Information Governance is Good Business

MARK BARRENECHEA

OpenText President and CEO

Contents

Introduction

OpenText Enterprise Information Management (EIM) White Paper Series is a set of publications from OpenText™ on the topic of Enterprise Information Management.

EIM is the discipline of discovering, managing, extracting value from, and building applications on top of unstructured enterprise information. At OpenText we know these Enterprise Information Management practices as the next generation of enterprise software.

To help present the topic of EIM, it will be described and detailed in the following white paper series:

- Enterprise Information Management (EIM)
- The Social Enterprise
- It's all Connected
- Focused on the Value
- The Journey
- Enterprise Content Management (ECM)
- Business Process Management (BPM)
- Customer Experience Management (CEM)
- Information Exchange
- Discovery
- Mobile and Cloud
- Security
- *Information Governance*
- Customer Case Studies

Information is a High Value Asset

It's no secret that the volume of information is growing significantly, continuing on an exponential growth path. For the enterprise, there is obvious growth of content within the firewall in email, file systems, corporate systems of all types, and even on paper. At the same time, there is also an explosion of high-value content outside the firewall, in wikis, blogs, social commentary, and customer interactions.

In some areas, issues of access to information are impairing the business. Systems that rely on paper are a prime example and still exist in many organizations. When information is dispersed and copied across many environments, it becomes increasingly challenging to collaborate on this information, difficult to ensure access to the latest version of content, and impractical to automate processes.

There is value in understanding data and turning content into meaningful enterprise information that can be used to optimize the business. When information is brought together in standard processes, analyzed, categorized and understood, that information can drive significant insight and competitive advantage.

Consider the case of an international firm bidding on a large capital project. Creating a response to the tender can be recreated from scratch or reused from previous projects. If information from similar projects is understood and can be easily reviewed and assembled, then the response to the tender demonstrates the experience held by the organization and offers a significantly higher chance of success.

As more is written about Big Data and competitive advantages in understanding and utilizing enterprise information more effectively, corporate executives outside of IT are focusing on information and process. They are recognizing the value of corporate information both inside and outside the firewall. In forward-thinking organizations critical business information is now recognized as a corporate asset that needs to be protected, and cost effectively managed and leveraged for maximum value to the organization.

Information Governance

There are many definitions of Information Governance, but at the heart it is about effectively using and managing an organization's information assets to derive maximum value, while minimizing information-related risks. It applies to all corporate information, regardless of form, function, or location. This includes structured and unstructured information, and ranges from content on file systems and email to information within productivity and line-of-business systems, on web, social, and mobile environments.

Information Governance is labeled in different ways; for example, it's sometimes referred to as GRC (Governance, Risk, and Compliance). It's often discussed in conjunction with archiving, retention, preservation, and disposition of business information. While it does incorporate these elements (as well as aspects of Records Management), it goes well beyond them to encompass all policies and methods of managing information throughout its lifecycle from creation or capture and classification, through management to long term archival or deletion. It involves policy, process, and technology aspects of information stewardship.

Governance is about leveraging information to conduct business. As such, a critical part of information governance is ensuring that the right information is presented to the right people at the right time. It follows that governance starts with understanding the organization's information needs. Governance is based on answering the following questions:

- Why is the information needed?
- Who can (and should) use information?
- How can they use the information?
- When can they use the information?
- Where can they use the information?
- What can they do with the information?

Information Governance aims to balance value with the risks and costs associated with corporate information. Often driven by the legal or compliance executives in an organization, the aspects of legal risk, compliance to regulations, and electronic investigation are paramount. The Records Information Management (RIM) groups are normally key stakeholders in the governance process as they define and implement management of critical corporate records. Elements of security, efficiency, and cost are key factors for the technology groups. All of this must come together with key business objectives, such as increased competitiveness, agility, and profitability.

Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management
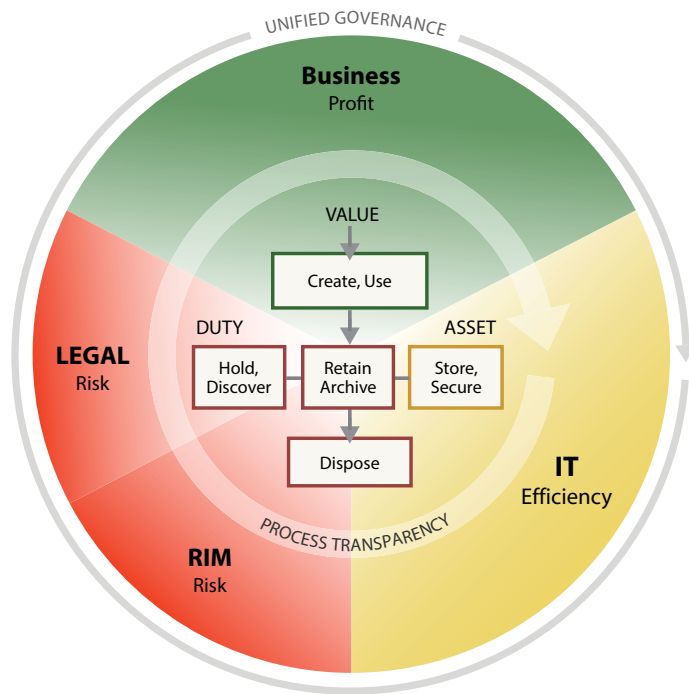
Duty: Legal Obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

FIGURE 1:

Information Governance Reference Model (IGRM)

Source: Information Governance Reference Model, 2012 – edrm.net

Corporate Impetus

While there are several reasons for organizations to consider Information Governance, regulatory compliance is the most significant business driver.

"Regulatory compliance is the No. 1 driver for data management in the eyes of business leaders – 70% of data management professionals in the Q1 2013 Data Governance Online Survey consider it a critical or high priority. However, data management organizations that keep pace with the business see another benefit to their actions: business innovation.[i]"
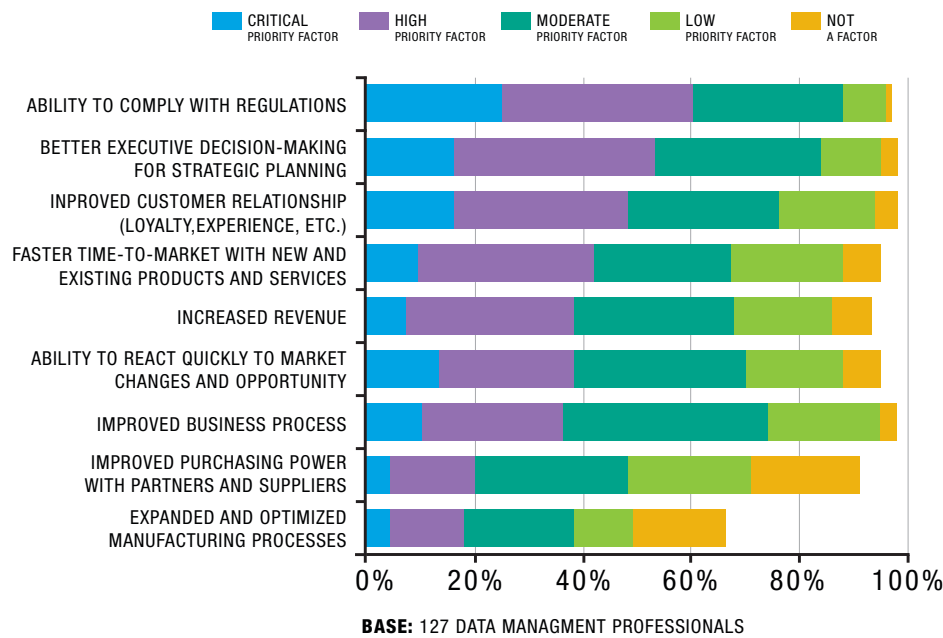
FIGURE 2:

Compliance is Key Driver for Information Governance

Source: Forrester Research, Inc: Data Governance Equals Business Opportunity. No, Really by Michele Goetz, Henry Peyret, and Alan Weintraub May 20, 2013

CRITICAL PRIORITY FACTOR   **HIGH** PRIORITY FACTOR   **MODERATE** PRIORITY FACTOR   **LOW** PRIORITY FACTOR   **NOT** A FACTOR

ABILITY TO COMPLY WITH REGULATIONS

BETTER EXECUTIVE DECISION-MAKING FOR STRATEGIC PLANNING

INPROVED CUSTOMER RELATIONSHIP (LOYALTY,EXPERIENCE, ETC.)

FASTER TIME-TO-MARKET WITH NEW AND EXISTING PRODUCTS AND SERVICES

INCREASED REVENUE

ABILITY TO REACT QUICKLY TO MARKET CHANGES AND OPPORTUNITY

IMPROVED BUSINESS PROCESS

IMPROVED PURCHASING POWER WITH PARTNERS AND SUPPLIERS

EXPANDED AND OPTIMIZED MANUFACTURING PROCESSES

0%   20%   40%   60%   80%   100%

BASE: 127 DATA MANAGMENT PROFESSIONALS

Regulatory Compliance

There are an increasing number of complex regulatory and legislative mandates driving the way organizations manage their business content. Examples of these include:

- Protection and preservation of content. In some industries information must be kept (archived) for 50 or 100 years.

- Defensible deletion of content such as personnel data related to an incident within defined timelines.

- Specific regions have Records Management regulations, often based on very lengthy and complex implementation and feature requirements specifications.

- Privacy regulations exist in most regions with increased oversight of types of information stored by organizations, what is shared, and where information is stored. The proliferation of cloud implementations is causing scrutiny and extensions of this type of regulation inclusive of Data Sovereignty legislation that requires organizations to ensure information is kept within specific geographical regions.

Failure to meet these types of regulations can result in significant financial penalty, legal liability, and loss of reputation.

Security

As one of the top concerns for CIOs, the need to ensure security drives action. Typically when we think of security, we think mostly of external or internal threats, which involve an explicit or inadvertent action taken to compromise the integrity of an organization's information. In the context of information, we need to flip this perspective and consider the information itself to be the object which may catalyze a security event.

When information needs to be retained for litigation or compliance purposes, it's imperative to ensure that the information remains intact, pristine and not only defensible, but discoverable and unmodified. Information that is not in this condition with the requisite controls and discovery mechanisms becomes a threat to the organization. It could be the defense of a lawsuit or audit, or the data needed for submission to bring a new drug to market; in either case – losing or compromising the information represents a financial and/or competitive risk to the enterprise.

The value of information must also be considered in the context of security. Protection of corporate intellectual property (IP) is an increasing concern for IT organizations as confidential information, plans, and corporate competitive advantage is housed in electronic format. Threats from both inside and outside the company must be considered as information is protected throughout its lifecycle. No organization wants to find itself exposed through WikiLeaks or other breaches of security causing loss of IP.

Another security-related consideration is the need to ensure disaster recovery. While it is a regular function of IT organizations to consider backup and recovery in all situations, this type of project will also cause examination of the importance of key information and systems, and the need to ensure that critical Information is protected from risk of loss.

Organizational Effectiveness

Increasingly strategic CIOs and business leaders look to Information Governance to drive improvements in many areas of organizational effectiveness. Consolidated, categorized, and analyzed information is used to drive a deeper understanding of success factors, business trends, and better strategic decision making. Well-governed information, together with consistent processes, drives greater process velocity and allows organizations to bring products and services to market faster and more effectively than their competition. The more information is brought together for analysis and decision making, the greater the opportunities for the organization to strategize and innovate.

Information Governance has moved into a top priority category for line-of-business executives as they recognize the opportunities it provides for their business to excel. They join the ranks of their IT and compliance counterparts in recognizing the value of effectively managing their enterprise information.

Compelling Events

While Information Governance inhabits the minds of innovative CIOs and many business leaders, and is something they seek to accomplish under ideal circumstances, it's often a compelling event that impacts the business that drives these stakeholders to take action. Organizations that have faced a major lawsuit or experienced the eDiscovery process with disparate systems often struggle to identify critical information within their systems, uncovering masses of duplicate and sometimes irrelevant data. Sorting through enterprise information for relevant business records can lead to excessive spending on legal reviews, and in many cases, the organization will face fines related to their inability to defensibly show they have produced all information within a timely manner. The same can be true of an electronic investigation related to a regulatory audit. When an organization has faced one of these situations, the cost and business disruption factors often drive action on Information Governance initiatives.

When an organization within their industry or a related industry is subject to litigation, public scrutiny through audit, or a security breach, organizations will evaluate the cost and risk factors involved. As they observe (and often benefit from) the cost to their competitors, organizations typically begin implementing processes and systems for Information Governance.

Holistic is Better than Tactical

As illustrated in the figure below, the key goals of Information Governance programs within organizations include savings on storage and infrastructure, unimpeded knowledge sharing, and the ability to respond quickly to investigations of all types. Consider how hard it would be to realize these gains if the systems implemented for Information Governance span only one or a handful of departments and projects.
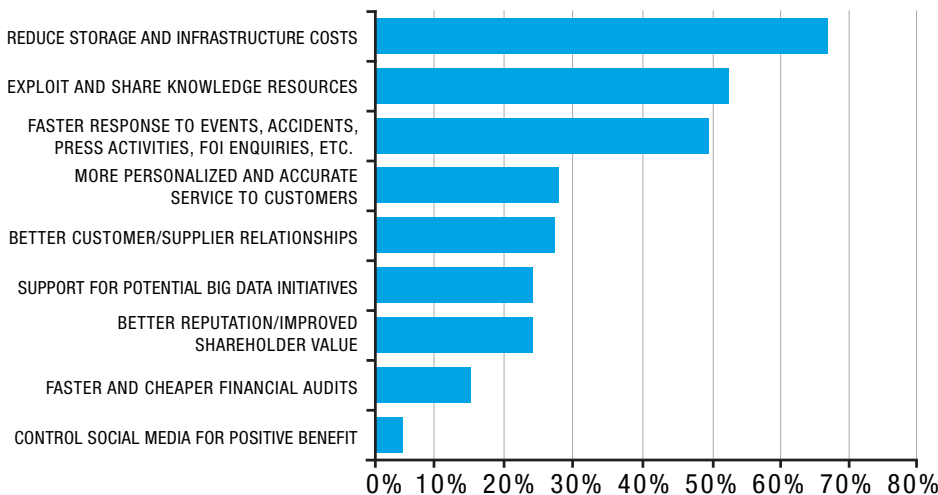

FIGURE 3:

Benefits of Good Information Governance

Source: AIIM Industry Watch: Information Governance – records, risks and retention in the litigation age. Doug Miles, 2013.

Storage and infrastructure costs are perhaps the easiest benefits to achieve with any system implementation, even one that does not span the full organization. A solution could be put in place for one department and storage savings realized. More significant savings can be realized, however, when the system is broadly implemented.

A large amount of content is duplicated across any given organization. A single document may be stored on the file system, sent to several people in emails, stored in a document management system, and published on the web.

If Information Governance is put in place across the enterprise, utilizing technology to archive and manage content across all environments, gains can be realized across enterprise systems. Archiving technology ensures that content is stored only once and access provided to it from within systems and environments. The storage and infrastructure savings are multiplied with each content source that is brought under governance.

When corporate information sources are consolidated through central governance, there is a level of consistency that is not possible with disparate systems. Policy can be consistently set and enforced across all the content sources under governance. If information is managed across many systems, there are several approaches to how it is managed, searched, kept or deleted. When an electronic investigation (audit or legal review) is initiated, many systems will have to be examined, information identified, and the policy dictated around that information well understood and documented. If policy is maintained centrally, then one central source of policy will need to be understood, documented, and defended. All information sources governed by that central policy can be searched once and information returned. This approach results in significantly less cost and time invested, in lieu of examining each and every different system of record for corporate information.

Does central policy imply that all information needs to be physically stored in one system? With robust Information Governance technology there is flexibility to maintain policy in one central location and manage the content either centrally or in the source system. Many organizations choose to put most of their managed content into an Enterprise Content Management (ECM) system, physically storing content to realize benefits such as infrastructure and user experience consolidation. However, some types of content may be left within their native system with policy managed centrally through ECM. Examples of this may include content within the file system, Microsoft® SharePoint®, or line-of-business systems in use within the organization.

Information Governance policy must be defensible in order to pass audit and legal review. This includes all parts of the policy from creation to management to disposition. When organizations have disparate systems and no overall governance, content deletion becomes very difficult and is seldom carried out effectively. Before content can be deleted it must be well understood and the corporate value of it assessed. A high percentage of organizations are not able to do this because they do not have complete governance in place. They are faced with either keeping everything (the most common approach) or deleting content without being clear about the consequences.

Keeping everything goes directly against a key reason (and benefit) for implementing Information Governance—reducing storage and infrastructure costs. Moreover, this approach dramatically increases the cost of electronic investigation as content must be searched, examined, and reviewed from all of the sources where it is stored. With the dramatically increasing volume of content, this approach becomes less and less tenable. The route to avoiding this is defensible deletion. This can be done when content is brought under governance, understood, classified, and then managed consistently.

Organizations that plan for Information Governance across the full enterprise realize stronger gains. They bring projects together and plan holistically, even though implementation may occur in phases. Some progressive organizations plan for Information Governance within the requirements for each project. This ensures business and IT alignment and Information Governance growth with each corporate initiative.

It Doesn't Have to be Hard

While it's clear that there is good reason to focus on Information Governance, many organizations do not believe they have reached a significant level of data maturity to date. "In fact, only 15 percent rate the data governance maturity as high or very high – defined as incorporating both business and IT, with top-level support and spanning major parts of the organization.[ii]"

Why is that? Well, it's because Information Governance isn't easy. It takes time and broad consideration.

Organizations have information stored in silos – fragmented across the enterprise in disparate line-of-business systems, email systems, productivity tools, and enterprise resource planning (ERP) systems, inside and outside the firewall. As companies acquire and merge, more systems and management methods are brought into the organization.

Interoperability of systems across many vendors is complex. Ask any IT group and they'll tell you that APIs for connecting systems vary considerably, information and metadata are categorized differently across systems, and search and process automation are difficult across different systems. All of this makes Information Governance more challenging.
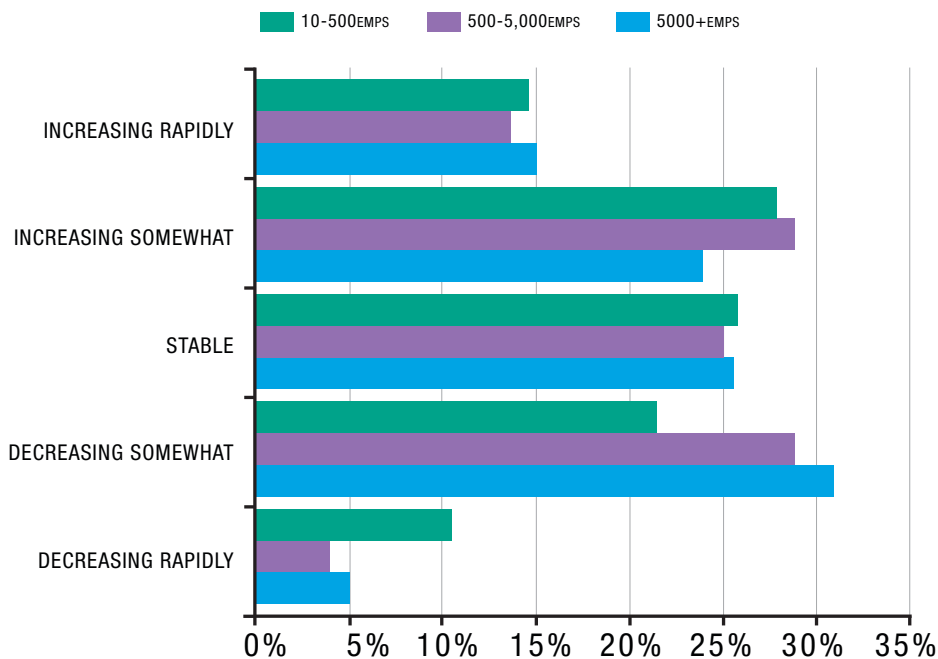

FIGURE 4:

Volume of Paper Records in Organizations Surveyed

Source: AIIM Industry Watch – Information Governance, March 2013

Progress toward the "Paperless Office" is slow. In a recent study, for 42 percent of organizations surveyed, the volume of paper records is still increasing[iii]. Paper continues to be a factor in most organizations. While paper is one of the most mature content types and many organizations do have retention and disposition policies around paper, they don't always have the same policies applied across paper and electronic content. Information on paper is largely isolated from efficient electronic processes, is poorly collaborated on, and causes bottlenecks when collaboration does occur.

Mobile and Application Flexibility

Computing choices are increasingly driven by users who are mobile, and so is the information they work with. People interact with information using corporate devices that may or may not be chained to a desk; they also interact with information using devices that have been self-provisioned. This puts corporate information outside IT management boundaries. The same is true for applications. People work where and how they want to. Many use consumer applications to create and collaborate on their content. This puts information outside the corporate firewall, and more importantly, outside of Information Governance policies. Examples of this include file-sharing services which put content at risk of security and ownership breach.

Using mobile technology that provides consumer-like abilities but is built on an ECM system is the desired path because it allows users to work with content on applications of their choice within a governed and safe environment. Information can be shared outside the firewall and the enterprise without risking ownership or security breaches. Device governance is provided such that content can be stored and utilized on mobile devices and if the device is lost, the content can be removed remotely.

Lack of Business Buy-in

When there is a goal of Information Governance across an organization, it's often applied inconsistently as systems and practices vary by department and region. Some groups may involve the compliance group as they plan for governance, others may plan it themselves, and still others do not consider governance as they bring in systems. The commitment of line-of-business leaders varies as well, either because they are not clearly aware of the issues or because they do not recognize the benefits. Gaining commitment from legal/compliance, IT, and line-of-business executives is key and must be incorporated into Information Governance planning from the outset.

User Adoption

Some organizations have implemented governance programs and not been successful. This may be because they have not achieved strong enough user acceptance of the systems. Governance should be built into systems and processes and presented as a manual task for end users. There are several ways to achieve this, including the classification of content through process or project or by mechanisms such as auto-classification. Classification methods can be built into the environment where the user works, whether that is within their office applications, email system, Microsoft SharePoint, ERP system, web, desktop, or mobile devices, without being obtrusive to the user. The key is bringing the governance technology to the user's environment of choice and making it easy, enabling them to spend their time doing their daily activities instead of finding ways to get around using the system. This is one of the key elements to look for with any Information Governance technology: optimal user experiences within the applications where users work.

Do Costs Outweigh Consequences?

When it comes to mitigating risks, one of the most important questions to ask is "What's the cost of doing nothing?" No real risk can be mitigated to a zero percent likelihood of occurring and some risks are 100 percent likely to happen. So how should an organization go about determining which risks to mitigate against and which consequences to prepare for? A key consideration is to understand the risk profile. A risk profile takes an objective look at the likelihood of identified risks to occur and their impact when they do occur.

If the organization is a litigation target, it makes very little sense to try and prevent court action (out-of-court settlements notwithstanding). Defensible deletion is a better tactic as it leads to reductions in discovery costs and legal fees. An added benefit of a defensible deletion program is that it makes organizations "info-efficient" by reducing the amount of outdated and irrelevant information that users have to sift through to get work done.

If the enterprise stores Personally Identifiable Information (PII) about stakeholders (for example, those in insurance, banking, healthcare industries) the likelihood that someone will try to compromise that information is quite high and the impact if they succeed is considerable. Spending time and money on mitigating against unauthorized disclosure is prudent. Not only does this protect against fraud and identity theft, it also protects brand reputation.

When crafting a risk profile, it's important to look at the organization as a whole, and to look at the different types of information individually. Not all information is created equally, and consequently does not expose an organization to the same risk if lost or disclosed without authorization. Identifying information that is critical to continued business operations allows organizations to craft policies that result in expending resources where it provides the biggest benefit. Identifying information that, if lost or disclosed, would cause nothing more than a minor nuisance prevents organizations from expending resources where there is little appreciable gain. In other words, there's no point in buying flood insurance if your house is on a desert mountaintop.

Successful Information Governance

What does success look like? The full lifecycle of content is managed over and above merely ensuring security and privacy. Policy is consistently applied across disparate systems and content types. Governance is built into processes and strategic information sources. In the successful implementation, Information Governance is managed by more than the IT and compliance groups. It becomes part of an expansive vision, as business leaders are actively involved and engaged in the process, building Information Governance into key projects. Line-of-business leaders recognize corporate information as a valuable asset and manage it accordingly.

Technology Options

Information Governance is built into most OpenText software in a variety of ways. There are some key areas that organizations should consider as they look to invest in a system for Information Governance.

Enterprise Content Management (ECM) is the core system that provides the foundation for Information Governance. The main components required for Information Governance are built into ECM and are bundled as Content Lifecycle Management (CLM). Key components in the CLM bundle include:

Document/Content Management – providing a variety of user experiences where content can be created, consumed, shared, and collaborated on. A number of governance abilities are built into document management including security, audit metadata management, collaboration, and process management. Organizations use content management to ensure there is a "single source of truth", the most recent version of any piece of information, and all the interactions with that content inclusive of the processes that operate on it.

Records Management is a critical piece of the Information Governance story. It provides the classification of content and drives the retention and disposition lifecycle of the content based on the classification. This is a particular area of strength in OpenText ECM as we continue to be market leaders by offering an ECM System with records management capabilities that help our valued customers meet their compliance regulation requirements around the globe, including ISO 15489, MoReq, VERS, DoD 5015.02, 21 CFR Part 11, Sarbanes-Oxley, and many more. Risk reduction and high security are also enhanced by Records Management as it helps provide security clearance beyond basic user rights, ensure data sovereignty rules are respected, and ensure defensible disposition of content.

Optional additions to Records Management include **Auto-Classification** which uses content analytics to review and understand content, and apply records management classifications to it. Transparent classification driven and audited by records managers leads Auto-Classification to become a high-value addition to Information Governance as it removes the burden from end users in classifying content.

Imaging is a method used to bring paper content into processes and let it participate in more comprehensive Information Governance. While physical records can be managed within the system, this alone does not encourage full process optimization and therefore does not realize all of the productivity gains possible with Information Governance. With imaging, documents can be captured, archived, and linked to all types of business objects within enterprise applications, bringing content into the context of Information Governance policies.

An optional addition to Imaging is **Capture Center** which provides Optical Character Recognition (OCR). OCR allows images to be translated into text as they are imaged into the system, metadata captured, and content classified as it is read into the ECM system.

Archiving provides secure, cost-effective, and multi-faceted storage for all enterprise information in a scalable repository built for high volumes of data at different stages of the content lifecycle. Leveraging a single, tiered repository to store and access critical information, archiving can ensure quicker response times to eDiscovery and proof-of-compliance requests, as well as minimized storage costs with compression, smart disposal, auto-classification, and de-duplication capabilities.

Optional additions to ECM include the many integrations available with other systems in the organization. This includes the offerings which combine ERP systems, processes, and content together with ECM. It also includes integrations with Email systems, File Systems, CAD and Engineering systems, and more. OpenText ECM excels at bringing Information Governance transparently to users wherever they work. Whether on premise, in the cloud, or on the desktop or mobile device, these integrations behave as the native environment does, easing the learning curve and maximizing user adoption.

OpenText InfoFusion is an Information Access Platform that provides the ability to connect with line-of-business and ECM systems to discover, analyze, and act on unstructured information. For organizations looking to bring systems together in a common view, search for information across these systems, and provide Information Governance across these content sources, InfoFusion provides an enterprise-class platform solution.

These are just a few of the offerings designed to deliver sound governance, manage risk, and enable compliance. When combined, they form a strong foundation for holistic Information Governance across the enterprise.

More than Technology

Not all information-related issues can be dealt with by applying technology. OpenText offerings exist to help organizations reduce discovery costs, and classify, secure, present, and dispose of information. However, if these systems are implemented incorrectly (if, for example, they are based on poor policies or provided to uneducated users), the effort and cost expended on implementing the tools have likely been wasted.

Prior to procuring and deploying technology, it's critical that an enterprise understand its compliance and governance obligations, as well as its risk profile. Once an organization has this understanding, it can bring together relevant stakeholders to craft appropriate policies and procedures. Technology supports effective governance policies and procedures; it does not replace them.

Key members of the legal and compliance groups, IT, and line-of-business leaders should come together to plan and implement an Information Governance program. Many organizations form an Information Governance committee that makes key decisions on the program. Key to success is carefully choosing the members of the committee to ensure commitment and decision-making power.

When there is an overall plan in place, ensure it keeps pace with the business, with information assets being considered in project prioritization and governance planned into project requirements.

Technology implementations are well understood by most IT and business groups. The user acceptance goal is paramount in these projects and should be taken into account during planning. Key user groups should be involved during the requirements, planning, testing, and early implementation to maximize adoption. Training is also a key component as these systems roll out and one that is often overlooked. Even when systems are very intuitive, a little training around policy, governance, and the systems can go a long way to increasing adoption and compliance to policy.

Balance Matters

Information Governance is about getting information to where it needs to be, faster and safer, so that maximum value can be achieved from this information with minimal risk.

Information Governance is not just about complying with regulations and minimizing risk, however, it's about maximizing the value of the information to create a good, profitable business. It applies to all enterprise information an organization is custodian of, regardless of format, function, or location. Of course Information Governance helps to minimize legal liability, secure sensitive information, and reduce unnecessary expenses, but it's really about treating information as a strategic asset. Properly and holistically applied, Information Governance improves a business. Public sector organizations are better able to assess and satisfy the needs of their constituents. Commercial enterprises are better able to understand their environments and act accordingly to become more profitable.

Governance does not have to be perfect to be effective. It merely needs to be consistently applied and organizations need to demonstrate best effort or good faith. If organizations choose to ignore policy, they are likely to be sanctioned when investigated. Information Governance policies need to be practical so they can be implemented with adequate training and adherence monitored regularly.

It's in each enterprise's best interest to be protected from information- related risk and harm. Good Information Governance doesn't impede the enterprise's ability to do good business, it enhances it.

i   Forrester Research, Inc.: Data Governance Equals Business Opportunity. No, Really by Michele Goetz, Henry Peyret, and Alan Weintraub. May 20, 2013
ii   Ibid
iii AIIM Industry Watch: Information Governance- records, risks and retention in the litigation age by Doug Miles. March 2013

OPENTEXT™

OpenText Locations

AMERICAS

Canada:
- Waterloo, ON
- Richmond Hill, ON
- Ottawa, ON
- Montreal, PQ
- Peterborough, ON
- Kingston, ON
- Calgary, AB

US:
- Tinton Falls, NJ
- Austin, TX
- Tucson, AZ
- Norcross, GA
- Irvine, CA
- Tallahassee, FL
- Chicago, IL
- New York City, NY
- Rockville, MD
- Columbus, OH
- Burlington, MA
- Bellevue, WA
- Tampa, FL
- Reston, VA
- Arlington, VA
- Rochester, NY
- San Antonio, TX
- Alpharetta, GA
- Brentwood, TN
- Brook Park, OH
- Concord, CA
- Emeryville, CA
- Gaithersburg, MD
- Latham, NY
- Richardson (Dallas), TX
- San Francisco, CA

Brazil:
- Sao Paulo, BZ

EMEA

Germany:
- Munich (Grasbrunn), DE
- Konstanz, DE
- Oldenburg, DE
- Düsseldorf, DE
- Kempten, DE
- Hamburg, DE
- Bad Homburg, DE
- Huerth, DE

Great Britain:
- Reading, UK
- Wimbledon, UK
- London, UK
- St Albans, UK
- Malmesbury, UK
- Preston, UK
- Sunbury, UK

France:
- Paris, FR
- Cachan, FR

Sweden:
- Stockholm, SE
- Gothenburg, SE

Switzerland:
- Baden, CH

The Netherlands:
- Hoofddorp, NL
- Amstelveen, NL
- Putten, NL

Ireland:
- Clonakilty, IE

Spain:
- Madrid, SP

Austria:
- Klagenfurt, AT
- Vienna, AT

Czech Republic:
- Prague, CZ

Italy:
- Milan, IT
- Rome, IT

Finland:
- Espoo, FI

South Africa:
- Johannesburg, ZA

United Arab Emirates:
- Dubai, UAE

APJ

India:
- Hyderabad, IN
- Bangalore, IN

Australia:
- Sydney, AU
- Melbourne, AU
- Canberra, AU

Japan:
- Tokyo, JP
- Osaka, JP

Singapore:
- Singapore, SG

Hong Kong:
- Hong Kong, CN

Korea:
- Seoul, KR

New Zealand:
- Auckland, NZ

Phillipines:
- Manila, PH

OPENTEXT™

About OpenText

OpenText is leading the charge with a practical roadmap to help today's C-suites advance how they interact with employees, customers and the supply chain to be fully prepared for 2020. For over two decades, OpenText has been a core contributor to the most successful businesses in the world. Ninety percent of Fortune 500 companies today are using EIM to transform their enterprise into a digital enterprise.

OpenText provides Enterprise Information Management software that helps companies of all sizes and industries to manage, secure and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit: www.opentext.com.

Contact OpenText

Sales

North America: +1-800-499-6544
International: +800-4996-5440
E-mail: sales@opentext.com

Partners

North America: +1-519-888-7111
International: +44 (0) 1189 848 000
E-mail: partners@opentext.com

Media Relations

North America: +1-519-888-7111
International: +44 (0) 1189 848 000
E-mail: publicrelations@opentext.com

www.opentext.com