aiim eBook

Delivering the priorities and opinions of AIIM's 193,000 community

MINIMIZE BUSINESS RISK:

TOP 5

Information Governance Obstacles You Must Tackle Now

In Partnership with

Canon
CANON BUSINESS PROCESS SERVICES, INC.

aiim

About this eBook

As the non-profit association dedicated to nurturing, growing and supporting the user and supplier communities of ECM (Enterprise Content Management) and Social Business Systems, AIIM is proud to provide this research at no charge. In this way, the entire community can take full advantage of the education, thought-leadership and direction provided by our work. Our objective is to present the "wisdom of the crowds" based on our 190,000+-strong community.

We are happy to extend free use of the materials in this report to end-user companies and to independent consultants, but not to suppliers of ECM systems, products and services, other than Canon, its subsidiaries, and its partners. Any use of this material must carry the attribution – "© AIIM 2017 www.aiim.org / © 2017 Canon Business Process Services cbps.canon.com"

Rather than redistribute a copy of this report to your colleagues, we would prefer that you direct them to www.aiim.org/research for a download of their own.

Our ability to deliver such high-quality research is made possible by the financial support of our underwriting sponsor, without whom we would have to return to a paid subscription model. For that, we hope you will join us in thanking our underwriter for this support:

Canon
CANON BUSINESS PROCESS SERVICES, INC.

Canon Business Process Services
261 Madison Avenue, 3rd Floor
New York, NY 10016
Tel: +1 212-502-2100
Web: cbps.canon.com

Process Used & Survey Demographics

The survey results quoted in this report are taken from the various AIIM Industry Watch reports listed in the references section of this paper. Responses were collected from individual members of the AIIM community using a web-based tool. Invitations to take the survey were sent via email to a selection of AIIM's 190,000+ registered individuals.

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.

About AIIM

aiim

AIIM has been an advocate and supporter of information professionals for nearly 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. AIIM runs a series of training programs, which can be found at www.aiim.org/Training.

Introduction

When many business executives hear the term "information governance" (IG), they assume that their enterprise has the policies, procedures, best practices and staff in place to help continuously minimize business risk. Often, however, this is not the case.

One way to begin correcting this situation is with a clear understanding of IG. Here's one definition: IG is an accountability framework that enables organizations to create, store, use and dispose of information in accordance with regulatory, legal, risk mitigation and business workflow requirements. As an Information Professional and business leader, there are five key areas of focus that can help you to teach employees of the importance of IG and align the organization to support your IG initiatives, policies, and practices. These are:

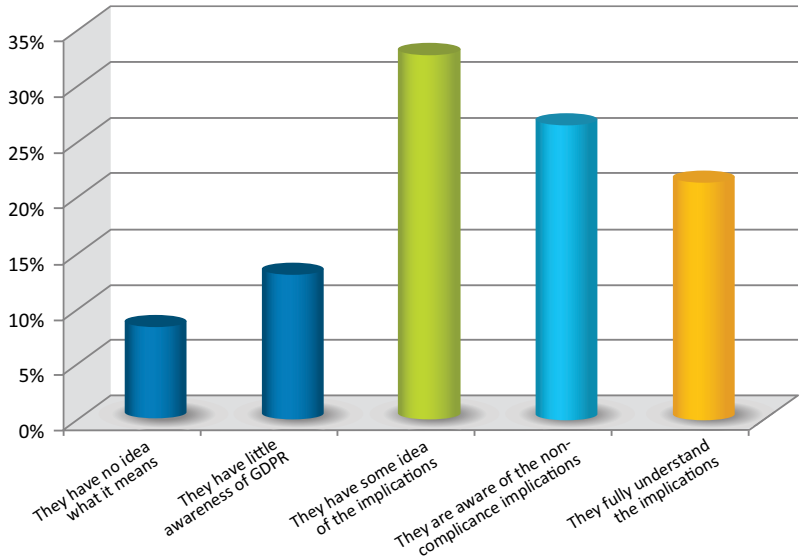
- *Keeping up-to-date on the latest regulation and compliance requirements*
- *The impact of the cloud for your data repository*
- *Managing data remediation*
- *Threat awareness*
- *The importance of metadata and managing retention*

Keeping Up-to-Date

Keeping up-to-date on the latest regulations, compliance requirements and court decisions is essential in the development and upkeep of your IG program. As one example, in April of 2016 the European Union (EU) passed the General Data Protection Regulation (GDPR). In particular there is emphasis on Personally Identifiable Information (PII) including how and where it is kept, if it can be kept, how and when it is destroyed as well as the need for Data Protection Officers (DPO) and much more.

While it is a EU regulation, the implications of the GDPR are far reaching in that as a multi-national business, it would impact you if you transact business in a EU governed country. So as you can see, this along with other government, legal and industry developments can affect the foundation of your IG program. It is imperative that you stay informed and updated on all of the regulations that relate to your business. Yet a recent AIIM study finds twenty-one percent of businesses feel their executives have little awareness (13%) to no idea (8%) of what the GDPR is, indicating for these businesses, it will be a struggle over the next several months, should they decide to take action.[1] (Figure 1)

Figure 1. On a scale of 1 to 5 (1 have no idea and 5 fully understand the implications) how would you rate the level of understanding your executives have of the implications of GDPR non-compliance?



As part of your IG program it is important to educate employees on structured, semi-structured, and unstructured data and content. This includes clarifying how these forms of data are captured, stored, managed, preserved, shared, and destroyed in ways that comply with your IG framework and are defensible across the enterprise and around the globe. So how do you help ensure compliance with industry regulation like the GDPR? Things to consider include:

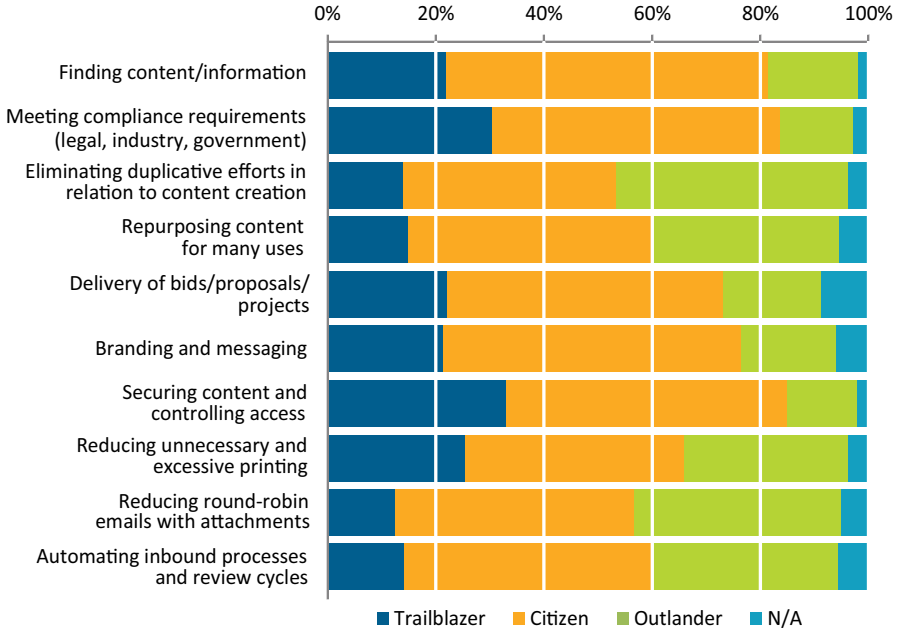
- *<u>First</u>, GDPR states the need for a DPO, so one of the first things you can do is hire or identify the qualifications and assign a DPO to your staff. (Guidelines can be found in the GDPR.)*
- *<u>Second</u>, read the GDPR to better understand its requirements. It's best that this be done by and with corporate legal counsel.*
- *<u>Third</u>, formulate a framework based on the GDPR guidelines and use this to develop your policies and processes. Then educate your employees on the new procedures and how to follow them.*

The Impact of the Cloud

Storing data in the cloud plays a role in every organization today, whether you realize it or not and whether it is sanctioned or not. As an Information Professional and business leader, your IG program must address use of the cloud as a data repository and as a collaboration tool for sharing information between individuals. It is important to identify who is responsible for maintaining your corporate data stored in the cloud, how it is organized and the approved processes and technology for migrating data.

One of the biggest challenges with cloud implementations is that cloud storage duplicates on-premise systems, which of course are duplications of network drives. This can result in a massive amount of Redundant, Outdated, and Trivial (ROT) content stored in silos across the enterprise. AIIM research finds that forty-three percent of respondents see themselves as Outlanders – having below average capabilities or typically waiting until the last minute to eliminate content duplication, indicating there is a lot of redundancy in their organizations[2] (Figure 2).

Figure 2: How would you describe your organization's experience in relation to the following business issues?



Include the cloud as part of your overall IG framework and plan. Even if cloud storage is not authorized, there is a strong likelihood, it is being done, and so it is in your best interest to build it into your IG plan with guidelines on appropriate use and a proper migration strategy. Things to consider include:

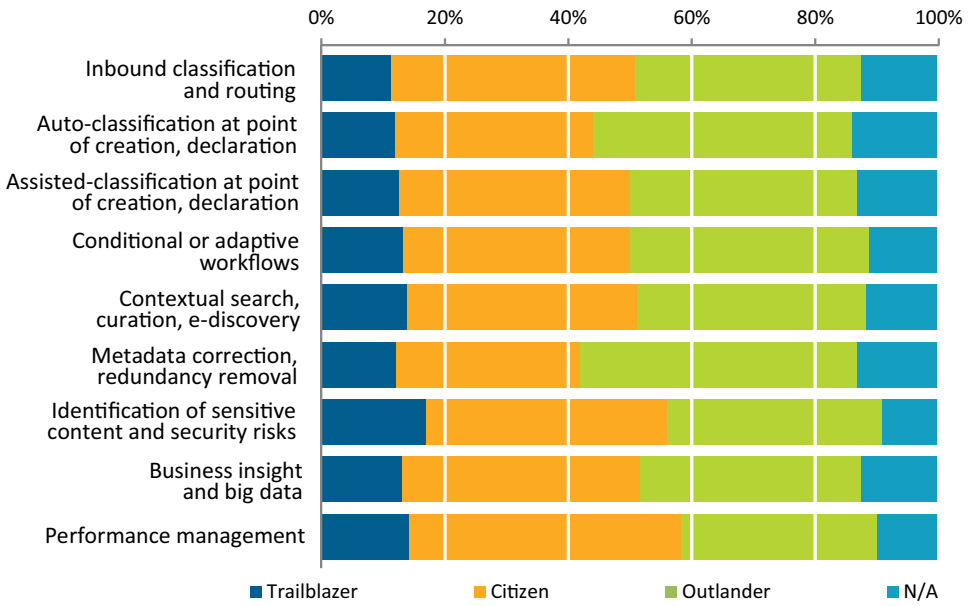
- ***First**, take inventory of your information assets. Especially with any PII, identify who is responsible for it, how it is being used, and how it is being shared.*
- ***Second**, select a cloud solution that will provide the right security and access controls and train your user base on how to use it properly.*
- ***Third**, formulate and implement a migration strategy and timeline to eliminate ROT. Monitor the migration activity to ensure that the strategy is being implemented efficiently and cost effectively.*

Managing Data Remediation

When your organization is audited and/or served a subpoena, are your data remediation program and related activities going to help or hinder the outcome? Are you consistently cleaning up ROT data? Effectively managing data remediation should be at the heart of your IG program. As an Information Professional, how are you positively influencing user behavior and helping to contain the proliferation of data? Employees are using shared and personal hard drives as well as other devices for data storage, making it more and more difficult to manage the massive amount of information being created and stored. Under these conditions, there is no ROT elimination, no consistency in storage syntax and naming conventions, and no data cleansing.

The negative impact of this scenario as it relates to audits and litigation support can be staggering. This includes the possibility of fines. In some countries the result of non-compliance is prison. There must be controls in place in order to know what data should be kept or disposed. Using analytics can help you identify what data you have, who owns it, and how to manage it properly. AIIM research finds that when we asked our respondents to position their organizations in relation to analytics use, seventeen percent see themselves as Trailblazers – as having exceptional capabilities and ahead of the pack in their respective market space or among peer groups - in using analytics to identify sensitive content and security risks. When we look at analytics to correct metadata and eliminate redundancy, twelve percent see themselves as Trailblazers or ahead of their peers in this area.[2] (Figure 3)

Figure 3. How would you describe your organization's use of analytics for the following?



When addressing data remediation, consider the use of analytics to help identify what you have in your existing repositories, classify that information properly, and filter and dispose of ROT. As part of your IG program, use analytics to provide consistent and defensible practices across the enterprise for both your stored and in-bound information.

Things to consider include:

- ***First**, implement a communication strategy to leverage captured and analyzed information across multiple departments and for multiple purposes. Embrace the mindset of "repurpose versus recreate."*
- ***Second**, capture information as early in the process and as close to the first touch point as possible. This information could be captured through mobile devices, as data through an electronic form, and even from an image scanned at a remote field office.*
- ***Third**, ensure that technologies including OCR, data capture, analytics and auto-classification are integrated with core enterprise systems that include ERP, CRM, and content management systems.*

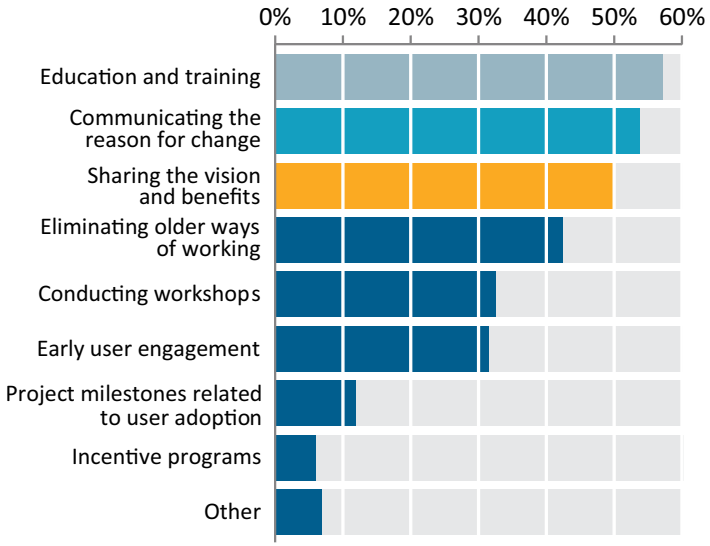
Threat Awareness

Just watch or read the news today and you will learn how important it is to be aware of the top threats to your data and do something about them. Hackers continue to be successful infiltrating systems in many ways, especially via email. As an Information Professional, you may be tasked with formulating plans to address these threats. While technology can be used to help manage these risks, one of the best defensive moves is to educate employees about the forms they take, how they spread, and how to safely and appropriately use various social media platforms for content sharing.

When employees download files from LinkedIn, Facebook, YouTube and others, they risk the possibility of downloading malware and other viruses. It is imperative that they keep their anti-virus/malware protection software up-to-date. IG policies should stipulate the need to monitor how these platforms are used and educate department heads on what the company considers to be best practices. From an IG perspective, this is change management in the form of altering risky practices and advancing the company's culture in relation to information sharing.

Change is one of the biggest challenges for most businesses. One of the best ways to address it is through education and awareness. AIIM research finds that fifty-seven percent of our respondents are focusing on education and training while fifty-four percent emphasize communicating their reasons for change. Fifty percent say they are sharing the vision and benefits of change[3] (Figure 4). The reality is that all of the strategies highlighted in Figure 4 should be part of a larger change management project that aligns employees with the company's IG program.

Figure 4: What change management steps is your organization taking to move the organization's process automation projects forward?



Change is not easy for many, yet often it is not malice but inertia that makes people so resistant to change. The key to successfully implementing change lays in the way we, as business leaders, approach the individuals facing change. Things to consider in relation to managing change include:

- ***First**, a communication strategy focused on GDPR, ECM and your IG framework as they relate to threat awareness*
- ***Second**, demonstrate using examples of how malware, and other threats could impact the corporate information ecosystem. For example, opening what appears to be a simple email attachment, or installing a Flash program from a game site rather than through a trusted source, opens your PC, phone, or tablet, to a threat that, when connected to your corporate network, could allow that threat to spread internally.*
- ***Third**, provide contact information and online resources like FAQs for guidance. This gives employees a place to turn to when questions surface about official policies. It also reminds them through login screen banners, and other regular communications methods that when in doubt, it is best not to open an attachment, or download an app or update until they have checked to ensure it is safe. Add a personal touch, that not only is corporate information at risk, so is their personal data when their phone is involved.*

Metadata & Managing Retention

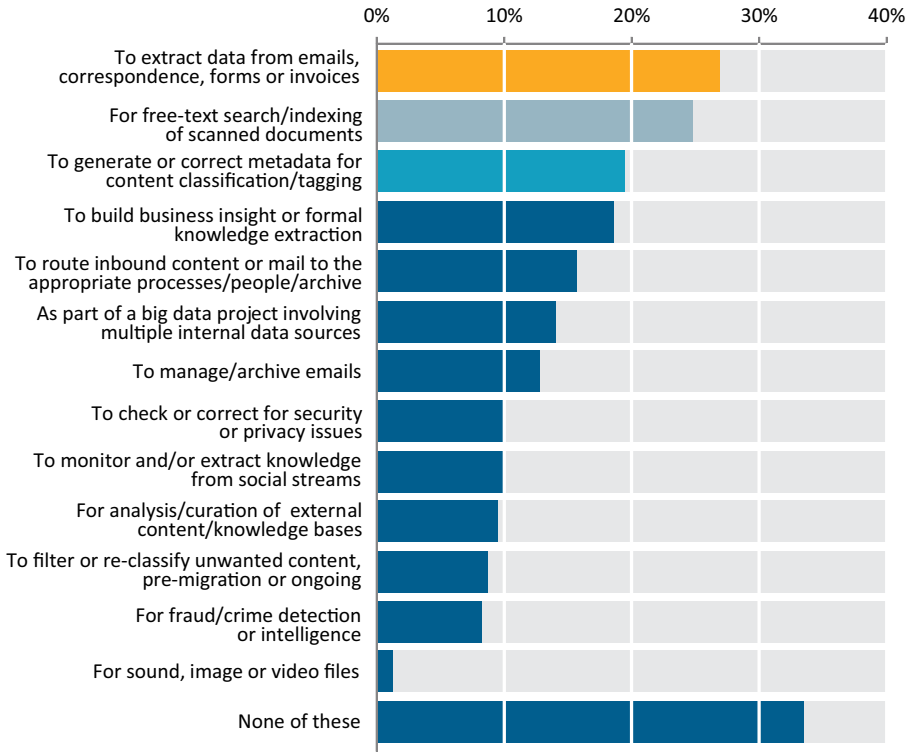
Audits, litigation and discovery demands are increasingly and unavoidably on the horizon for most large companies. Knowing how to leverage metadata in your information taxonomies can make a significant difference in your ability to provide the demanded information quickly and accurately. This is also true in how you address data retention and data retention lapses, which can be costly. Imagine for a moment that you are brought into litigation and required to produce all of the information related to a pending case. Note that I did not say "records" but rather "information," and as part of this information metadata is included. How will you provide this?

First, how will you find all of the relevant information across your enterprise, and how will you extract the metadata in order to review, cull and eventually provide relevant documents to the opposing party? This challenging task can span emails, text messages, correspondence hidden within content that was scanned and more. Second, if information has been disposed of, how will you ensure defensibility in accordance with your IG policies, assuming you have such policies relating to your information and not just your records?

As an Information Professional, it is important that you ensure internal personnel and even your retained law firm are diligent in disposing digital and electronic records on behalf of you and your clients. They should be trained on your IG policies, practices, and methods to ensure compliance with the proper disposal of documents, metadata, and electronic records. Your IG framework should include regular practices to cleanse, update, and refine metadata wherever possible, especially for unstructured content like emails and correspondence.

AIIM research finds that metadata correction and classification are in use by 19% while 25% are using analytics for free text search of scanned documents, signaling the need for improved findability combined with more robust and in-depth search capabilities[4] (Figure 5).

Figure 5: Are you currently using content analytics on unstructured content in any of the following ways?



Metadata is often overlooked by many organizations yet it is one of the most critical elements in effectively managing information and making it readily available. It is a vital tool in securing, retaining and disposing our information as well as defending our management practices when required to do so. A few things to consider include:

- ***First**, develop a strategy to leverage captured and analyzed information across multiple departments and for multiple purposes*
- ***Second**, establish a continuous improvement program that will periodically review and refine your metadata*
- ***Third**, make metadata refinement an on-going process improvement practice that looks for ways to improve upon the foundation you have set and not just a one-time occasional project*

Conclusion & Recommendations

As the business leader or information professional in your company, it is your responsibility to ensure that corporate information governance policies, procedures, tools, and training are in kept up to date in support of meeting compliance requirements and minimizing corporate risk. You must be ready to overcome any IG related obstacle, and tackle it head-on. This means keeping up-to-date on the latest regulatory changes like GDPR and understanding the requirements and impact it has on your company. It means adjusting your policies, procedures and employee training to ensure they support compliance and aligning technology use to support those policies, procedures and employees.

Use cloud technology to enhance collaboration and accessibility but include it in your IG program and do not just turn it loose. Assign responsibility at the departmental level for oversight on how information is stored in the cloud, how it is organized, and migration of information from network drives and PCs to the corporate cloud application. Provide training across the enterprise on proper migration and disposition practices to ensure compliance is maintained and ROT is eliminated.

Change employee behavior and perceptions related to data remediation and instill a mindset that to keep all things for all time is not a best practice and in fact places the company at risk. Teach employees to *identify* and *classify* information properly. Give them the tools to help them filter and dispose of ROT properly. As part of your IG program, incorporate analytics technologies to provide automated practices across the enterprise for both your stored and in-bound information.

Heighten employee awareness around threat potential, in particular when using unauthorized applications that are downloaded to smartphones and tablets, or social sites that can and do bring malware with them. Your IG policies must stipulate appropriate use and approved technologies. As an organization, you should actively monitor how these platforms are used and take corrective actions when required. Work with IT to implement preemptive measures by installing malware detection, virus detection and software capable of wiping out infected devices remotely.

Finally, refocus attention on metadata. Metadata serves many purposes from increased findability, to applying security and accessibility controls, to managing retention. Your IG policies must address metadata on multiple levels from capturing metadata, to the types of metadata required, to the metadata lifecycle. As part of your continuous metadata process, your company should cleanse, update, and refine metadata wherever possible, especially for unstructured content like emails and correspondence.

The key to all of this is that the responsibility does not rest with one person or group. It rests with the entire company and with every employee. The IG framework must be designed to address compliance requirements, establish corporate standards, align with the information ecosystem, and still be flexible enough to change as requirements demand. The five obstacles presented here are a great beginning but are by no means the end. Here are five recommendations to help you begin your IG journey.

Recommendations

- *Incorporate the technologies like cloud, analytics, classification, and optical character recognition to extend your capabilities and overcome your information governance obstacles and limitations in identifying vital business information that needs protection.*
- *Secure PII and all information of a sensitive nature from unauthorized access, loss, or exposure while at rest in a repository or while in transit whether on-premise, in cloud applications, or on mobile devices.*
- *Automate the capture, identification, classification, and processing of information at first touch point to ensure it is brought under corporate control quickly, efficiently, and consistently.*
- *Include people, process, and technology as part of your information governance strategy to ensure a holistic approach is taken across the enterprise.*
- *Use external resources to assist with the development and implementation of your IG program, including professional associations, subject matter experts, and solutions providers who can share the best practices they have witnessed with other companies like yours.*

References

[1] Understanding GDPR in 2017

[2] 2017 State of Information Management: Are Businesses Digitally Transforming or Stuck in Neutral?

[3] Business Process Automation in 2017: Designing an Intelligent Workplace

[4] Business Process Automation in 2017: Designing an Intelligent Workplace

UNDERWRITTEN IN PARTNERSHIP WITH

About Canon

Canon
CANON BUSINESS PROCESS SERVICES, INC.

Canon Business Process Services, a wholly owned subsidiary of Canon U.S.A., offers information governance services that address the controls and metrics necessary to capitalize on valuable information and to establish governance across the enterprise. We are a leading provider of information management, eDiscovery, business process outsourcing and specialty workforce services.

Our mission is to help clients improve operational performance while reducing cost and risk. Canon Business Process Services has been named a Global Outsourcing 100 Leader by IAOP for the past eleven years and recognized in the Gartner Magic Quadrant for Managed Print and Content Services for five consecutive years. We have also been acknowledged by CIOReview magazine as a "20 Most Promising Legal Technology Solution Provider."

Learn more at cbps.canon.com and follow us on Twitter @CanonBPO.

cbps.canon.com

About AIIM

aiim

AIIM (www.aiim.org) 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.

Founded in 1943, 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, with programs and content for practitioners, technology suppliers, integrators and consultants.

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

AIIM Europe
Office 1, Broomhall Business Centre,
Broomhall Lane, Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.org