
Best Practices in Information Governance

Marydee Ojala 20 Information Governance Gets Respect

Ever get a song stuck in your head? Talking about information governance with experts in the field, I suddenly found myself reminded of Aretha Franklin's classic Respect. In the back of my mind, she was spelling out R E S P E C T in that incredibly strong voice of hers as background music to my thoughts about how attitudes toward information governance have changed...

Robert Cruz, 22 Best Practices in Information Governance Actiance, Inc.

Information Governance—as a discipline—has undergone a strange and wild ride over the past couple of years. Finally, we have moved past endless debates on definitions and usable frameworks, thanks to the efforts of the Information Governance Initiative (IGI) and other IG leaders and practitioners...

Ken Lownie, 24 The Real Differentiators in IG Solutions Evertteam Software

According to Gartner, Information Governance (IG) is: "The specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information."...

Susan Emery, Viewpointe. . . . 26 6 Ways to Keep Business Content from Getting Out of Control

Regulated industries such as financial services, healthcare or insurance require business to balance innovation and risk mitigation. Can you keep pace with digital transformation without risking security, privacy or retention policy requirements?...

Produced by:
KMWorld Magazine
Specialty Publishing Group

For information on participating in the next white paper in the "Best Practices" series, contact:

Kathryn Rogals
Publisher
561.483.5190
kathy_rogals@kmworld.com

KMWorld
KMWorld.com

Premium Sponsors:

actiance[®] **evertteam**

Information Governance Gets Respect

By Marydee Ojala, Conference Program Director, Information Today, Inc.

Ever get a song stuck in your head? Talking about information governance with experts in the field, I suddenly found myself reminded of Aretha Franklin's classic *Respect*. In the back of my mind, she was spelling out R E S P E C T in that incredibly strong voice of hers as background music to my thoughts about how attitudes toward information governance have changed. Just like Aretha requested, information governance is getting a lot more respect these days, both when it gets home and when it's at the office.

And why would that be? Information governance is hardly a new concept. Gaining control over internal information has long been an important activity. However, too frequently it had low priority and inadequate resources. Now that companies are realizing the value of protecting information, it is seen as a crucial part of business strategy. This is particularly true of regulated industries, such as finance, insurance, energy, and pharmaceuticals.

The Information Governance Initiative (IGI; iginitiative.com) is widely credited with moving the discipline forward. It has legitimized information governance as a free-standing business exercise, distinct from enterprise content management (ECM). It is not seen as synonymous with information security but the two are most definitely related—or perhaps joined at the hip is a better way to phrase it.

Components of Information Governance

But what do we mean by the term information governance? Everteam's Ken Lownie points out that the definition of information governance is far from set in stone. It encompasses a number of different functional areas, including records management, information security, knowledge management, big data, and data science.

Lownie identifies five core capabilities of information governance:

- ◆ Connecting to every piece of content and data within the organization
- ◆ Discovering information by analyzing content, cleaning it up, eliminating duplication, and migrating to secure repositories
- ◆ Archiving content with an eye toward how long it should be retained
- ◆ Managing information to ensure legal compliance
- ◆ Analyzing content across the enterprise, providing advanced search capabilities

Cleaning Out the Garage

To find out more about Everteam's take on information governance, I spoke with Firas Raouf, the company's CEO. He likens it to the laborious task of cleaning out your garage. It's a task people tend to put off. It's very easy to put things into your garage, things you're not sure what you want to do with long term but you're not sure you should throw away. Maybe, just maybe, you'll need that old item some day. And so you keep it, along with other "stuff," until you can no longer park your car in your garage. You know there's 10 things you definitely need to keep, but you can't find them amidst all the clutter. When

"The principle of keeping information stored just in case you might need it in the future is not a good idea... Best practices in information governance stress having rules to guide you in determining what to keep, what to discard, and when to take action."

the amount of stuff becomes overwhelming, you know it's time to apply information governance techniques—although you probably won't call it that.

The principle of keeping information stored just in case you might need it in the future is not a good idea. In fact, it's not really a principle of information governance. Best practices in information governance stress having rules to guide you in determining what to keep, what to discard, and when to take action. Take that software you bought years ago when it was the latest and greatest. But now it's old and tired. It's not just you: Most organizations have software that hasn't been updated. "Old software never dies," commented Raouf. "It becomes entrenched, with tentacles everywhere. It's hard to convince people to throw it out and to find the budget to justify replacement."



Marydee Ojala

Marydee Ojala is conference program director for Information Today, Inc. She works on conferences such as Enterprise Search & Discovery, which is co-located with KMWorld, and WebSearch University, among others. She is

a frequent speaker at U.S. and international information professional events. In addition, she moderates the popular KMWorld webinar series.

Ojala is based in Indianapolis, Indiana and can be reached at marydee@infotoday.com.

Pain Points

Raouf recommends against telling people they need to implement information governance because they're not likely to understand information governance as a category. Instead, ask them about their pain points. It might be archiving legacy operations, mitigating storage costs, or migrating to the cloud. By focusing on pain points, you can start small, with one application.

Everteam's approach is to focus on the pain point and bring in information governance concepts. For example, add retention schedules to the metadata. This can be easier said than done. Raouf once asked a customer about his company's retention policy and was told it was "keep for 10 years then discard." His next question was if the destruction process was managed. No, it wasn't. Raouf concluded that meant the company did not actually have a retention policy.

Hacking is on many people's minds, thanks to highly publicized events from retail stores to entertainment companies. Thus, information security is a growing concern for companies who don't want to be the next victim. Can you completely prevent attacks? Raouf thinks not, but you can certainly take steps to minimize risk and be less vulnerable. The amount of information being stored has increased exponentially. But it's not only the volume that makes enterprises vulnerable from a security standpoint, but also the failure of a centralized command and control mentality. Raouf estimates that today, with all the different places where information can reside, 80% could be outside the ECM system. That makes it difficult to regulate and manage. Not only that, says Lownie, ECM platforms are over 20 years old and the information governance piece of it is frequently "an afterthought."

You can't clean out your garage, which you've been filling up for years, in one afternoon. You can't set up an information governance program that effectively solves every problem on a short timetable, either. Get the CFO to acknowledge the problem,

start small, and take it one step at a time is Raouf's advice.

Value and Risk

When considering risk, it's the hackers who command attention. But that's not a company's only vulnerability. As Robert Cruz, Senior Director of Information Governance for Actiance, Inc., explained when I talked with him, the value of information governance in mitigating risk lies in managing the many communication channels that exist. He's adamant that, although email is not going away, there are probably 150 other ways people are communicating. Particularly in the financial services industry, those communication channels are being scrutinized by regulatory bodies.

Employees may not even think about some of those communication channels as being work-related. They send an email to a colleague in the same company. That is clearly work-related. They text to the same colleague. They probably recognize that the text is work-related. They make a phone call. Yes, work-related. But what about social media? What about new tools and evolving networks? What about videos and app sharing? What about communication tools like WhatsApp? Given that people may shift from one communication tool to another in the middle of discussing the same topic, it's a complicated relationship.

Cruz thinks that companies need to have policies about acceptable use of communication channels, particularly social media. One multinational bank, for example, bans employees from using Snapchat. It is grounds for termination. He also knows of at least one case where a tweet, probably considered as completely innocent and non-controversial by the tweeter, was construed as advertising. Another problem area is posting something to Facebook that contains non-public information that legally cannot be disclosed. Blog posts could also reveal information that is non-public. The policy should be tool neutral and spell out the exact definition of non-public, material information. It should also address the protection of intellectual property.

One difficulty with the proliferation of communication channels is distinguishing between business and personal usage. This may not be immediately obvious to younger employees. They don't always see a dividing line. That makes creating a policy to explain it to them extremely important. They need to know when a tweet, Facebook status update, LinkedIn comment, blog post, or Instagram post could actually create risk for their employer. Cruz is encouraged, however, when he sees millennials recognizing that data and records belong to their employers.

Policies that were written before the emergence of all these new communication channels need to be revisited and rewritten, probably on a regular basis. Policies may

need to be specific to the job role, Cruz says. Perhaps the sales staff can use Skype for business purposes but not turn on the video camera. Perhaps interactions on social media need to be reviewed before they are uploaded. Perhaps some types of messaging are blocked completely. It's important the policy statements not be too stringent. This can have the effect of encouraging non-compliance. Policies should "help people do their jobs with the structure of the policy."

Gluing It All Together

Actiance, says Cruz, can "glue communication channels together." The necessity to capture information from multiple channels and possibly millions of transactions can overwhelm the system if not done properly. Information governance, then, is not simply about documents, spreadsheets, and presentation slides. It's conversations. And it's conversations that could occur anywhere. "Data is nomadic," he says, "it doesn't want to live in a single location."

"Information governance goes well beyond policy statements. It's about more efficient use of technology so that information that needs to be preserved is preserved in the proper way, for the proper time period."

Unique to Actiance, according to Cruz, is the ability to capture conversations. It can take a snapshot of, for example, a series of tweets from a particular individual, the entire thread of a Twitter conversation, all the tweets of a person on a specific day, or who was on Twitter that day. It can also see what's been changed or deleted. All this conversation data is sent to an archive with the format intact.

Keeping context is necessary. Archiving conversations by converting to text messages disassociated from the thread is not very helpful, since the context of the conversation is lost. Indexing has to be robust so that it can understand all the various communication channels and meld them together, says Cruz.

Best Practices

Cruz's take on best practices revolves around the notion that information governance

involves not only traditional content but also newer communication channels.

His first point is that information is all over the place. This results in both increased value and increased risk. It's a business fact that "content containing business records or sensitive information can be anywhere, including the cloud."

Secondly, there's a real need for policies to be up to date. With new communication channels coming into favor (and falling out of favor), policies should be reviewed on a regular basis. Now that waiters take orders on iPads and no one uses quill pens, why would your information governance policy that was written 10 years ago still be useful? The same holds true for retention policies. Are they still valid in today's world?

Training is the third best practice. Companies should involve employees when designing training so that it is tailored to their actual needs. Training should evolve as new technologies for communication appear.

Closely related to training is his fourth best practice, that information governance tools should be designed for today's communications.

Finally, Cruz stresses cross-functional involvement. If a policy is going to be successful, if information governance rules are going to be adhered to, then buy-in from multiple departments within the enterprise is necessary. Collaboration is now standard in most organization and blocking the use of collaborative tools is a strategy designed to fail.

Controlling Respect

If central command and control doesn't work for information governance for the modern workforce, who have multiple devices and multiple communication tools, then what does? Everteam and Actiance, I think, both recognize that sometimes you simply have to be forceful and say that certain activities are not permitted. At the same time, you should be encouraging employees to explore new technologies that could add value to information and benefit the company.

But information governance goes well beyond policy statements. It's about more efficient use of technology so that information that needs to be preserved is preserved in the proper way, for the proper time period. It means engaging employees so that they feel they have a role to play in the information governance arena. It means following through so that retention schedules are not just promulgated but actually put into practice.

The stakes are higher than ever. Regulated industries have long been subject to certain strictures, but now the regulators are demanding more oversight. Non-regulated industries are also coming under more scrutiny. Information governance may not be the sexiest topic around, but it is getting more respect—and that's a good thing. ■

Best Practices in Information Governance

By Robert Cruz, Senior Director of Information Governance, Actiance, Inc.



Robert Cruz

Robert Cruz is the senior director of information governance for Actiance, Inc. He has more than 20 years of experience in providing thought leadership on emerging topics, including cloud computing, information governance, and

eDiscovery cost and risk reduction.

Information Governance—as a discipline—has undergone a strange and wild ride over the past couple of years. Finally, we have moved past endless debates on definitions and usable frameworks, thanks to the efforts of the Information Governance Initiative (IGI) and other IG leaders and practitioners. Finally, information governance appears to have separated itself from failed enterprise content management (ECM) concepts and early, seven-figure ocean boiling IG projects to “defensibly dispose” of digital ROT (and, BTW, simply relabeling ECM as “content services” provides little utility other than the nostalgic value of harkening back to FileNet circa-2006). And, finally, IG seems to have carved some form of peaceful coexistence

with information security as more firms have recognized the two are inter-linked by the concept of “information risk.”

But, what have we learned that can be elevated to the stature of “best practice” in information governance? Touring the country in recent years and talking with Compliance, Risk Management, and eDiscovery executives has led me to a few practices that I’d like to highlight.

1. Information Value and Risk are Everywhere

More firms have come to the realization that governing content that has value is not just about files, documents, or email. Some

have learned the hard way that a Tweet can contain advertising for a product that is outside of FDA approval guidelines, or that a Facebook post can contain non-public information subject to SEC Regulation Fair Disclosure, or that a text message can be sent with content that violates data privacy laws. Others have simply recognized that sensitive, high-value content might be carried in any number of communications tools that have enabled employees to do their jobs, whether in the form of voice, video, messaging, or other app.

In fact, one major bank indicates that they sent more IM than email last year. A recent survey from PwC also finds that more than 40 percent of respondents feel that a social media presence is important in their choice of a healthcare provider. And, today, WeChat has over 1 billion users around the world—including a dramatically growing number of business users. The reality of information governance in 2017 is that it needs to consider the fact that content containing business records or sensitive information can be anywhere, including the cloud.

2. Your Policies Need to Reflect Today’s Communications

Have you touched your employee communications or records retention policies lately? If not, it may be time to dust them off to ensure that you are keeping up with the ways that individuals are doing their jobs. Policies designed for email may need re-inspection to reflect specific ways these rich tools can be used by employees. Similarly, retention policies may be worth a touch up as you consider the possibility that a conversation that includes information covered under a non-disclosure may be taking place right now on Skype for Business. In fact, according to the Information Governance Initiative’s Annual Survey (of which Actiance is a sponsor), projects to update retention policies are among the most common IG initiatives that firms have undertaken.

However, the issue is not just about retention policies. Many organizations have policies that require that content

Information Governance Initiative
www.iginitiative.com



IG PROJECTS UNDERWAY OR PLANNED IN THE NEXT YEAR

IGI	
Updating policies and procedures	69%
Scanning paper documents	50%
Data consolidation and cleanup	47%
Migration of unstructured information from one system to another	46%
Defensible deletion	42%
Decommissioning an archive or system	40%
Implementation of a new corporate governance framework for IG	37%
Data loss prevention	31%
Implementing legal hold tracking	30%
User rights audit and analysis	22%
Big Data analytics	15%

Data derived from the Information Governance Initiative Annual Report 2015-2016. More info at www.iginitiative.com. © 2015 Information Governance Initiative. Licensed under the Creative Commons Attribution-NonDerivatives 4.0 International License. This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to the Information Governance Initiative.

be inspected before delivery, sometimes referred to as “pre-review” or “moderation.” Policy violations that are surfaced (such as the mention of an investment guarantee in financial services) can lead to action from a compliance reviewer to block that message, escalate to senior management, or to notify and warn the sender of the violation. Other policies may require that specific individuals not communicate with other specified groups, for example, individuals within a tax department of a consultancy may not communicate with those in the advisory services department.

In each of these scenarios, organizations should be actively evaluating how existing policies can be applied to each new channel of communication. Additionally, when new tools introduce new capabilities, firms should determine if they need to 1) adjust policies, 2) explore how those new features can be controlled, or 3) disable those features. A common example is organizations deploying a tool such as Microsoft Skype for Business, where the App Sharing feature may be one that the organization needs to evaluate considering existing policies.

3. Employees Need to be Directly Engaged in Design of Information Governance Training

Given today’s feature-rich communications tools, IG leaders need to work closely with end users to understand how specific roles will make use of key features. For example, it may be advantageous for salespeople to collaborate with prospects over video, so governance policies should outline accepted and prohibited uses of tools like this with input from individuals whose jobs require those tools to interact with prospects. Similarly, individuals with access to information with high business value (e.g., intellectual property or data covered under non-disclosure agreements) should be consulted to understand how they might leverage new collaborative tools so that policies can be defined accordingly.

Since new tools with new features are emerging on a regular basis, training should be ongoing to keep pace with newly

“Understanding how new communications and collaborative tools will impact current regulatory compliance, eDiscovery, and investigative tasks is a critical task to learn early—not when the next major event is at your doorstep.”

deployed technologies, and in a fashion where end users can share and promote best practices in use of those tools—and governance policies can be further refined.

4. Your Governance Tools Must be Designed for Today’s Communications

Equally important, organizations should be asking whether the technologies they currently use to capture, retain, supervise, and discover business records (or data that might be responsive to civil litigation) were designed for the communications of a different era. Those continuing to leverage technology designed 10–15 years ago may be in for a big headache the first time a large legal matter or regulatory inquiry arrives that requires the review and production of social media, instant messaging, or voice communication.

For example, all major archiving products and eDiscovery review tools were designed specifically for email. Many have the capability to understand other communications formats, but must first convert them into individual email messages to be processed. In order to review a conversation taking place over a series of Tweets, for example, a series of independent messages need to be threaded together to understand the conversational context. This process is not only time consuming, but also significantly increases the risk that important parts of that conversation may have been deleted or missed entirely.

Understanding how new communications and collaborative tools will impact current regulatory compliance, eDiscovery, and investigative tasks is a critical task to learn early—not when the next major event is at your doorstep.

5. The Likelihood of Governance Success is Directly Proportionate to Cross-Functional Involvement

Finally, and somewhat obviously, is that the success of information governance initiatives are directly related to the quantity and quality of cross-functional support and buy-in from compliance, legal, infosec, and IT stakeholders. The importance of this alignment has been heightened by shifting communications and collaboration patterns experienced by organizations as business users have proved to be resilient in their desire to use whatever communication tool that is demanded by their customers, partners, and prospects. Blocking the use of these tools has been proven to be a failed strategy. Fewer IT executives are claiming to be aware of all the communications and collaborative tools that are in use today by their end users. More are recognizing the need to implement a process to understand and evaluate the tools available in the market and prepare for the possibility of their use (sanctioned or otherwise) by their employees.

Cross-functional programs to assess the business value and potential risks of new communications and collaborative technology continues to be more the exception than the rule. However, it is a positive step we have seen being taken by more organizations who have acknowledged that the days of information governance programs focused only on the use of email, files, and documents are numbered. ■

“The reality of information governance in 2017 is that it needs to consider the fact that content containing business records or sensitive information can be anywhere, including the cloud.”

Actiance is the leader in communications compliance, archiving, and analytics. Actiance provides compliance across the broadest set of communications channels with insights on what’s being captured. Actiance customers manage over 500 million daily conversations across 70 channels and growing and include the top 10 U.S., top 8 European, top 5 Canadian, and top 3 Asian banks.

The Real Differentiators in IG Solutions

Ken Lownie, Vice President US Operations, Everteam Software

According to Gartner, Information Governance (IG) is:

“The specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information.”

I have been in the enterprise software industry for thirty years, but I am still not sure I understand that definition. The definition is so wide that it seems to encompass most other software categories.

In fact, Wikipedia lists 28 different functional areas for IG, from records management and information security to knowledge management, big data and “data science” (whatever that means). It begs the question: what categories of software are NOT included within IG?

I am setting out in this paper to break down—deconstruct—Information Governance in a way that should be much more useful if you are trying to address an IG need in your organization.

As you will see, it comes down to understanding Information Governance as a set of five core capabilities and realizing that IG solutions share a great deal of DNA with Enterprise Content Management (ECM) software.

The Five Core Capabilities of IG

One way to approach your Information Governance plan is to think of it as a series of 5 steps, or stages that every information item stored in your organization must go through.

Connect: Your organization stores information in systems and repositories across the organization, including both structured, transactional data in business systems and unstructured content such as documents,

emails, web content and images. The first step in IG is to have a method to connect to information in any system in your organization. Each “connector” can then be used to view, inspect, extract and manage information regardless of where it is located.

Discover: Once you have connected to each source system, you need to assess what is in each repository. Using the insights derived from file analytics, you can map out the necessary actions to cleanse the content, delete duplicates, migrate to secure repositories, and mitigate exposure related to private information (PHI and PCI).

Archive: Archiving includes offloading inactive content from production applications to reduce costs, increase application performance, and to address compliance requirements. It includes moving inactive content to lower cost storage tiers as it ages, and archiving content according to compliance policies and application decommissioning needs.

Manage: At the center of IG is records management functionality to address key compliance and governance requirements, including retention/destruction management based on defined policies. It includes processes for the collection, indexing and analysis of records (digital or paper based, structured or unstructured) produced anywhere—and by any system—in your organization.

Analyze: Once in place, a centralized IG system provides the ability to search and analyze all content across the enterprise. That means federated search across multiple content repositories and the use of advanced content analytics to investigate issues and identify insights.

Virtually every Information Governance project involves one or more of these capabilities, combined and integrated to track and control information created by the organization. Best practices in IG starts with



Ken Lownie

Ken Lownie is the vice president US operations at Everteam Software. He started his career at Lotus Development, and since then has played a founding and executive role at several software companies. Lownie is responsible for guiding Everteam’s marketing and sales strategy in the US, and in his role as vice president of customer success he oversees the delivery of services and support to US customers.

defining requirements in terms of these five capabilities, which simplifies the process of choosing IG solutions.

The Shared DNA Between IG and ECM

For us at Everteam, one simple way to think of IG is that it involves a set of use cases that involve the management of content from creation to destruction. As noted above, the use cases tend to center on regulatory, cost reduction and IT infrastructure requirements, and essentially comprise a subset of the functionality provided by ECM solutions.

Wait, what? IG is just a set of ECM use cases? I am not exactly saying that, but I am saying that many classes of IG problems have a lot in common with the things that traditional ECM platforms addressed.

The reality, however, is that the well-known ECM platforms are more than 20 years old, and over their lifetime they added core IG capabilities like records management through poorly integrated, acquired technologies. The result is that for traditional ECM platforms, IG is an afterthought, not a core competency. And that is a recurring pattern in the enterprise software space.

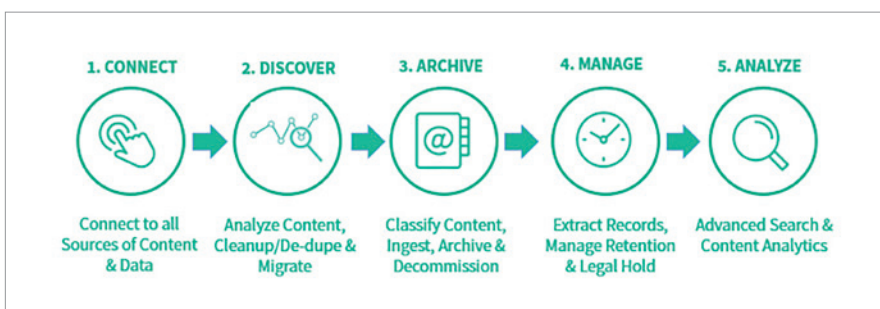
Old Software Never Dies, But It Does Become Unmanageable

Here is a simple rule—let’s call it The First Law of Enterprise Software:

Every class of enterprise software eventually collapses under the weight of its own complexity.

A software system that starts as a well-architected solution to a specific problem inevitably adds capabilities and features to address a wider set of problems as the vendor seeks to add new customers with new use cases. Eventually, through cycles of evolution and acquisition, the once-elegant system becomes unwieldy as disparate components built on different architectural models are cobbled together.

After enough cycles, the result is an inelegant system with high costs of ownership



created by the complexity of configuring, managing and upgrading the system. And when the complexity and costs become so high that customers balk, the cycle begins anew with new software products that deconstruct the problem space and deliver simpler, better-architected solutions.

This is the recurring pattern of enterprise software. Eventually, enterprise software solutions become overly complex and overly expensive, as vendors seek to meet revenue growth targets by adding new capabilities (and new customers). And this certainly appears to be the case with the ECM platforms that underlie many Information Governance solutions.

What started in the 1990's as document management software, a straightforward solution to managing access and versions of documents, evolved in the next decade to an all-encompassing category including the capability to capture, manage, store, preserve and deliver all types of content. Companies like Documentum and OpenText went on buying sprees in a race to fill every niche in the ECM category, from capture solutions to records management to digital asset management.¹

One specific area of functionality that those vendors added through acquisition relates to records management. Unfortunately, those records management capabilities are poorly (or in some cases, barely) integrated with the original platform. The knock-on effect of that type of architecture is that the records management and Information Governance capabilities can be difficult to configure, inflexible and expensive to manage over time.

Architecture as a Differentiator

The fact that IG solutions are late additions to ECM platforms makes it critical to evaluate not just "what" an IG solution does, but "how" it does it. In other words, architecture matters.

One of the biggest differentiators between IG solutions today is in the architecture of those solutions. Rather than a set of functions evolved and assembled in a complex code base that can be difficult to configure and corral into an effective application, the best of the new generation of IG solutions feature a componentized architecture that simplifies building and integrating applications.

This approach to building IG solutions provides a number of benefits:

- ◆ Each service can be deployed, tweaked, and then redeployed independently without compromising the integrity of an application.
- ◆ Initial configuration and deployment are faster and easier because the system is configured through a specific, centralized point of control.
- ◆ You can deploy only the components required by an application, rather than all

components, reducing the size and complexity of the application.

- ◆ You can simplify upgrades by allowing specific services to be updated one at a time without compromising the integrity of the entire platform
- ◆ Microservices allow applications to be much more scalable because you can independently scale the service requiring more power. Specifically, more instances of a service can be added, rather than adding more "cores" to run the entire application at a larger scale.

Microservices Architecture

An architecture based on microservices is the best instantiation of the idea of a componentized architecture. Microservices architecture breaks a large application into a set of small, modular services. Each service supports a specific business goal.

***"Flexibility,
and ease of connection
and integration
are among
the most essential
attributes in an
IG system."***

The services use a simple, well-defined interface to communicate with other services, enabling the mixing and matching of components as required to meet the needs of a specific use case or application. In the case of an IG solution, one service (Audit Events Service) may be invoked when an auditable activity has to be recorded, and another (Retention Policy Service) called when a complex retention rule has to be calculated.

The services model enables enterprises to create applications to address specific business needs and integrate them together in a predictable, repeatable manner. The result is software that is easier to configure, easier to integrate, easier to manage, and highly scalable.

Connectivity is Crucial

IG software sits at the nexus of business processes, collecting and tagging content as

it is created, and managing and tracking it afterward. Given that central position, it is essential that an IG software product easily connects to all the other systems that create and consume content. In fact, flexibility, and ease of connection and integration are among the most essential attributes in an IG system.

Connectivity and integration should be more than possible; it should be designed into the architecture of the product. A connector-based design with pre-configured connectors for major enterprise software systems should be standard components, with simple installation and defined functionality.

A portfolio of connectors greatly enhances an IG solution. An application that starts as a repository, archive, and records management solution for one type of content, created by one system, can be easily expanded by connecting it to additional systems with additional types of content. The result is an application that can be implemented and then modified, expanded and reconfigured by adding or disconnecting connectors, without additional reconfiguration or customization.

The ultimate impact of a better-architected IG system is in the flexibility to build and change applications and the long-term total cost of ownership. A more flexible, agile architecture ultimately means software that is easier to configure, easier to connect to other systems and easier to build applications with.

IG Solutions Differentiators

At Everteam, we have thought a lot about what comprises the core capabilities of an IG framework. Our thinking led us to the five core capabilities of Information Governance: Connect, Discover, Archive, Manage, and Analyze.

We then decided that the best way to ensure a complete portfolio of IG capabilities was to build our IG solutions on a microservices architecture, that would ensure high levels of usability, configurability, and scalability. And our approach takes full advantage of a connector-based model to simplify connecting to—and integrating with—other enterprise software systems.

These decisions reflect our belief that any organization approaching an IG initiative should be looking at what differentiates IG solutions today. Those differentiators include a focus on the core Information Governance functions and a modern, agile architecture that makes implementation easier—and pays back faster. ■

Everteam is a global software vendor with over 25 years of experience delivering highly sophisticated implementations of Content Management, Information Governance and Business Transformation solutions for mid-to-large corporate enterprises and government entities.

¹ For example, in the six-year period between 2001 and 2007, Documentum purchased 11 companies.

6 Ways to Keep Business Content from Getting Out of Control

By **Susan Emery**, Vice President of Product Management, Viewpointe

Regulated industries such as financial services, healthcare or insurance require business to balance innovation and risk mitigation. Can you keep pace with digital transformation without risking security, privacy or retention policy requirements? Is there a way for your business, legal and IT executives to establish shared priorities and act collaboratively to reduce risks, comply with laws and regulations, eliminate needless cost and respond more nimbly to competitive needs and markets? These challenges are real. The solutions require you to rethink how technology is used to meet essential business and compliance requirements and expert guidance from a trusted partner.

To manage business content across its useful lifespan, it is key to identify a cost-effective approach that offers best-in-class technologies and delivers all of the needed services. These include professional services to assist in assessment, methodology, and project management; content services that deliver capture, search, retrieval, hold and disposition; as well as managed services to administer, secure and monitor your organization's most important and sensitive information. The benefits of a three-pronged approach include the ability to:

- ◆ Control costs for a lower total cost of ownership through minimized capital investments and IT overhead
- ◆ Analyze your unmanaged enterprise data and determine what information to manage, leverage and trust based on its value to your business
- ◆ Manage mass volumes of data by archiving content based on value while defensibly disposing of redundant, obsolete and trivial (ROT) data
- ◆ Enforce corporate retention, disposition and legal hold policies consistently across the enterprise to help ensure compliance and mitigate risk
- ◆ Improve your ability to collect and classify information through automated and consistent processes, reducing the burden on end users
- ◆ Respond quickly and cost-effectively to eDiscovery, audit and internal investigation requests while increasing predictability

To help address information challenges and automate content processes, Viewpointe offers OnPointe, a suite of cloud-based content service solutions with a foundation in compliance

and information management. Viewpointe has the expertise to assist with professional services to guide implementation and project success, content services to meet functional requirements with system connectivity and embedded end-user interfaces and proven managed services in a private cloud environment to keep content secure. In addition, Viewpointe delivers the promise of flexible, future-proofed cloud services without sacrificing the security and compliance demands of regulated businesses.

Viewpointe allows you to take control of business content across a broad range of enterprise applications, messaging systems, content repositories and even file shares that often go unmanaged. Designed to handle petabytes of information, OnPointe provides specific services and integrations to ingest and classify many types of structured and unstructured information. With our extensive APIs, even custom or in-house developed applications can be integrated, helping to ensure consistent governance of data.

The OnPointe suite of private cloud-based content services includes five key capabilities:

- ◆ Content capture and management
- ◆ Search, retrieval and version tracking
- ◆ Security and privacy controls
- ◆ Retention management and disposition
- ◆ Workflow automation of content processes

OnPointe for Enterprise Applications helps reduce costs and improve the efficiency of managing content held in both active and legacy enterprise business systems. Through comprehensive lifecycle management and automation, OnPointe for Enterprise Applications helps you meet governance policies, legal obligations and business goals while promoting lean, agile and compliant information management practices.

OnPointe for Print Stream and Image enables you to capture and archive high volume output streams for better management, governance and access to customer statements, invoices or other transactional reports. Individual records can have the appropriate classification and retention rules applied and users can view information in a simple standard PDF or text formats, securely and simply.

OnPointe for Messaging provides the ability to capture email, text from SMS and instant messaging systems as well as cloud services, including Twitter, LinkedIn and



Susan Emery

Susan Emery has over 17 years of experience in enterprise content management software and hosted services focused on maximizing the value and reducing the cost of stored content. An ARMA Certified Information Governance Professional with a background in design and usability, Emery concentrates on customer success drivers across information management and information governance to break the vicious investment cycle enterprise organizations experience in these challenging areas.

SalesForce.com. Duplicate and irrelevant content can be identified and safely discarded in line with your retention policies, lowering storage needs and reducing the complexity and risk of potential eDiscovery orders.

OnPointe for File Shares brings governance and control to file storage areas which often go unmanaged in large enterprises. Content on network drives, SharePoint projects, as well as collaborative sites can be collected, archived and classified, ensuring that approved retention schedules are applied. ROT data can be defensibly deleted in line with your retention policies.

OnPointe eDiscovery helps you manage, identify, preserve, collect, process, analyze, review and produce responsive information helping to minimize the risk, costs and business disruption associated with the discovery process.

OnPointe for Structured Data helps you retire legacy applications yet maintain access to your most important content, manage the growth of your enterprise databases, and produce meaningful production-level test data while protecting sensitive information. Designed for integration with your overall information governance policies, OnPointe for Structured Data provides the ability to discover, identify, and place on hold relational data across heterogeneous environments while facilitating compliance, eDiscovery and disposition.

Why Viewpointe?

Viewpointe has a proven track record managing large volumes of sensitive data and has demonstrated its capability to execute upon clients' content lifecycle and management policies. ■

Viewpointe delivers cloud-based managed services that streamline the information lifecycle and automate business processes with a foundation of compliance and information governance. Known for its time-proven expertise in information strategies and managed services, Viewpointe makes it possible to address today's business opportunities and risks while planning for tomorrow's challenges. To learn more, visit us at <https://www.viewpointe.com/onpointe>

For more information on the companies who contributed to this white paper, visit their websites or contact them directly:

actiance®

Actiance

1400 Seaport Blvd, Building B
Third Floor
Redwood City, CA 94063
PH: 1.650.631.6300
Contact: info@actiance.com
Web: www.actiance.com

everteam

Everteam

2745 Atlantic Avenue
Boston, MA 02111
PH: +1.650.596.1800
Fax: +1.650.249.0439
Contact: info@everteam.com
Web: www.everteam.com

Viewpointe

Viewpointe

227 West Trade Street
Suite 2000
Charlotte, NC 28202
PH: 1.704.602.6650
Fax: 1.704.602.6669
Contact: info@viewpointe.com
Web: www.viewpointe.com

Produced by:

**KMWorld Magazine
Specialty Publishing Group**

Kathryn Rogals
Publisher
561-483-5190
kathy_rogals@kmworld.com

For information on participating in the next white paper in the "Best Practices" series, contact:

kathy_rogals@kmworld.com • 561-483-5190
