of information as a whole. Electronically stored information (ESI) regardless of what it is or where it is must be included in the IG policies, practices and enforcement efforts to minimize and eliminate data loss and exposure.

There is some movement to take a more holistic approach to IG, according to some of our respondents, "Records management knows what should be done for ESI, but essentially IT controls electronic records. Each time RM convinces management that IG needs to be implemented with an understanding of content, not just technology, a new management team comes on board" or "Records Management was moved to IT Security and oversees physical and digital documents as well as building the taxonomy governance for all content repositories." Yet there is still much work ahead.

When we asked our respondents to share how much the perception of information governance has progressed from management of declared records, to management of ALL ESI for access, privacy, security, compliance and ediscovery nearly one quarter say they have been looking at things this way for more than three years now while nineteen percent have plans in place to move in this direction within the next twelve to eighteen months. (Figure 3)

Figure 3: To what extent would you say the perception of information governance in your organization has progressed from management of declared records, to management of ALL electronically stored information for access, privacy, security, compliance and ediscovery?

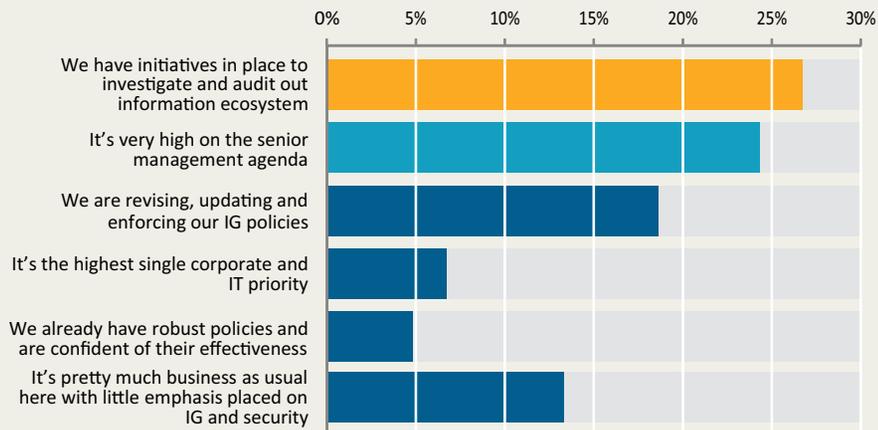


As we noted in the introduction there is a high level of importance placed on IG and data security with senior management, but we are also seeing some effort to update and enforce policies as reported by nineteen percent of our respondents. Still there are those – thirteen percent – who say their businesses have placed little to no emphasis on IG and continue to conduct business as usual. (Figure 4)

Of course IG and security are not often seen together and are regularly addressed separately. This is validated by some feedback gathered that included statements like, "information security is a priority, but information governance as a unifying discipline is not well understood," "We have great data security but poor IG," and "We have great data security but poor IG."

# PERCEPTIONS OF INFORMATION GOVERNANCE

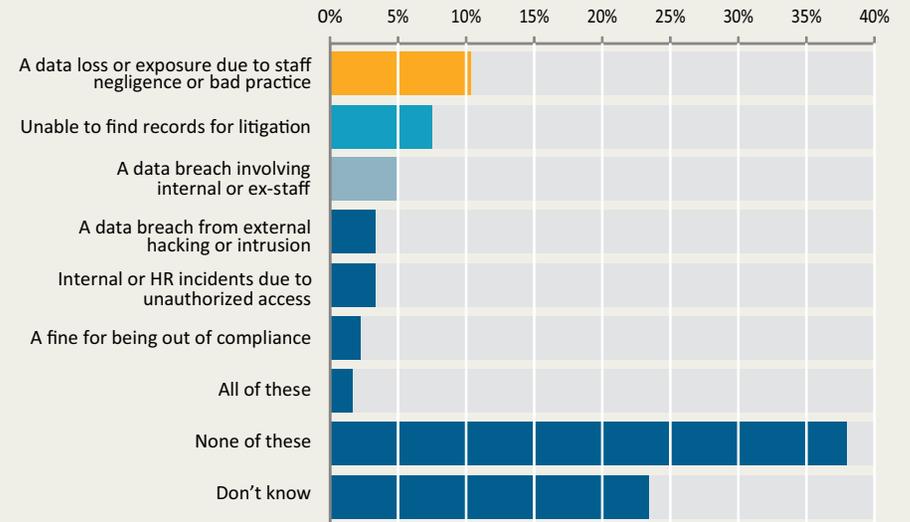
Figure 4: How would you describe the level of maturity and importance placed on information governance and data security in your organization, in the light of recent leaks, hacks, and email issues?



**“Data security should be part of the overarching IG program and policy framework, not isolated and managed as a separate entity.”**

When we asked about knowledge of data loss or breaches, nearly a quarter said they didn't know of any while thirty-eight percent said they hadn't had any of the ones we listed. Ten percent did report data loss due to staff negligence or bad practices. (Figure 5) In fact along with this, we heard not only is data loss from staff negligence common, so are compliance fines, and ediscovery costs can run over \$1M due to the inability to quickly and accurately find information.

Figure 5: Has your organization suffered any of the following in the last 12 months?

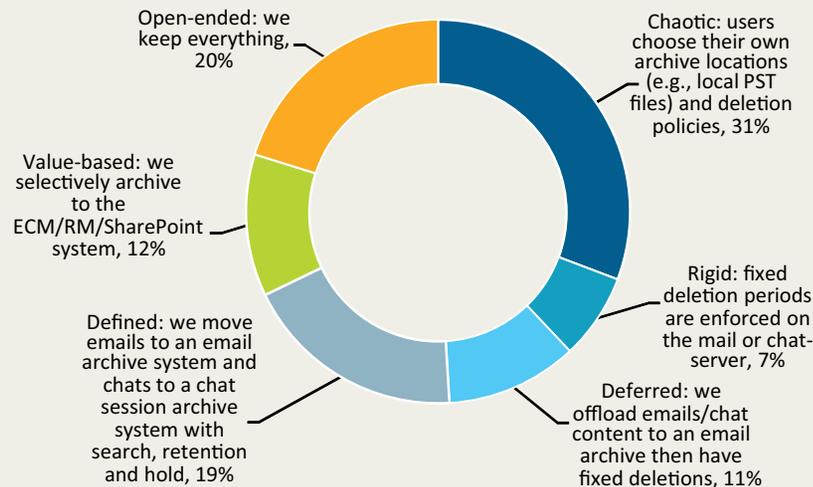


Sharpening the focus even more, we aim the IG lens at emails and chat sessions, and asked how businesses are governing their use. Chaotic was the response we received from thirty-one percent of respondents who said their users choose their own archive locations and for twenty percent it is open-ended with everything being kept. Only twelve percent told us they have a value-based approach where they selectively archive emails and chat sessions to their ECM, RM, or SharePoint systems. (Figure 6)

This has been and remains an area of contention for businesses. They know emails, chats, and even more so today – tweets – are considered “official records,” yet they have no idea how to approach managing these content sources. Some prefer to ignore them, some choose to keep it all and hope they never have to sort through it, and the small percentage look for the value and extract that portion and discard the rest. It is the latter that are the Trailblazers and know the value of their information.

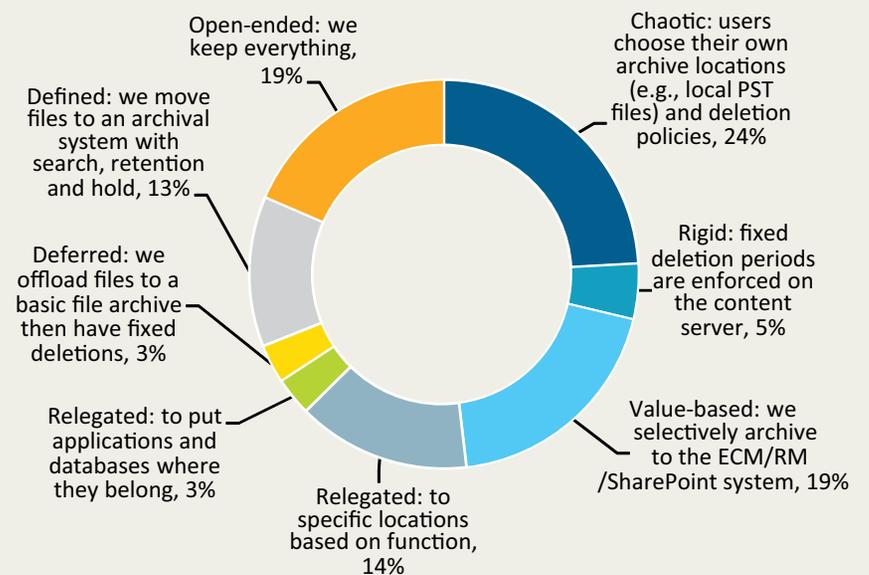
# PERCEPTIONS OF INFORMATION GOVERNANCE

Figure 6: How would you describe the governance of emails or chat sessions in your organization?



Stepping back to look at files, another area of contention for many businesses, we asked the same question about governance in relation and found similarly that nearly a quarter report a chaotic state of users choosing their own archive locations and nineteen percent using a value based approach. Here we also found that fourteen percent are relegated to specific locations based on role. (Figure 7) So while there are some similarities with emails and chats, which is of little surprise, there is some difference in how files are managed based on role which begs the question if they do this for files, at minimum, could it not also be done for the rest?

Figure 7: How would you describe the governance of files in your organization?

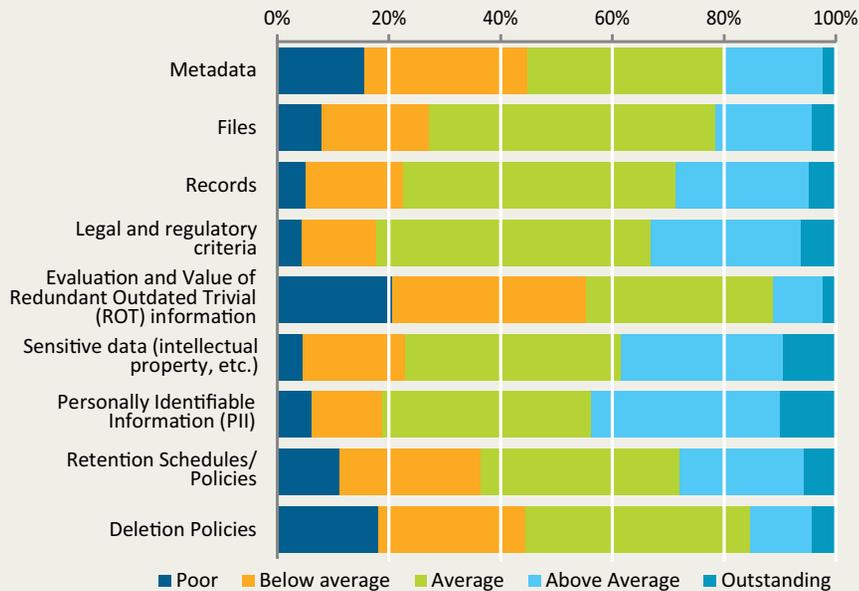


Migration is also an area that needs to be considered as part of an IG framework and how each element of information will be handled as part of the migration process. For example when it comes to Personally Identifiable Information (PII) ten percent of our respondents see themselves as being outstanding and thirty-four percent above average in relation to the migration governance of this information. When referring to metadata however, sixteen percent see themselves as poor and twenty-nine percent as below average in migration governance. (Figure 8) So it is not just the content or records but also retention schedules and policies, deletion policies, legal and regulatory criteria, all of this and more that must be part of the migration governance plan. Have you looked at your migration governance plan lately?



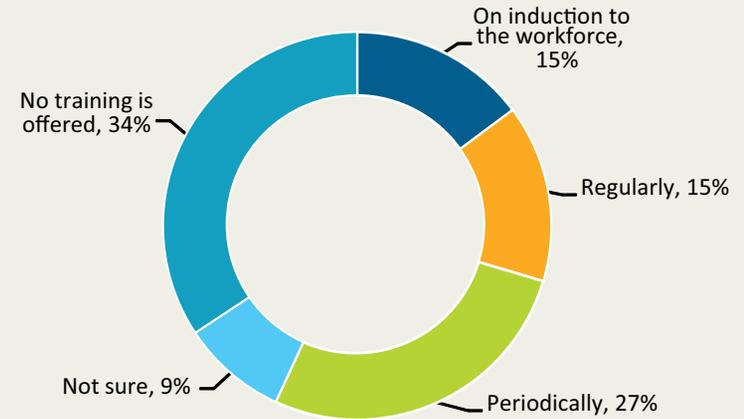
# PERCEPTIONS OF INFORMATION GOVERNANCE

Figure 8: On a scale of 1 to 5 (1 being poor and 5 being outstanding) how effectively do you manage governance over your data migration projects?



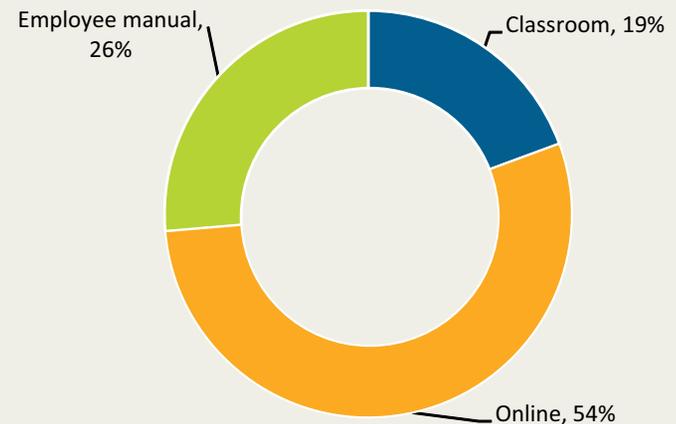
Having a plan on what to manage is actually part of the policy element; there must also be a training element to teach the employees and anyone likely to interact with your information, about your policies, procedures and technologies. This would be internal and external parties. So does your business train employees in IG? Not at all was the answer we received from thirty-four percent of our respondents and only at the time of induction to the workforce was the response from fifteen percent. (Figure 9) So if any wonder why there is a risk of data loss by employee negligence or bad practices?

Figure 9: Does your organization conduct information governance training for the employees?



For those that do get training fifty-four percent say it is delivered online, twenty-six percent receive it in their employee manuals and nineteen percent in classroom settings. (Figure 10)

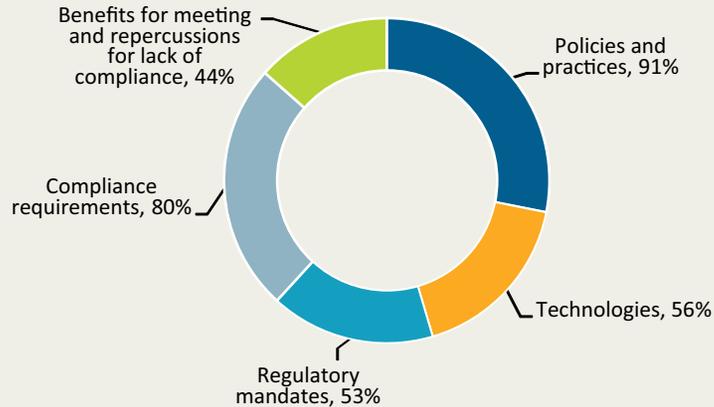
Figure 10: How is your IG training managed/delivered?





What they get in their training is information about the policies and procedures (91%), compliance requirements (80%), and for fifty-six percent, technology training. (Figure 11)

Figure 11: What does your IG training consist of?



## Putting The Pieces Together

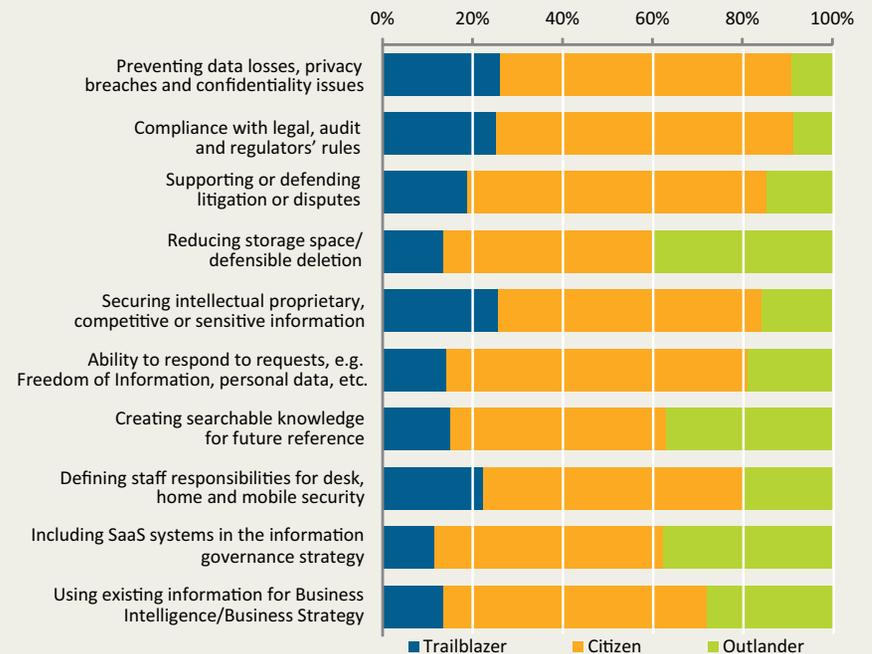
IG is one of those areas of business that is like the buzz of a mosquito. It's there, you hear it, and you know you have to deal with it before it bites you but you just can't seem to get to it. And then it is too late. Many businesses take swats at IG but do not have a solid framework in place to do it right or continue to improve upon what they have put in place. By the comments and responses we received, IG still seems like a mosquito to many, ready to bite at any moment and that bite could cost millions of dollars.

One of the first, and simplest steps that can be taken is training. Yes there is the cost of time and the money related to that time, but what is the cost of not doing it if vital business data is lost or exposed due to human error and it could have been prevented for a few thousand dollars? Just look at the online capabilities available today that enable you to provide training to your employees and partners with minimal disruption. Many businesses now make it part of the normal workday process that each day the employee must attend a half hour online session as part of their performance criteria in an effort to maintain high corporate standards, and keep corporate information safe, secure, and properly managed.

## Information Governance Policies

We all know that IG is the framework setting policy for the way information is managed, but how good are businesses when it comes to their current IG practices when matched against different business activities? We asked our respondents to position themselves in various areas and found that twenty-six percent see themselves as Trailblazers in preventing data loss, and twenty-five percent the same for compliance with legal, audits, and adhering to regulatory rules. When it comes to defensible disposition of their information, forty percent position themselves as Outlanders when it comes to reducing their storage space and defensible disposition of their information. (Figure 12)

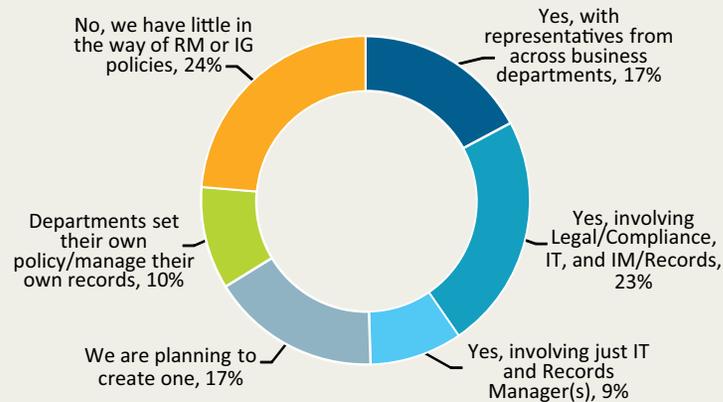
Figure 12: How would you position your company in relation to addressing the following: (Matrix: Trailblazer – Above average; Citizen – Average; Outlander – Below Average)



# INFORMATION GOVERNANCE POLICIES

If this is the case, who is driving or steering the IG direction? For nearly half of the respondents, there is a committee of some sort that may be cross-departmental, involve IT legal, IM, and the records department. For nearly a quarter there is little in the way of policies at all, let alone an oversight committee. (Figure 13)

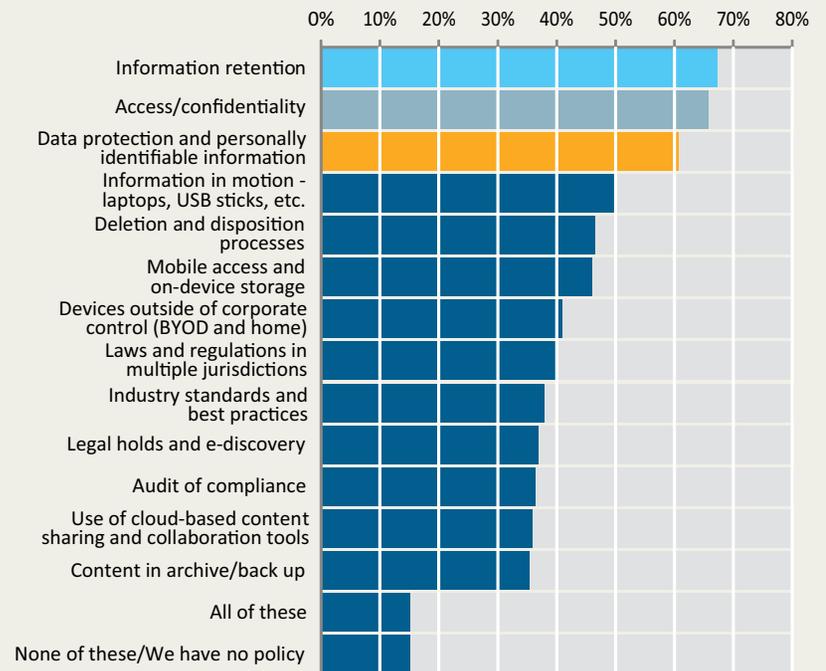
Figure 13: Do you have an Information Governance Committee?



**“Cross departmental IG committees provide greater insight across the business, to ensure measures taken in one department do not have an adverse impact in another.”**

When looking at the policies themselves, there are certain elements one might expect to find. For example, sixty-four percent of our respondents include information retention and sixty-five percent include access and confidentiality as part of their governance policy. Considering the emphasis on PII, sixty-one percent took the right approach by including this into their IG policy as did the fifty percent that included information in motion meaning it is on laptops, on USB sticks, etc. There is a group of fifteen percent, and these would be in the Trailblazer category, that report have every one of the elements we listed in their IG policy, indicating their level of seriousness when it comes to truly taking control of their information ecosystem. (Figure 14)

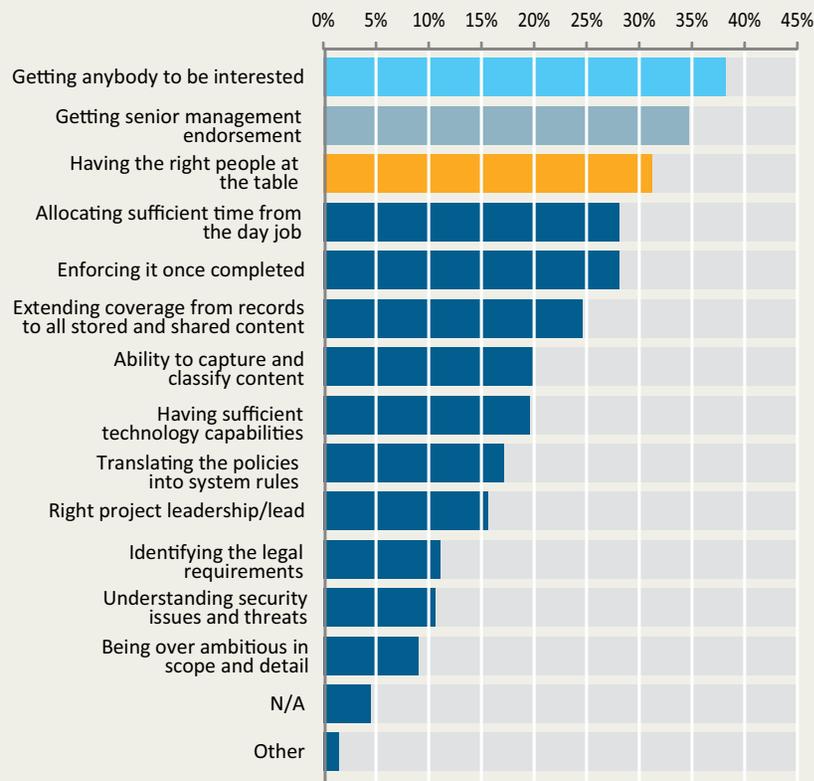
Figure 14: Which of the following elements are included in your information governance policies?



The biggest challenges reported in relation to IG are getting anyone interested (38%) getting endorsement by senior management (35%), and having the right people involved (31%). Twenty-eight percent of our respondents also equally report that they have difficulty allocating enough time from their day job to support IG efforts, and difficulty enforcing IG policies once they are complete, indicating that even though there may be verbal support from management, it is nothing more than that. (Figure 15)

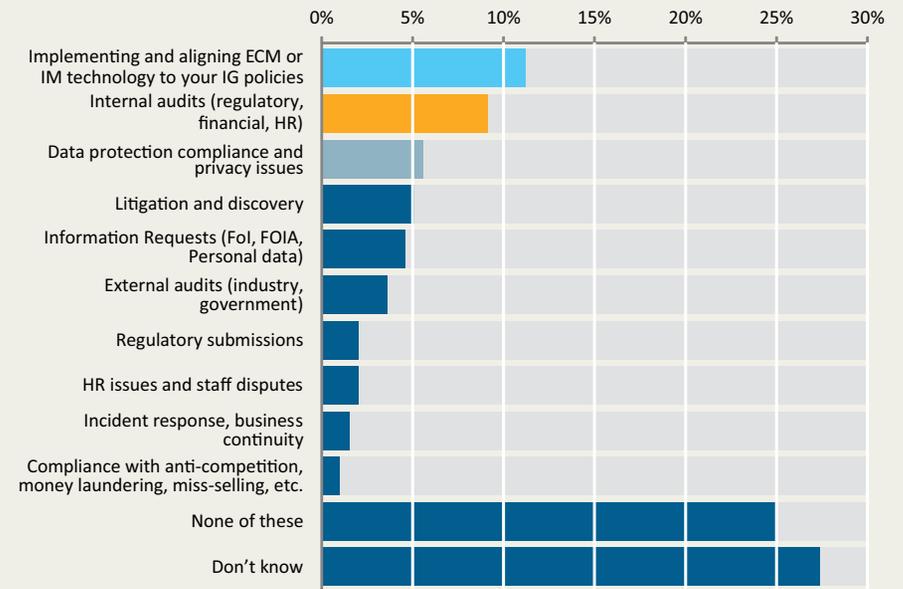
# INFORMATION GOVERNANCE POLICIES

Figure 15: What have been the three biggest issues with creating an information governance policy?



We know that non-compliance with regulatory and legal requirements can be an issue but what of non-compliance with IG practices. This points back to the lack of knowing how or inability to enforce IG policies within the business. For the majority, the response was what we expected, either no issue was evident or the respondent did not know of an issue related to non-compliance with IG policies. Eleven percent reported that there were issues implementing or aligning their ECM or IM system to their IG framework with nine percent also citing issues with their internal audits. Additionally, six percent saw issues with data protections and privacy compliance and five percent with litigation and discovery. (Figure 16) So while it is unseen for many, there are underlying issues that arise in relation to IG and non-compliance though not everyone will be aware.

Figure 16: In your organization, has non-compliance with good IG practice created a significant issue with any of the following in the last 2 years?



## Putting The Pieces Together

IG policies are an important part of the overall IG framework, but they are only as strong as they are enforceable. Time, support, and adherence to them are essential to the impact they will have and role they play in business and ensuring regulatory compliance as well as smooth business operations.

Non-compliance with IG policies, while unseen by most, will have an impact at some level and must be recognized as such. The better the policy, the closer they are followed, the stronger and smoother the business will operate overall.



# STORAGE

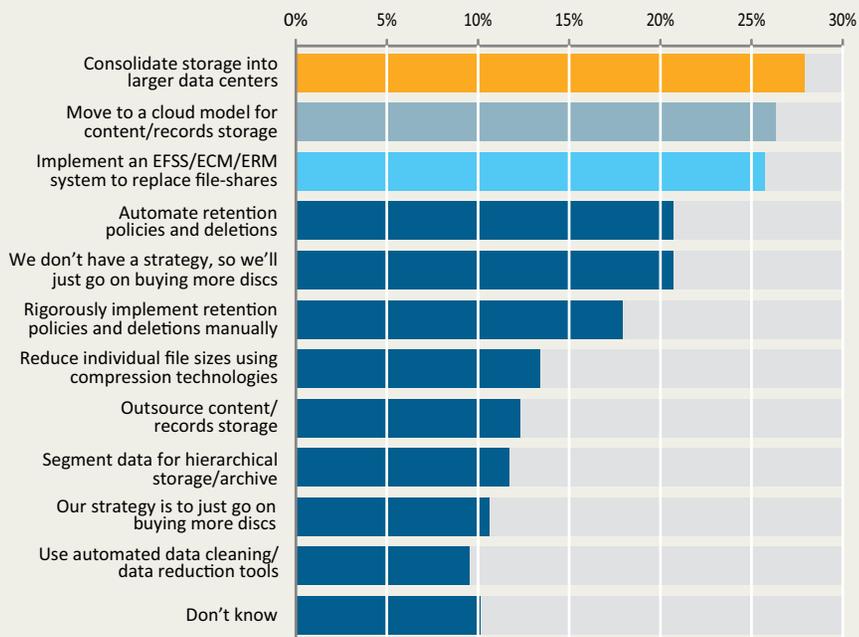
## Reduction



## Storage Reduction

Information growth is a multiplying issue for many businesses with multi-channel inbound information entering from many sources, at an all time high. Email, chat sessions, social media, and even video are all contributors to the growth factor and the need to address the governance of storage of this information. Twenty-eight percent of our respondents report that they are consolidating their storage into larger data centers while twenty-six percent are moving to a cloud model for their content and records storage needs. (Figure 17)

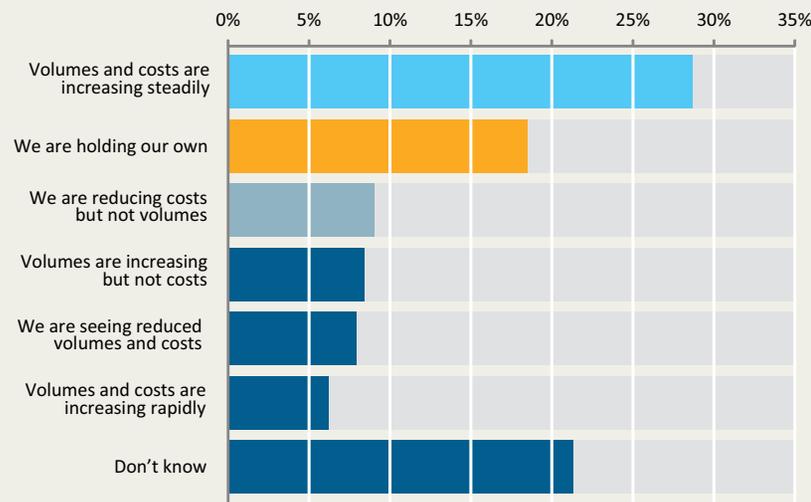
Figure 17: Which of the following strategies have you adopted to deal with the cost of storing rapidly increasing information volumes?



While buying more discs is not a sound approach, strategically speaking, several of the approaches outlined above should help alleviate some of the pain caused by this information glut. Yet twenty-nine percent of our respondents report that their volumes and costs continue to increase

while nineteen percent say they are holding their own. Nine percent cite a reduction in costs with increased volumes while eight percent cite the opposite, increased costs while lowering volumes. Indications that one is managing their information better than the other? Perhaps. (Figure 18)

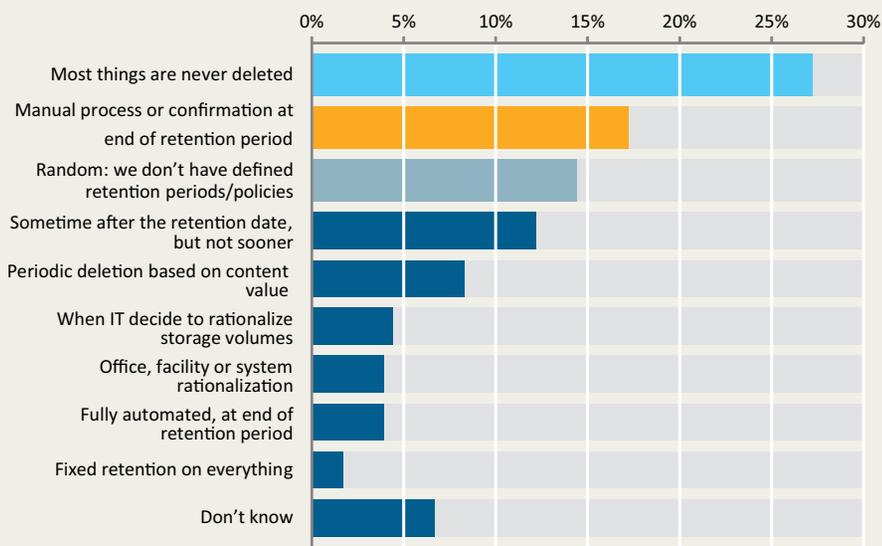
Figure 18: To what extent would you say your strategies (or lack of) are working?



We all know that one way to the amount we manage is to reduce the amount of storage we maintain, and that means we must delete information. Yet, when we asked about deletion, twenty-seven percent of our respondents report that most things are never deleted and seventeen percent cite having a manual process at the end of a retention period which of course means it is labor intensive and time consuming leading to additional costs. Fourteen percent told us they have no defined retention periods at all, indicating there is no deletion, it is done randomly, or it is left to the discretion of the employees. (Figure 19)

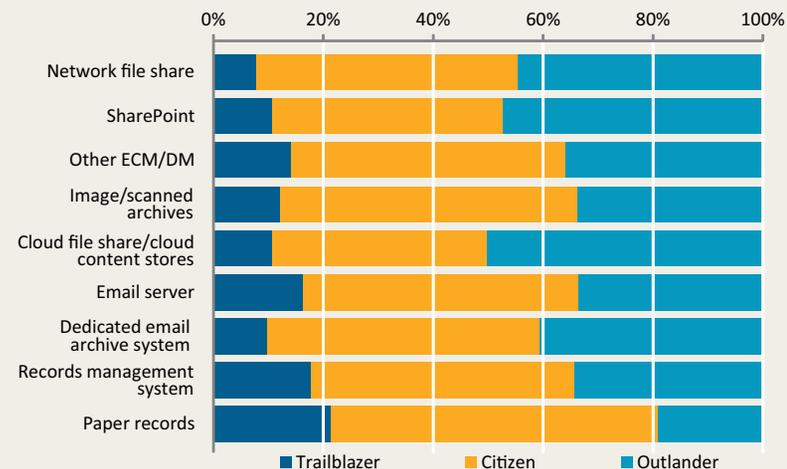
# STORAGE REDUCTION

Figure 19: How rigorously would you say content deletion is carried out in your organization?



Retention or effective retention management should be part of every IG discussion, not just for records, but also for information as a whole. Considerations should be given to the types of information and the location. When we asked about how businesses are dealing with retention based on storage locations, and to rate their effectiveness, twenty-one percent positioned themselves as Trailblazers with paper-based systems and eighteen percent with RM systems. When it came to cloud, fifty percent see themselves as Outlanders and forty-seven percent the same for SharePoint. This is likely due to the fact that many businesses utilize SharePoint as a technology first approach and may try to apply some sort of governance after the fact, and cloud is often used by the employees first, the adopted by the business if even officially, so it is unlikely any governance is in effect there either. (Figure 20)

Figure 20: How would you position your organization in relation to effective retention-period management in the following: (Matrix: Trailblazer – Above Average; Citizen – Average; Outlander – Below average)



## Putting The Pieces Together

There are many ways to view storage. Some see it inexpensive to purchase without considering the ongoing costs to maintain, and potential risk it presents in relation to maintaining outdated information. Some see it as a renewable resource that can be reused as space is cleared through deletion, and made available for new information. Some see storage as a cost factor and seek to eliminate it.

No matter how you view it, storage needs to be managed properly and needs to be part of the IG framework, not just what devices to use, but how it is used, when it is used, what it is used for, what is stored there and for how long. The deletion of information should be based on set retention policies with defined methods of destruction that are defensible should they be challenged in times of audit or litigation. IG sets the tone and paves the way for your business to manage and reduce storage according to your business needs and requirements.



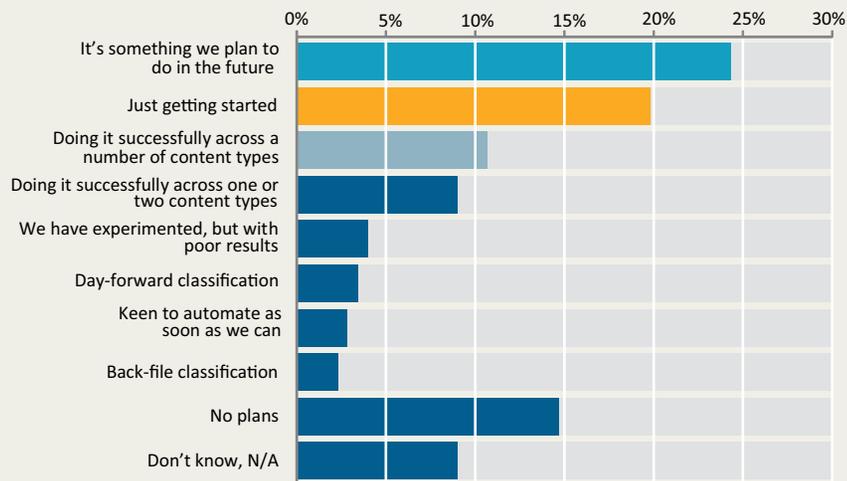
# AUTO- CLASSIFICATION



## Auto-Classification

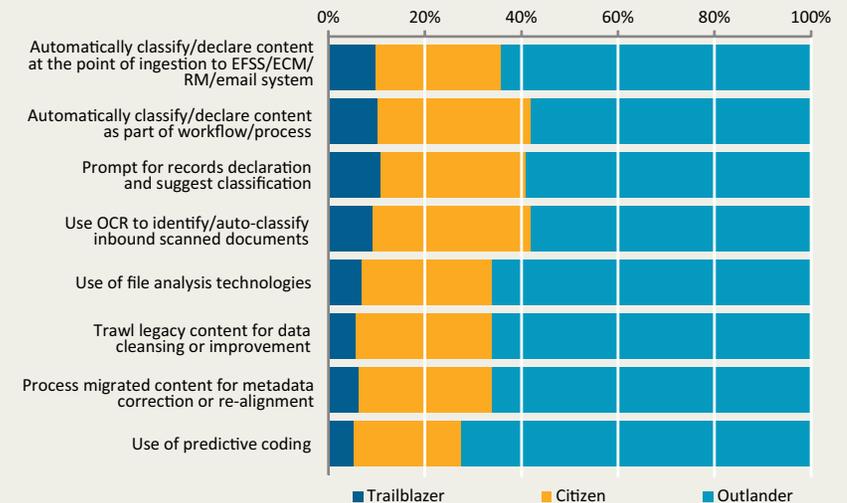
Automation is one way to help manage various processes, maintain consistency and accuracy, and support compliance. Auto-classification is one way to automate the declaration and classification of records and information to apply metadata, security and access controls, and assign retention periods. Eleven percent of the respondents we polled reported they are currently using auto-classification aligned with their IG practices across a number of information types with twenty percent just getting started. It is the planning stage for twenty-four percent and not even on the scope for fifteen percent who say there are no plans at all for auto-classification. (Figure 21)

Figure 21: How would you best describe your overall plans for automated declaration/classification of records?



Turning our attention to various capabilities, we asked our respondents to rate their companies on various activities and automations. Eleven percent see themselves as Trailblazers in prompting and suggestion for records declaration and classification, and ten percent see themselves as same for automated declaration and classification of content ten at the point of ingestion to their EFSS, ERM, email, and ECM systems. Sadly, the majority see themselves as Outlanders in every area we presented even though some capabilities, like the use of OCR to identify and auto-classify inbound scanned documents, have been available for a couple of decades. (Figure 22)

Figure 22. How would you position your company in the following areas? (Matrix: Trailblazer – Above Average; Citizen – Average; Outlander – Below average)



Use of automated tools is not restricted to auto-classification and in fact has expanded to include detection of security risks and misallocated access or confidentially for thirty percent of our respondents and file duplication as reported by twenty-seven percent. Along these lines, twenty-seven percent also report using automation to monitor unusual activity and non-compliance with appropriate use policies, indicating good alignment with their IG framework. (Figure 23)



Figure 23: Do you use any automated tools to perform the following functions?

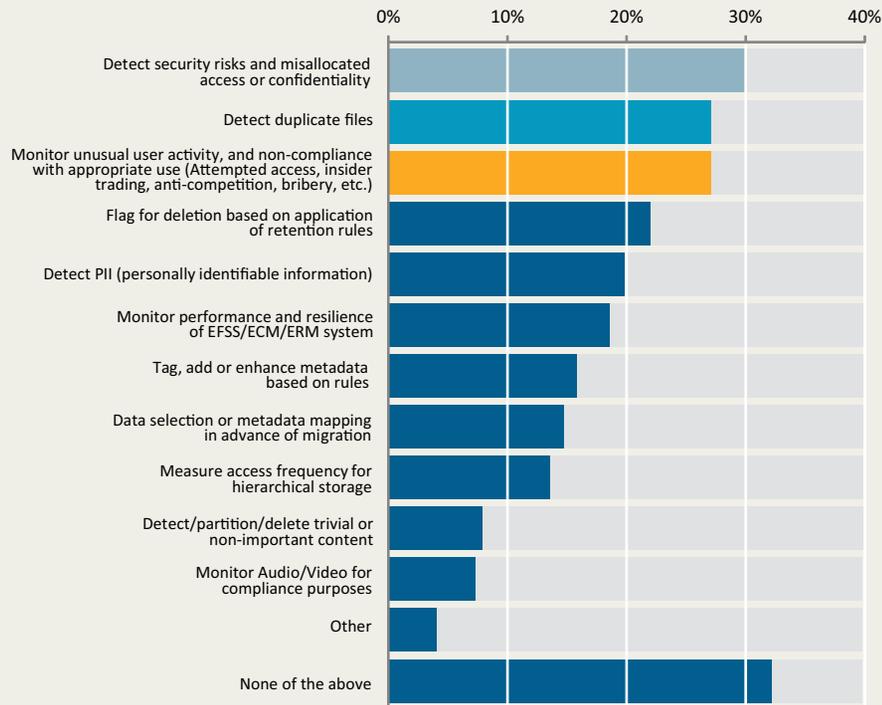
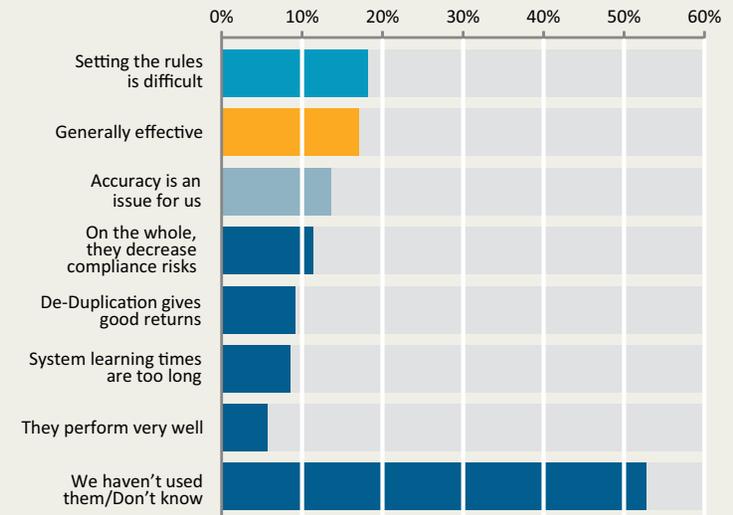


Figure 24: What have been your experiences with classification tools?



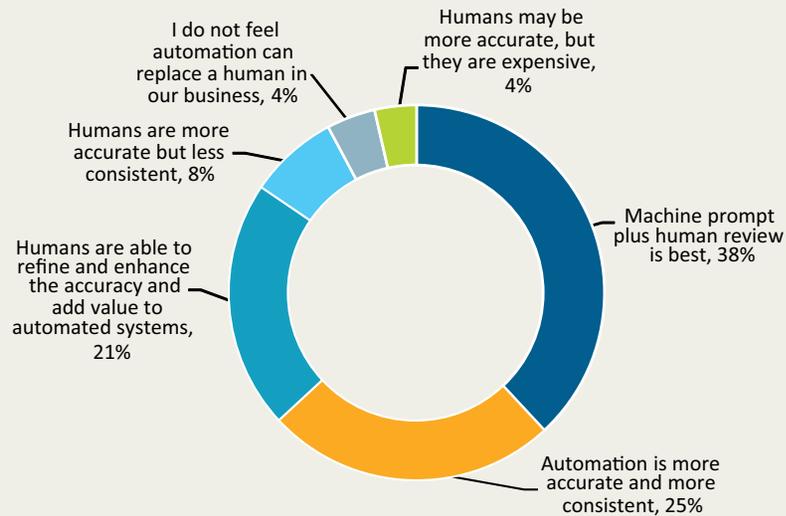
Is machine accuracy higher than human accuracy? According to one quarter of our respondents, the answer is yes, and there is more consistency with machines as they are less prone to make a mistake once the rules are in place. Thirty-eight percent see a combination of human and machine as the best combination of accuracy, given the machine being good at identifying data and the human able to put things into context. (Figure 25)

While some have had great results with classification tools, others may not have been so fortunate. Six percent reported that these tools have performed very well for them and eleven percent feels that overall, have helped decrease their compliance risks. For eighteen percent the level of difficulty setting the rules is too high and fourteen percent say that they have issue with the accuracy rates. (Figure 24) As with any technology, there is an expectation and a realization along with a learning curve. Many times the expectation is that out-of-the-box, the product will deliver at one hundred percent accuracy when the realistic approach is that it will take time and effort to achieve a reasonable level and transaction rate.



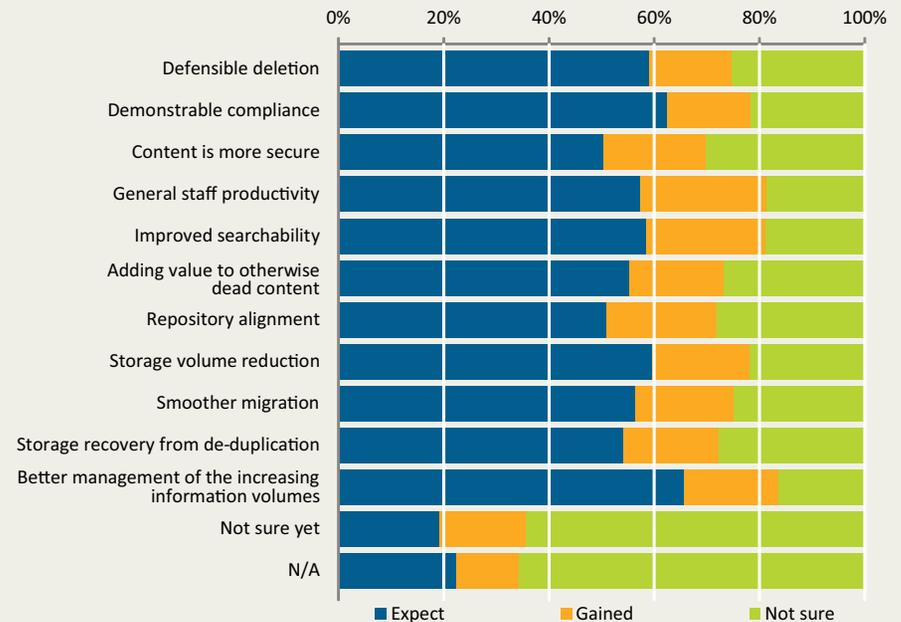
# AUTO-CLASSIFICATION

Figure 25: In your experience, describe the accuracy that automated systems achieve compared to manual?



There is always an expectation that goes along with technology use and any changes we make in business, and this holds true of auto-classification in relation to IG. Defensible deletion was an expected benefit for fifty-six percent of our respondents yet only sixteen percent report actually gaining it. Likewise, sixty-six percent of respondents expected they would have better management over the increasing volumes of their information yet only sixteen percent report gaining in this area. (Figure 26) Could it be that they were oversold on the technology, or perhaps they did not have a clear understanding of the underlying business problem they were trying to solve in the first place? Of course we did see earlier in this report that enforcement of IG policies is an issue and that deletion of information did not happen for many so perhaps it is the combination of these that resulted in the inability to gain the expected results. One thing is clear; the expectation far exceeded the result.

Figure 26: What benefits would you expect or what benefits have you gained from automated classification? (Matrix: Expect; Gained; Not sure)

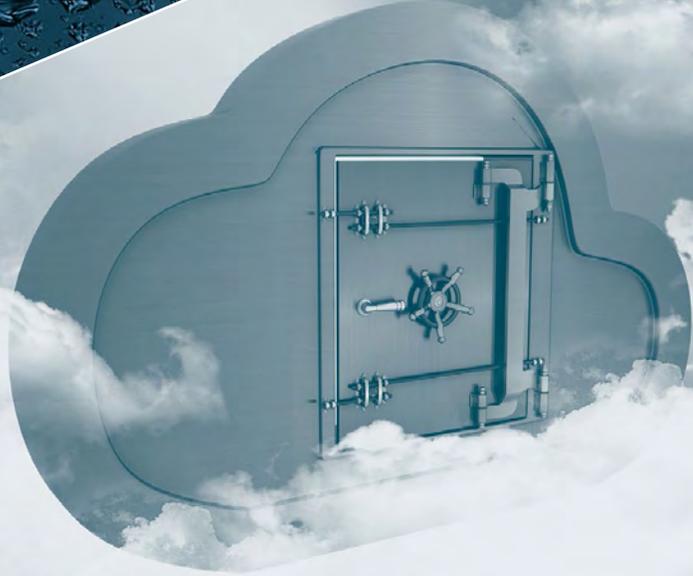


## Putting The Pieces Together

Automation, auto-classification, the use of various recognition technologies are all tools that can help businesses become more efficient, consistent, and compliant in their day-to-day activities. While there is work to be done to set-up the rules and train these technologies, the end result can reap great benefit in both a return-on-investment, and defensibility through consistent practices. The key is to identify what you are trying to accomplish, establish governance around the information, tools and methods related to their use, and set realistic expectations as to what you will and will not be able to accomplish with in specific timelines.



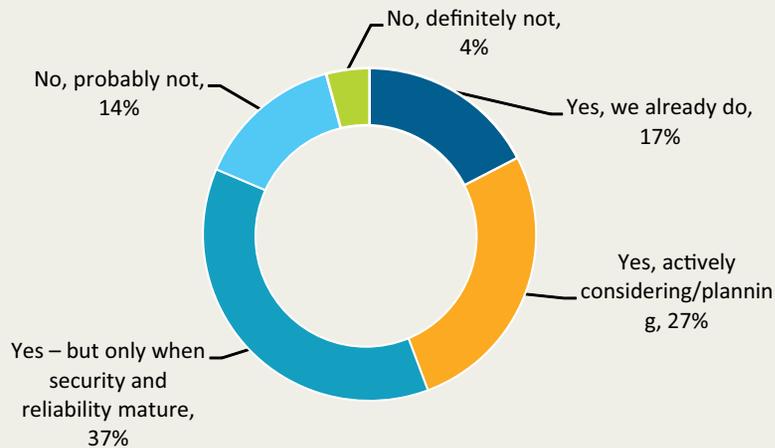
# CLOUD



## Cloud

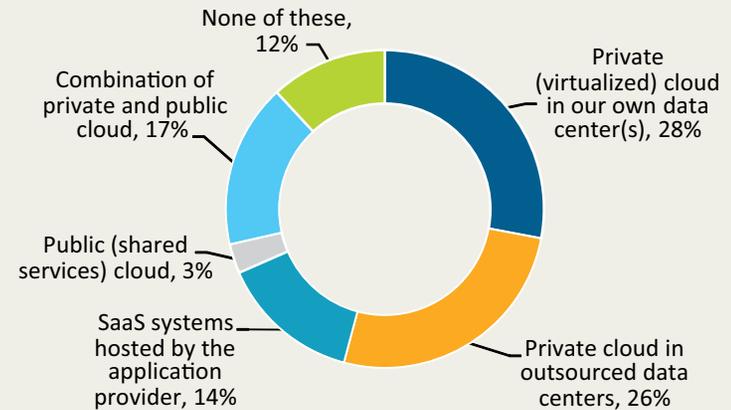
The cloud is in use in your business, whether you have officially adopted it or not, chances are, someone is using it somewhere to share files with internal or external parties. The questions are do you or would you consider adopting cloud for your business records? While many of use the cloud today for personal use like banking, only seventeen percent of our respondents say they are using the cloud or a SaaS system for their records today with twenty-seven percent indicating they are planning for it. Thirty-seven percent still show reluctance due to the reliability and security concerns. (Figure 27)

Figure 27: Would you consider adopting a Cloud/SaaS system for your records?



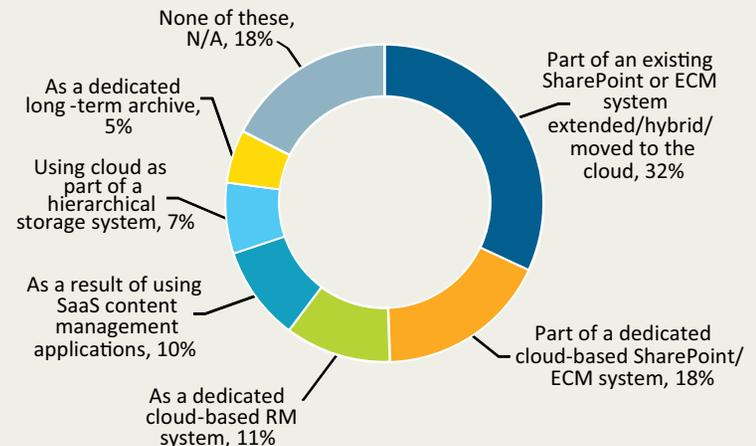
When asked about cloud model preference and find that twenty-eight percent report they prefer a private cloud in their data center while twenty-six percent prefer a private cloud that is outsourced. Seventeen percent see the combination of a private and public cloud as the best approach to meet their needs. (Figure 28)

Figure 28. Which of the following is your preferred cloud model for your records system(s)?



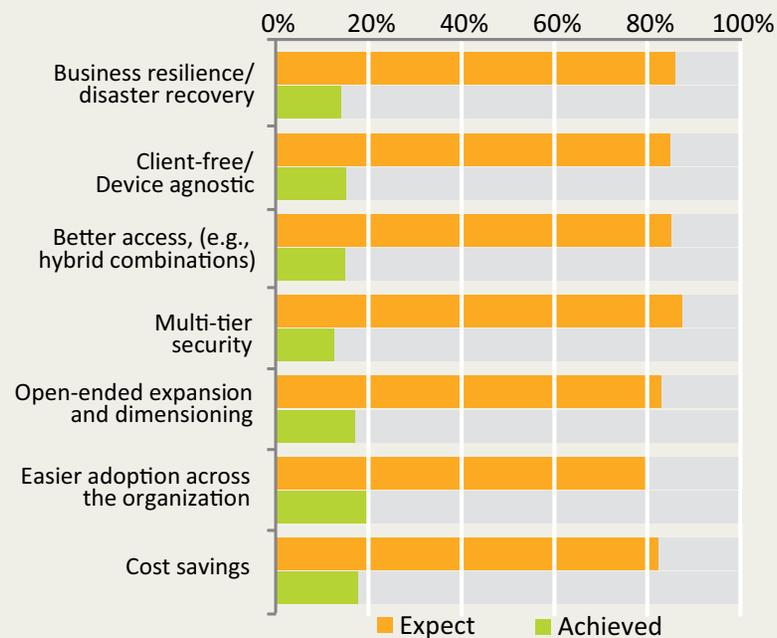
It is not surprising that the majority prefer a private cloud model in order to maintain a level of control. The question becomes one of how this is addressed in their IG policies in relations to responsibilities, monitoring, and auditing and accountability of the provider when services are outsourced. When asked how the cloud would be used, thirty-two percent said they would extend their SharePoint or ECM system as a hybrid and eighteen percent would make it part of a dedicated SharePoint or ECM system. (Figure 29)

Figure 29: What would be the most likely way that you would (or do) use cloud for your records?



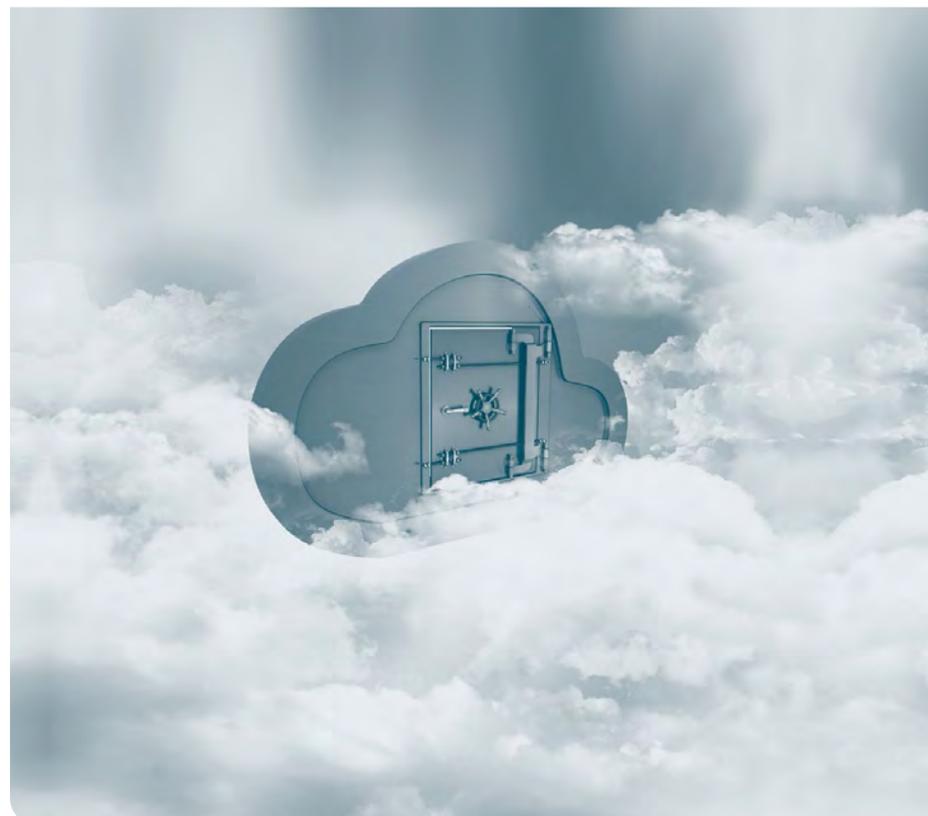
As with auto-classification, there is an expectation of benefit and a realized benefit gained so we asked that of cloud. Eighty-seven percent of our respondents said they expected to have multi-tiered security while only thirteen percent report achieving it. Another expectation was better business resilience and disaster recovery for eighty-six percent while only fourteen percent say they actually achieved that. The best result, still with low achievement against expectation was that of adoption across the enterprise with eighty percent expecting it and twenty percent achieving it. (Figure 30) Once again it begs the question of how the expectation was set in relation to solving a business problem.

*Figure 30: What benefits would you be looking for or have you achieved in a cloud solution?*



## Putting The Pieces Together

There is great opportunity to be found in cloud use as we see in this report, there is still much reluctance on the part of the user community due to distrust in reliability and security. But is it a question of reliability on the part of the service provider hosting the cloud application or connectivity and when it comes to security, what levels of security are required and how are they to be handled? All of this can and should be spelled out in an IG framework with the service providers required to follow these policies and your business ready to audit and challenge them the same as you should enforce and challenge your employees. Remember, a contractor or contracted service is your responsibility and it is on you to ensure they follow the same rules you are required to follow.



# LEGAL HOLD

## and ediscovery



data  
protection

secure  
Mobile  
devices

ediscovery

Internet  
security

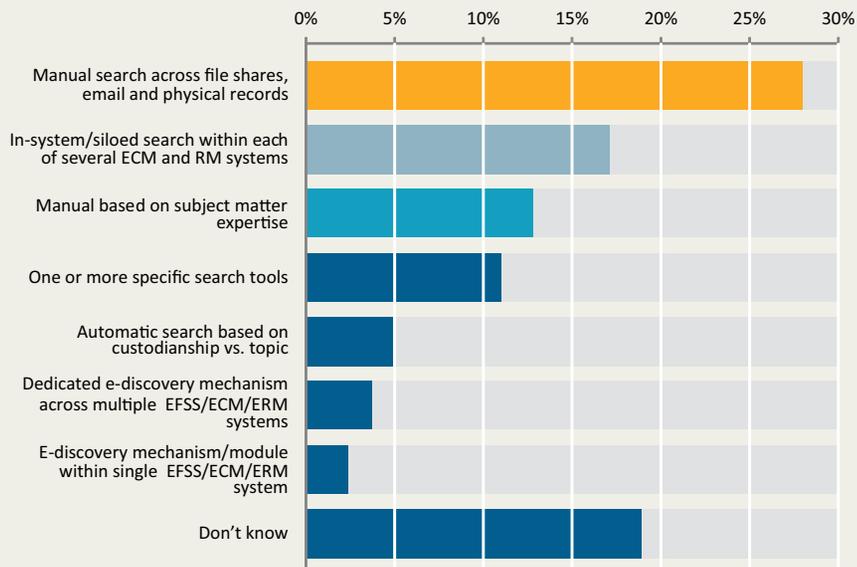
Cyber  
security

secure  
storage

## Legal Hold and ediscovery

Ask most employees about legal hold or ediscovery, and they will likely have no clue what you are talking about. If you ask them about your company's policies related to either of these, chances are high that they will not know what these policies are, even if they are spelled out in the employee handbook. When we asked specifically about ediscovery, twenty-eight percent of our respondents told us they do a manual search for information across their file-shares, email, and physical records. Seventeen percent cite the ability to conduct in-system (siload) searches within each ECM and RM system, and thirteen percent conduct manual searches based on subject matter expert. (Figure 31) These are extremely time consuming and costly approaches that will also result in information being missed and overlooked due to an inability to identify every possible location.

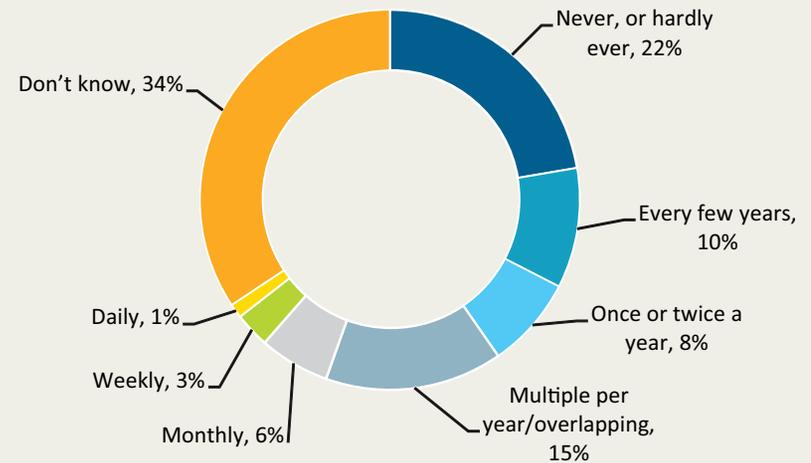
Figure 31: What is your primary ediscovery mechanism?



Thinking about the amount of effort related to ediscovery and the fact that a hold is typically placed when this type of search is required, it begs the question, how often does a legal hold or investigation of this type occur in your business? Weekly was the answer we received from three percent of our respondents and monthly for six percent. While this may be the extreme,

fifteen percent do indicate this happens multiple times per year and is typically overlapping, while twenty two percent hardly ever experience them. (Figure 32) This could be due to the nature of their businesses or perhaps the difference between those who are well prepared and equipped for such occurrences where the impact to on the general population is minimal, and those who are not so well prepared and the impact is significant.

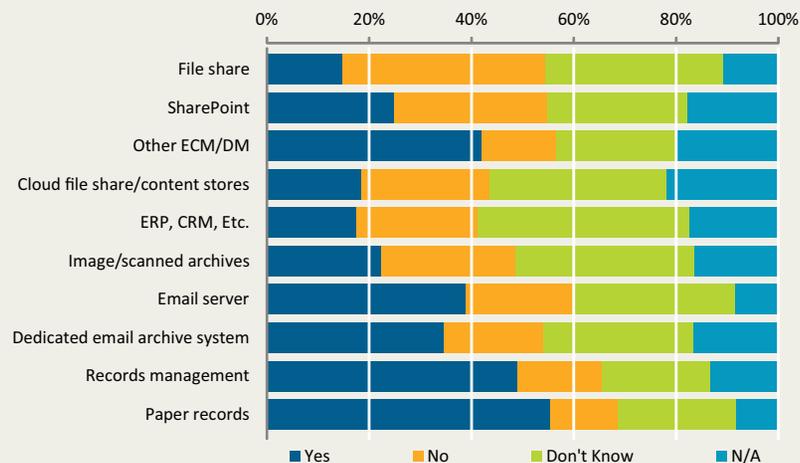
Figure 32: How often do you have legal holds applied to stored electronic content pending litigation or investigation?



It could be that the percentage of respondents described above indicating they hardly have any legal holds may not be aware of them due to automated systems in place, minimizing the amount of human interaction required to implement the hold. For example, nearly half of our respondents indicate they have effective legal hold mechanisms on the records management systems, forty-two percent on their ECM and DM systems, and thirty-nine percent on their email servers. This would indicate some level of efficiency in these areas minimizing the need for employee involvement. On the other hand, forty percent do not have good hold mechanisms on their file-shares and thirty percent report the same for the SharePoint systems, indicating the need for increased employee engagement in these areas. (Figure 33)

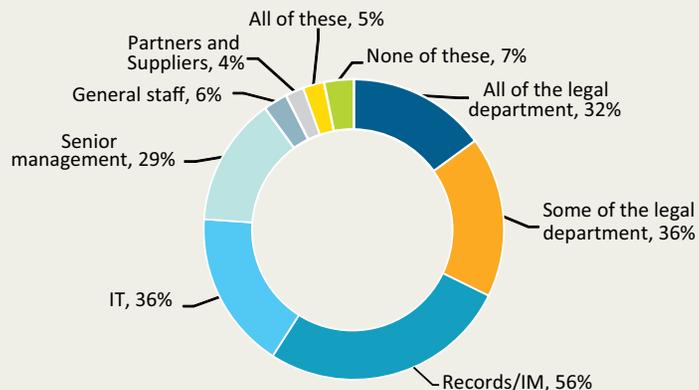
# LEGAL HOLD AND EDISCOVERY

Figure 33: Which of your content systems has an effective legal hold mechanism?



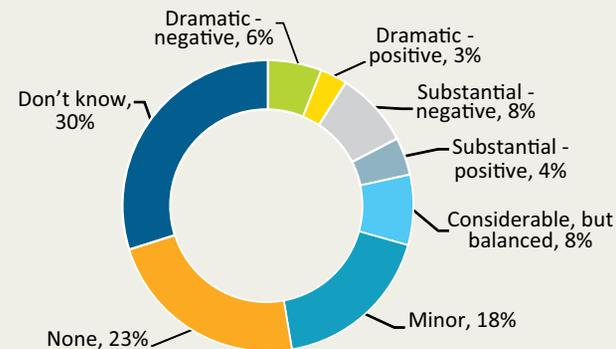
Understanding the policies and mechanisms of a legal hold is critical to their success and defensibility so it stands to reason that certain individuals within the business should be expected to have a high level of understanding and others a basic level. Surprisingly, thirty-six percent of our respondents feel that only some of their legal departments understand the policies and mechanisms while thirty-two percent feel all of their legal departments have this understanding. Fifty-six percent are confident their records manager understand the policies and mechanisms, and only twenty-nine percent feel their senior management understand the policies and mechanisms of a legal hold. (Figure 34)

Figure 34: Who in your organization would you say understand the policies and mechanisms of legal hold?



Retention plays a major role in the amount of effort required to find information during a legal hold and ediscovery investigation. The more information you have, the more you have to sort through, so it stands to reason that the more you can legally dispose of, the better off you will be in relation to these investigations. When we asked about the impact of retention in relation to fines, damages, or awards hinging on the validity, completeness, or retention of records, twenty-three percent said there was no impact at all and eight percent said it was considerable but balanced between positive and negative impact. Six percent said they saw a dramatic negative impact with eight percent seeing a substantial negative impact while three percent saw a dramatic positive impact and four percent a substantial positive impact, indicating the difference between sound and poor retention practices. (Figure 35)

Figure 35: How would you describe the financial impact (positive or negative) of fines, damages or awards resulting from cases or potential cases in the past two years, which hinged around the validity, completeness, or retention of your electronic records?



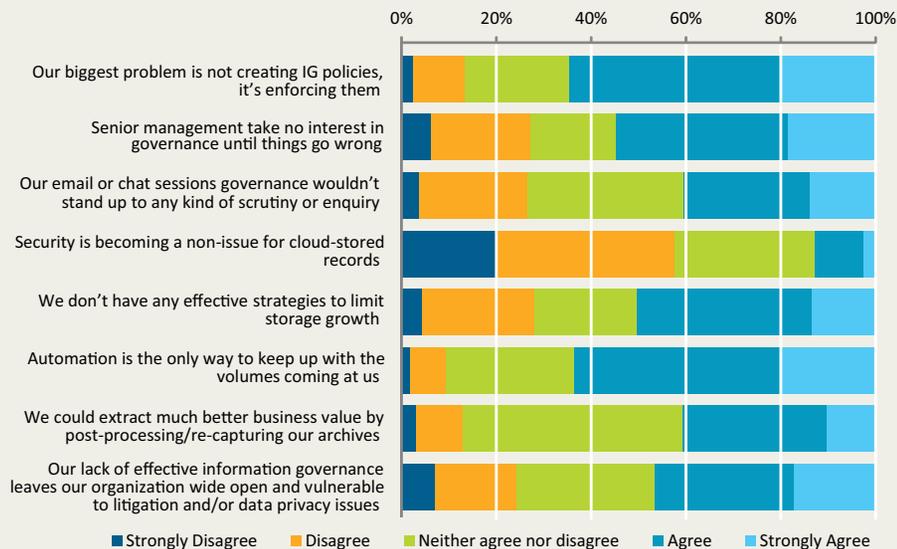
## Putting The Pieces Together

Many businesses see legal hold and ediscovery as something for the legal department to be concerned with but in fact, it is something every employee should be aware of and it should be part of the overall IG framework. When legal hold is issued, and ediscovery investigations begin, information must be found and preserved else the business is at risk of fines and in some countries employees can be prosecuted for obstruction of justice based on intentional destruction of evidence. IG can establish the policies and technology can help enforce those policies, in some cases so transparently there is no impact to or involvement required of the employee.

## Opinion and Spend

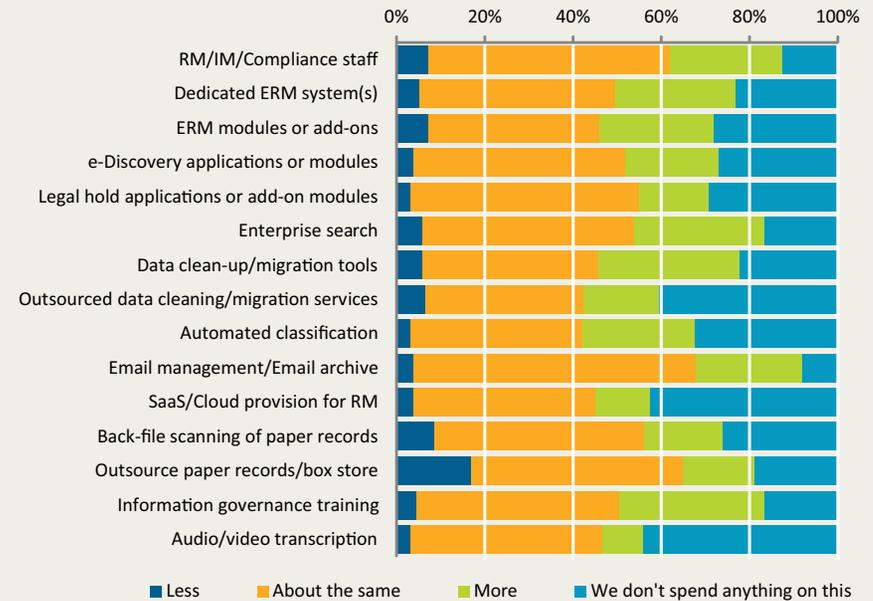
We know that IG enforcement is seen as a major issue for many businesses, the majority of respondents in this report. The same could be said of the lack of support given by senior management even though a few say it is high on their agenda. One thing is also clear from the majority and that is the message that automation is the key to future success and the only way to keep with the increasing volumes of information according to the forty-three percent who agree and twenty percent who strongly agree with this statement. (Figure 36)

Figure 36: How do you feel about the following statements?



Given that automation technology seems to be the direction of the future, one might think that is where the money will flow, yet when we look at spending over the next year, thirty-three percent will spend more on training, thirty-two percent on data cleanup and migration tools, and thirty percent on enterprise search. (Figure 37)

Figure 37: How do you think your organization's spending on the following products and applications in the next 12 months will compare with what was actually spent in the last 12 months?



## Putting The Pieces Together

Business are focusing on areas where they should see results quickly; by training their employees, cleaning their data assets and enhancing their search capabilities, they will increase findability. From an IG perspective, all of this needs to be part of the IG framework and an ongoing or continuous effort not just a single shot. The next step should be automation wherever and whenever possible to enhance operations, gain better consistency, and enhance defensibility and compliance.

# CONCLUSIONS

&

## Recommendations



## Conclusions and Recommendations

The real world view of governance and compliance has not changed much since our 2015 report in the sense there is still a lack of true support from management, though we are seeing a slight increase in the level of importance being placed on IG, likely due to regulatory reasons. There is still much chaos in relation to email, file-shares, and even SharePoint when it comes to managing retention and deletion of content and information as a whole, but not with records of course. There are still gaps in IG when it comes to addressing cloud, mobile, and external access controls, and there is still concern over security and reliability of the cloud. Most interesting, and perhaps unsettling, is the perception that corporate legal is viewed as only somewhat understanding the policies and mechanisms of legal hold in some organizations, given they are the ones responsible to issue and manage the process.

It is clear there is still a long way to go in many organizations, when it comes to building an IG framework, implementing it across the enterprise, and educating all who interact with corporate information about the policies, processes, and tools to be used. There is no best time, only a right time to begin and that is now. Take the steps to understand what is actually in place; what is working, what needs enhancing and what is missing. Then formulate a plan to make it all move forward. Here are some things to consider that may help you in your IG journey.

## Recommendations

- Create an information governance team including representatives from IT, Records Management, Compliance, Legal, and Line of Business.
- Review the risks posed by the types of information that you hold should they be lost or exposed, and make senior management aware of the potential consequences of a breach, including those involving internal staff or caused by general negligence.

- Draft an information governance policy. Focus initial efforts on areas where the content is the most sensitive (e.g., HR records, customer records, IP), but also where there is least governance at present (e.g., email, shared drives, cloud file shares, mobile).
- Set retention periods for specific content types and audit your ECM system(s), records management system, and email archive to ensure that they have retention management configured and switched on. Also check that procedures are in place for setting legal holds.
- Pay particular attention to your email management. Use value-based criteria to set deletion policies. Consider selective archiving using automation, and ensure that the archive is optimized for search, ediscovery, and legal hold.
- Consider running automated metadata correction, de-duplication, and retention policy enforcement across all of your content systems in order to remove redundant, out-of-date, and trivial content, and to improve search capabilities.
- If you have extensive image archives of scanned documents that are largely unsearchable, consider re-capturing them with modern OCR to create enhanced metadata and improve potential for analytics.
- Investigate day-forward automated classification, particularly for email, process archives and routine inbound content. Consider using automation to simplify user-filing accuracy, and in effect, automate ongoing compliance.

If unsure of where to begin or how to begin, seek professional assistance and/or training to help determine the right path. Look to current suppliers and service providers for guidance. Turn to professional associations and peers to find advice and training that will provide best practices. It is better to take a step forward and learn than to take no step and fall behind.



# SURVEY DEMOGRAPHICS



# APPENDIX 1: SURVEY DEMOGRAPHICS

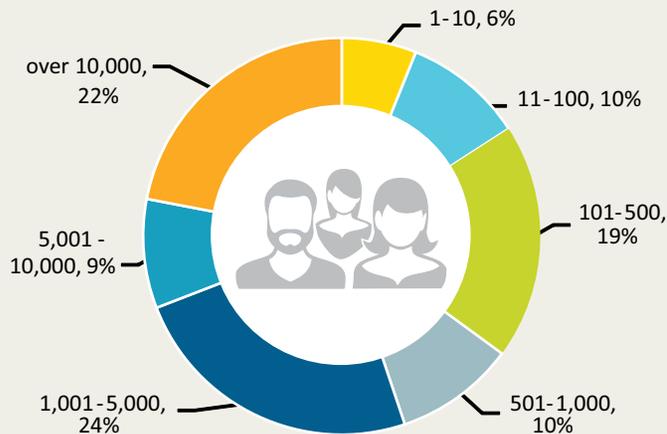
## Survey Demographics

### Survey Background

The survey was conducted with a web-based tool collecting responses from 218 individual members of the AIIM community during the month of June 2017. Invitations to take the survey were sent via email to a selection of the 195,000+ AIIM community members and through various social media outlets.

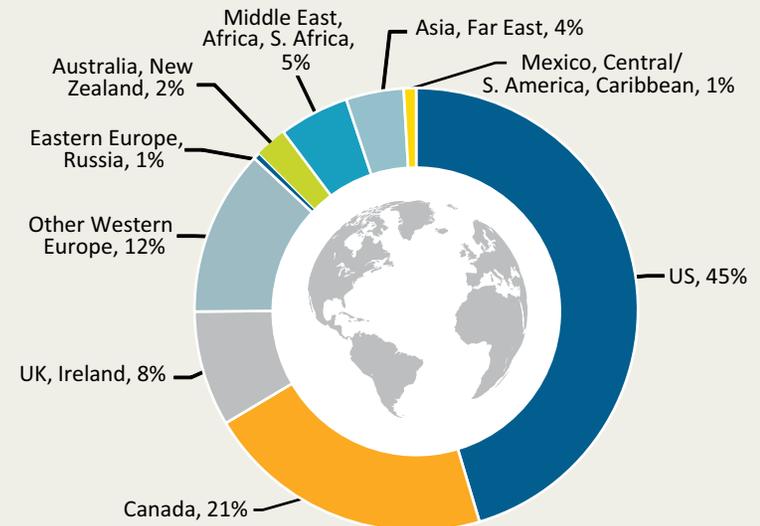
### Organizational Size

AIIM survey respondents represent organizations of all sizes. Larger organizations over 5,000 employees represent 31%, with mid-sized organizations of 501 to 5,000 employees at 34%. Small-to-mid sized organizations with 1 to 500 employees representing the largest segment of survey takers at 35%.



### Geography

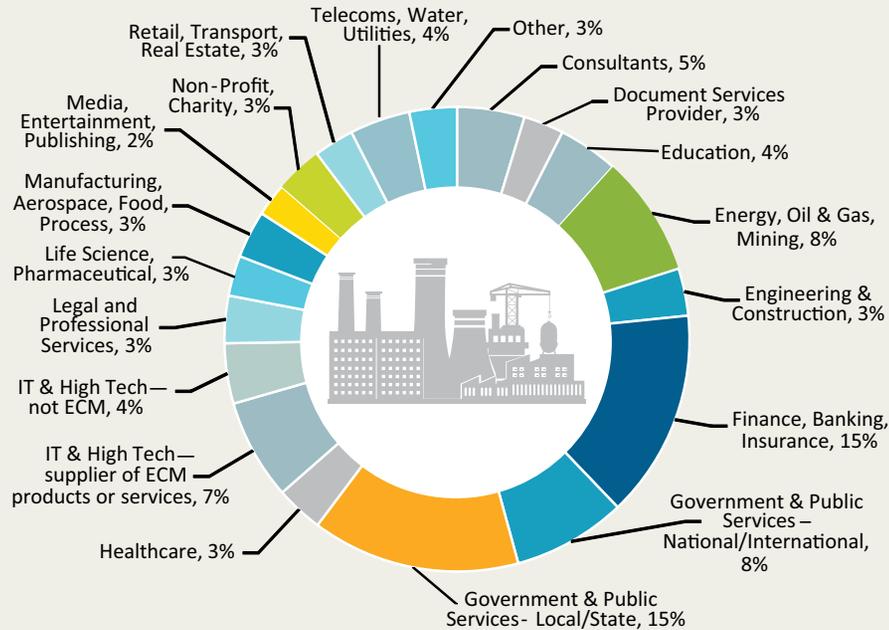
66% of the participants are based in North America, with 26% from EMEA-R, and 8% rest-of-world.



# APPENDIX 1: SURVEY DEMOGRAPHICS

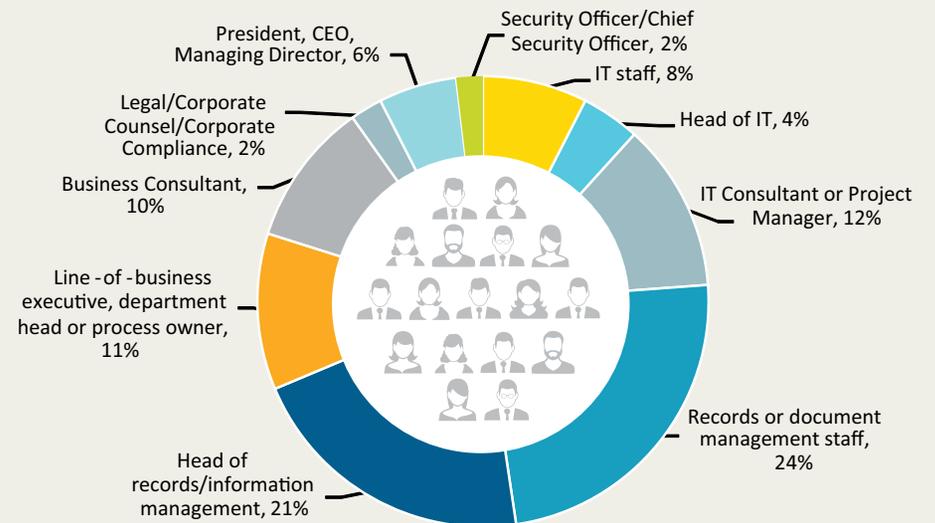
## Industry Sector

Local and National Government together make up 23%; Finance, Banking, and Insurance 15%; and Energy, Oil, Gas, and Mining 8%.



## Job Roles

21% heads of records and information management; 24% records or document management staff; 17% C-level Executives, Presidents, CEOs, and Line-of-Business Executives.



## Open-ended Comments

Respondents were able to provide open-ended comments about digital transformation. Here are a select few that represent the general:

- More emphasis is being placed on stronger IG and automated classification for better records management and better search functions.
- Not enough smart people get together in the same room to develop a comprehensive strategy to address the challenges this survey addresses (at least in the Federal Government); not enough people are looking forward and thinking about the positive impacts big data, cloud computing, and machine learning can have in this space. I feel like the only one at my agency and it's exhausting (like bashing my head against a wall repeatedly while things continue to get worse). Most people don't see or don't care.
- IG is fundamental thus governance tool like policies be in place and most importantly compliance must be measured to allow accurate compliance.
- Providers have oversold the ease and effectiveness of their ECM products and so companies are skeptical and slow to take on big changes. Success is dependent on the engagement at all levels of business and too often IT and RM try to do it all. That may work for implementation but not for long-term operation.



## opentext™

### opentext™

OpenText™ Enterprise Content Management (ECM) solutions help organizations Connect Content to their Digital Business.

Based on industry-leading content lifecycle management, document management, and a large and growing list of content services, OpenText ECM solutions capture and deliver content in the context of your organization's key business processes.

OpenText ECM Solutions transform Personal Productivity with simple, intuitive tools and user experiences; Process Productivity with integration into lead applications such as SAP®, Salesforce®, and Microsoft®; and Control with trusted OpenText governance and security.

Utilized by the largest and most innovative companies and governments in the world to transform and drive their digital business, OpenText ECM solutions are available and deployed on-premises and in private and public clouds.

Learn more about OpenText ECM solutions at  
[www.opentext.com](http://www.opentext.com)

## You've just downloaded and read the latest AIIM Industry Watch Report on Governance and Compliance 2017. What now?



Take your skills to the next level by learning how to map, design, capture and automate operational processes using a combination of strategies, and technologies with AIIM's Training Courses

Learn more, visit: [www.aiim.org/training](http://www.aiim.org/training)



AIIM ([www.aiim.org](http://www.aiim.org)) AIIM is the global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data.

© 2016

#### AIIM

1100 Wayne Avenue, Suite 1100  
Silver Spring, MD 20910  
+1 301.587.8202  
[www.aiim.org](http://www.aiim.org)

#### AIIM Europe

Office 1, Broomhall Business Centre,  
Worcester, WR5 2NT, UK  
+44 (0)1905 727600  
[www.aiim.org](http://www.aiim.org)