ACC DOCKET

Informed.
Indispensable.
In-house.

BUILDING A BUSINESS CASE FOR AN

Information Governance Program

CHEAT SHEET

- *Create a strategic roadmap.* At this step, the team will review current legal, regulatory and business needs, and size up the company culture and budget.
- *Update your policy.* Updating your records management policy is a chance to build a consensus with the business units on what should be saved.
- *Map data for discovery, privacy and records.* A data map is an inventory of the data sources that tells you what you have, where it is and who is responsible for managing it.
- *Select and deploy technology.* The steering committee should work as a whole to select the right technology and assist in deploying it across the enterprise.

By Annie Drew and Mark Diamond

Building a Business Case for an Information Governance Program

The accumulation of information and documents can overwhelm companies, create compliance risks, drive up the cost of ediscovery, threaten privacy breaches and sap employee productivity. Traditional approaches, spread across multiple functions and lines of business, often fall short in their ability to control, manage and dispose of this ongoing accumulation of information. Increasingly, companies are combining records management, ediscovery, privacy and data security into corporate-wide information governance programs that seek to bring together all key stakeholders to develop cross-functional solutions that address the growing risks resulting from the unstructured proliferation of data. An effective program can have a measurable and positive impact on the business.

The problem

The increase in compliance mandates and a harsher ediscovery landscape, coupled with the dramatic growth of digital information, causes challenges for many organizations. Companies have seen a significant increase in the volume of documents, both paper and electronic, as well as data created and received. Today, the average employee sends and receives more than 100 emails per day, and 25 percent of those sent contain attachments.[1] The average employee also creates or modifies 20 or more files per day. Some of these emails and files contain business records, creating a compliance challenge involving sorting records from non-records, and applying appropriate retention. Adding to that complexity is the reality that the digital landscape is continually evolving; web-based social networking and other types of new media content, such as Yammer, are creating new and nuanced compliance challenges. Among this clutter of data may reside protected or other sensitive information, requiring systematic identification, security and disposal, resulting in penalties and loss of reputation if companies fail in this effort and suffer a breach. This amassing data also has an acute impact on discovery, where the volume of information not only directly drives up the cost of discovery but, as companies often don't know what type of documents are where, also forces them to overpreserve in litigation by a factor of 10.[2] Too many documents and data are adding significant challenges for in-house counsel.

Despite this glut of documents and data, most companies do a poor job of identifying, classifying, securing and disposing of email, files and other electronic information. Companies suffer from a "save everything" culture, where employees save email and documents on desktops or file shares well past any required record retention period or beyond any remaining business value. This issue is often compounded when employees use their personal devices or unauthorized web-based repositories. Paper-based records processes either don't capture electronic information or end up filling offsite warehouses with paper copies of electronic documents. Like snow on a glacier — each year, as files, emails and documents accumulate, a little melts away, but most piles up layer upon layer.

Ironically, the biggest casualty of employees' "save everything" approach may be employees themselves: The average employee spends as much as six hours per week — twice what is considered best practice — managing, searching and identifying documents.

Where traditional, siloed programs fall short

Traditional, siloed approaches to data governance fall short. Responsibility for collecting and managing documents and data may fall to legal, records management, compliance, privacy, IT, information security, HR and/or individual business units. With these wide spread responsibilities, no one group owns the coordination and governance of overlapping and intersecting needs and risks. Records management groups may be responsible for official records, but not the management and control of non-record documents. The legal team may be responsible for litigation response, but have no insight or control over the use of new devices and/or cloud-based repositories. IT groups manage data storage, but may have limited knowledge of the criticality of the actual content, which is owned by the business units. Information security is responsible for securing the firewall, but has little say or control over employees use of web-based solutions or personal devices. The privacy team, if a company has one, focuses on policies to ensure compliance with global privacy regulations, but successful implementation is dependent on other groups in the organization. And often, business units are just too busy to make any of this a priority.

What's more, similar tasks, such as data mapping, may be undertaken by multiple groups, independently. And the needs of employees and business units are often ignored, resulting in unsanctioned self-help. So, it is common to find disjointed initiatives and a lack of coordination among groups that is ineffective, wasteful and, most of all, risky to the ongoing business of the organization.

In general, everyone desires better control of information and data, because doing so provides cost-saving, productivity, innovation and compliance benefits, but (naturally) no one wants to end up owning the whole problem. The result is that companies get stuck, and the problems get worse.

What is information governance?

Increasingly, companies are taking a unified information governance approach to controlling their documents and data. Formally speaking, information governance is the specification of

Annie Drew is associate general counsel and chief compliance officer for SIG SAUER, Inc., in Newington, New Hampshire, where she oversees the company's corporate compliance and ethics program. *annie.drew@sigsauer.com*

Mark Diamond is founder and CEO of Contoural, an independent provider of information governance consulting services. Diamond and his company serve more than 30 percent of the Fortune 500. *markdiamond@contoural.com*

decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.[3] Simply stated, information governance combines traditional records and information management (RIM), ediscovery, privacy, data storage and security, defensible disposition and business productivity into real-world, executable strategies that allow companies to better manage, retain, secure, make accessible and dispose of their documents through cross-functional initiatives.

Instead of having different initiatives at a functional or divisional level, an organization-wide information governance program strives to create work streams that address common needs and minimize risk. It seeks coordinated control of data and documents for retention, business use, access and disposition. Information governance recognizes that the key is gaining effective control of data and documents foremost, and that good control through a single program can serve multiple records, discovery, privacy and productivity needs.

A key element of information governance initiatives is that they combine a prioritization around legal and regulatory requirements with employee behaviors and business needs, in addition to a very strong bent toward measurable execution. No two information governance programs will necessarily look the same, because they must reflect the differing business realities that are faced within their respective organizations.

Why build an information governance program?

Good information governance means that the organization stores

The challenge of Yammer compliance

Collaboration is key in moving quickly and efficiently through a tough project in order to stay competitive. As tools for this type of communication, email, instant messaging and texting often fall short (if you can believe that!), and budgets tend to limit the investment in an expensive enterprise solution. As a result, employees take matters into their own hands and, as with everything nowadays, find a solution on the web like Yammer, a "private social network that helps employees collaborate across departments, locations and business apps."[1] Employees are invited to join their company's social network for free by simply entering their work email address and are then encouraged to invite other colleagues to join. A group can be created within the network to facilitate the exchange of real-time information and relevant documentation between employees working on a project, or information can be shared by an employee with the entire network by simply making a post. Important announcements can also be circulated by HR and other functions interested in pushing out information to the entire network. Seems like a great tool, right? Solves everyone's problems — allows for more efficient collaboration and it's free! So, why is this an information governance challenge, you ask?

Simply, the information being shared on this platform is not in the company's control. It sits on someone else's server. This creates a whole host of potential risks: ediscovery logistical challenges when there is a need to produce responsive materials from this repository; privacy violations when sensitive data is stored on a third party's platform; records management policy issues with the storage of documents outside of the company's control; data security concerns related to the potential disclosure of proprietary confidential company information. A few possible solutions exist: Buy the enterprise solution from Microsoft to gain control over the documents and data shared via Yammer; train the employee population on how to use the tool and rely on "proper" use to protect the company; or simply block access to the site. With multiple risks linked to responsibilities across the organization, who should own (and, if needed, pay for) the solution? Cross-functional collaboration is key, allowing each stakeholder to take part in shaping the appropriate solution for the entire organization.

[1] *www.yammer.com.*

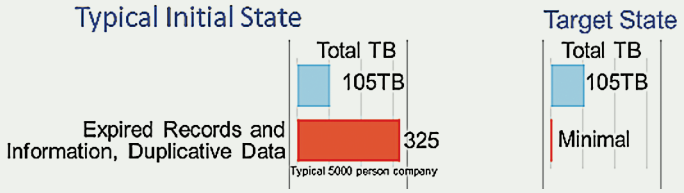
What's the difference between information governance and data governance?

During the past two years, many companies have launched IT-led data governance initiatives. Is this the same as information governance? Data governance is a framework for managing all the data within an organization[1] and focuses on "big data" type initiatives to maximize the income generation potential of data and increasing confidence in corporate decision-making. While information governance and data governance have a few overlapping areas, the two are distinct functions, and a well-designed information governance program both complements and provides input into a data governance initiative.

[1] *Data Management Association.*

Taking a metrics approach to measuring information governance

The effectiveness of information governance programs can be measured by high-level, yet intuitive, metrics around records, privacy data, ediscovery costs and defensible disposition. The example below illustrates the amount of expired records and low-value content that can be deleted from a typical 5,000-person organization. Assess your current state and define longer-term targets for your future state. For defensible disposition, a well-designed program, for example, can reduce 60 percent or more of older legacy data. Use these metrics to track the progress of your efforts.



less unneeded paper and electronic information, and asserts good control over what remains. When you adopt an information governance program, you can expect to achieve some clear wins from a business standpoint:

- **Enabling compliance.** You apply retention policies as appropriate and remove what is not needed to promote compliance with pertinent legal and regulatory mandates, such as those spelled out in FRCP, HIPAA, ISO, FIP, PCI and DSS, as well as under specific state privacy laws.
- **Protecting sensitive information.** With guidelines for proper management, it's easier to secure what must be protected, such as personally identifiable information (PII), trade secrets and other types of corporate confidential data.
- **Reducing storage and operational costs.** IT can centralize the control of information deletion to defer or avoid expenditures and improve application performance.
- **Optimizing ediscovery.** You will be able to assert control over information before the next legal action, and establish repeatable and predictable legal hold processes to minimize business disruption.

Perhaps the biggest win will derive from better employee productivity and enhanced collaboration. Employees can search and locate what they need to improve their job performance by reducing the time they spend in personal information management (saving and searching for email, files and other information) by two to four hours per week. Also, when a project is finished, an employee leaves or a group is disbanded, information that may otherwise be isolated on desktops or in personal archives can still be leveraged for future business value.

From a change management and business engagement perspective, be thoughtful about marketing. Sell your program on employee productivity benefits — records compliance, privacy and better discovery just come along for the ride. Shared victories also lead to a positive side effect: Functional groups across the organization can develop closer and more trusting work relationships. Each group can rightly claim its role as an enabler of — and not an obstacle to — overall business progress, and the legal department will be viewed as helping drive the business forward.

Key steps in creating an information governance program

What does an information governance program actually do? This, of course, varies based on your company's priorities, business environment, industry, compliance requirements, litigation profile, culture and size. However, even across industries, implementation of successful programs shares some common steps.

Create a strategic roadmap

Before executing your initiative, create a "big picture" strategic roadmap. First, build your steering committee (discussed later). Assess where you are today and the level of maturity you want to be in the future. At this step, the team will review current legal, regulatory and business needs, size up the company culture, and evaluate the appetite for expenditure to make it happen. Are our policies up to date? Do we start with email or unstructured data first? How and when do we apply technology, and do we need an archive or content management system? How do we address the older, legacy data? How quickly do we execute this? Frame goals in terms of benefit objectives and proposed metrics for measuring success.

A good roadmap divides large initiatives into much smaller, executable projects with specific and measurable deliverables, combining policies, processes, technology and people. Equally important, avoid the temptation (often promoted by law firms or technology vendors) to purchase a "race car" program, when often a "sedan" or "golf cart" program will do just fine. A well-executed sedan program is more likely to achieve compliance, while reducing costs and risks, than a race car program that is perpetually being assembled in the shop. Also, be wary of anyone who offers an out-of-the-box assessment or roadmap.

Look at peers in your industry for reference. Compare your proposed

approach against industry frameworks from ARMA,[4] Sedona,[5] IAPP[6] and Gartner.[7] The key is balance: a broad approach that achieves compliance, while meeting the needs of the business and, most importantly, is actionable within your organization.

Make sure that the strategic roadmap is detailed, precise and executable. The roadmap itself may be the basis of the request for funding, so be sure to make it clear. This may take a few iterations.

Policy updates

Many records management, privacy, discovery and other information governance-related policies created in a paper-centric or siloed world may need to be updated. Newer legal and regulatory requirements for retention and privacy require updated policies. Many older policies may need to be updated to reflect a media-agnostic approach that does not, for example, classify email as a record type, but rather recognize that email is a medium that contains records and non-records. Additionally, many organizations are updating their policies to synchronize the practices for securing records and privacy or confidential information.

Finally, it may be a good idea to use the policy-update process to better harmonize management of both records and content that has business value. Updating your policy is a chance to build a consensus with the business units on what should not be saved and what should. Strive for practical and achievable policies that are easy to execute.

Litigation readiness and discovery response

Because of their urgency, discovery actions and legal holds can be expensive and disrupt business operations. Sometimes, it is hard to get out of this reactive mindset. An important goal of the information governance program is to proactively develop processes and procedures that lower risk and reduce cost — developed outside the glare of matter-specific discovery. An investment in proactive data management will have a much bigger impact on making reactive ediscovery processes more efficient.

To start, determine the amount and variety of information under management; identify data sources with possible litigation impact, and the systems used to create and store them; review existing legal hold processes for major and minor matters; and identify risk exposure levels and responsiveness gaps. Develop procedures and tools for consistent and defensible hold notice management and tracking. This includes identification of custodians and potential legal hold triggers, repeatable decision processes for issuing hold notices, and methodologies for determining information pertinent to a legal hold.

Data mapping for discovery, privacy and records

Among the best ways to prepare for litigation, manage privacy information, and establish defensible records and privacy policies is to use a data map. A data map is an inventory of the data sources that tells you what you have, where it is and who is responsible for managing it. Many organizations already have separate data maps for discovery or privacy. These are sometimes difficult to maintain. Often, a better approach is to have a well-designed, jointly-managed data map that captures metadata for a number of drivers. This is centrally managed and updated by a number of groups, making it both more accurate and easier to maintain.

Selecting and deploying technology

Careful preparation and planning are essential when using technology to address information governance challenges. Even if technology selection and deployment is IT's domain, the steering committee should work as a whole to inform what is the right technology, and deploy it across the enterprise. Questions addressed by the group should include: What is the right

Using an example to sell the need for an information governance committee

Various countries in Europe have passed legislation requiring notifications explaining the use of certain types of analytical cookies and opt-out options to website visitors prior to entering a website. No single group can own the implementation of a process to comply with these regulations. First, an analysis needs to be conducted to determine if any of these European laws impact your business. All websites must be considered, along with the use of cookies and all likely visitors. This initial assessment requires input from IT related to the current status of the websites, marketing concerning current and future plans to utilize cookies, and legal/privacy regarding application of the laws to existing practices. Once the determination is made that the law(s) requires some type of disclosure and opt-out, a notification(s) needs to be drafted with input from IT and all marketing stakeholders to confirm accuracy and applicability. A technical implementation plan will have to be created to ensure that opt-out functionality can be used without affecting the usability of the website. And, of course, you then have review and sign off of all stakeholders prior to implementation (which will have to include authorization for any expenses associated with the project!). This is just one example of a cross-functional project that, without an information governance committee, would lack a clear owner.

technology for us? What features do we need, and equally important, how do we avoid overbuying? Are there existing technology solutions we currently own that could do the job? Should solutions reside on-site, hosted or implemented in the cloud? Can compliance with regulations and internal standards be assured? Start by understanding current challenges, existing processes and desired business outcomes in order to develop clear requirements that inform suppliers as to what the solution must do, who will use it and how it will be used. This greatly increases the likelihood that any acquired solutions will be fully optimized.

Behavior-change management and training

Employees who needlessly save too many documents are the bane of compliance and ediscovery programs. Proactive behavior-change management helps employees accept and embrace changes to their current working environment so that their behavior can fit within organization-wide guidelines and procedures. Your team must lead the way to turn a "save everything" mindset into a compliant, "save smart" information-sharing approach. Understand employees' pain and articulate how your information governance program delivers real benefits for the company and employees. Be creative! Create multiple communication and training vehicles, including letters to employees from executives, email blasts, webinars and CBT (computer-based training). Don't be afraid to retool the program, if only temporarily, should the change process be too burdensome.

Legacy data disposition

By the time you've reached this step, your organization will have plans in place for managing current (i.e., active) documents and the information that will be created in the course of daily operations. But saving information that is obsolete, expired and not needed for legal, regulatory and business reasons can be costly. The defensible deletion of legacy email, electronic documents, back-up tapes and paper records will help you reduce storage costs, lowering the risk and expense of discovery. Policies for defensible deletion demonstrate that reasonable steps are in place to protect the information and the organization itself. Courts have held that such policies must be routine, transparent, carried out in good faith and consistently applied.

Don't limit your defensible disposition targets to just email. Also, focus on fileshares, back-up tapes, desktops and remote locations. Often, a very quick win will be disposing of older, unneeded paper stored offsite. Armed with up-to-date policies and defensible processes, much offsite paper can be compliantly disposed off, providing a quick win for the program.

To summarize: Start with broad organizational buy-in for your information governance program by involving representatives from multiple organizations — including executives — in an information governance steering committee. Craft a program that matches your company culture, litigation and regulatory profile. Regardless of the specific order by which your program is developed, be sure to articulate business goals and objectives in ways that all stakeholders can embrace. Communicate, communicate, communicate! Many an information governance program has fallen short of its goals because employees either don't know about it or don't believe in it. Finally, be prepared to monitor, audit and update the program to accommodate changing business requirements.

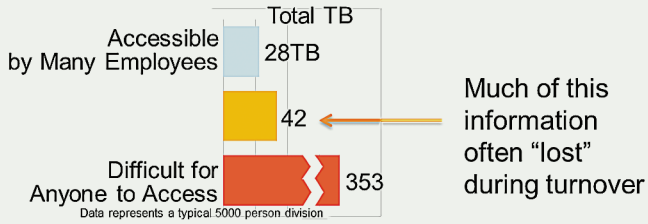
Establish a steering committee and its charter

An effective information governance initiative can be a big win for your company, but getting started can be

Can you get business units to agree to save less (unneeded) information?

"Our marketing manager had all the company graphics stored on her laptop. IT wiped her hard drive before realizing it, and we spent weeks trying to re-create the materials."
– Real-life example from mid-sized technology company

Business units have significant pain around the accumulation of too much information. Much information is stored in employees' individual siloes of email or files. When an employee retires, or there is some other type of turnover, much of this information is effectively lost, forcing its recreation by the employee's successor. Information governance programs can enable the valuable and useful information to be sorted from low-value information. This useful information can then be centrally managed, controlled and accessed by others. In developing your program, identify these and other information pains, and when launching your initiative, use your solutions to these pains to drive the program forward.



One of the biggest challenges in starting an information governance program is getting separate functions (with separate budgets) to work together on an integrated initiative. To overcome these challenges, you should form an information governance steering committee.

tricky. Many of these types of initiatives veer off the road and get stuck in the mud. According to Contoural client research, more than 75 percent of information governance programs struggle to get started, often because of poorly defined scope, or failure to break the initiative into smaller, executable pieces. One of the biggest challenges in starting an information governance program is getting separate functions (with separate budgets) to work together on an integrated initiative. To overcome these challenges, you should form an information governance steering committee. Steering committee members can include (legal) records management, litigation, (compliance) privacy, audit, risk management, (IT) messaging, infrastructure, information security, HR and business units. The final composition can vary from organization to organization. Although a larger group may seem unwieldy, better to be more inclusive earlier in the process than having an excluded group stall your initiative.

Early on, conduct roundtable discussions to identify issues and generate stakeholder buy-in. (See sidebar.) Identify a suitable senior management sponsor or sponsors to whom the committee is accountable. Develop a "charter" that outlines the specific business issues to be faced, responsibilities of team members and expected business benefits of the information governance program.

Your steering committee must pose, and answer, some tough questions. What should you focus on, and in what order? Who should own what? What is your timeframe? Finally, you must confront the elephant in the room: Who pays? Ideally, no one group should be solely responsible. There is no way to answer these questions — and achieve real business benefits — unless there is a committed, engaged and active cross-functional information governance team in place. The most successful steering committees take a matrix approach to functional responsibilities coordinated together in a single initiative. Extra time spent building consensus within your steering committee is time well spent.

Strategies for engaging senior management

The other difficult challenge of information governance is selling the idea to senior management. This is an area not well understood by senior mangers since it is driven by events, such as litigation or privacy breaches, that may or may not occur. On the other hand, with every day that passes, data growth continues to overwhelm the capability of organizations to manage it.

At some point, your steering committee will be asked to make a business case for senior management. Some successful approaches include the following:

- Approach management as a committee, not a single group. This will add significant weight to the proposal.
- Don't weigh too heavily on compliance requirements. Management may end up thinking: Yes, we are required to be compliant, but assuming that we've gone this far without it, do we really need to do it now?
- Information governance is not inherently complex, so keep your descriptions simple and avoid buzzwords.
- Demonstrate how your proposed strategy is the right size for your company and culture, and how you, in many cases, have taken a sedan — instead of a race car — approach.
- Present your initiative in phases, with clear completion criteria at the end of each phase, and a go/no go at the end of each phase, while still keeping a bigger picture view of what needs to be accomplished over a longer period of time. This reduces the risk of programs stalling out.
- Don't forget to include how a successful program not only aids records and ediscovery, but also other corporate initiatives, such as FCPA compliance or data governance.
- Be up-front about program costs, including internal resources and capital expenditures of technology, as well as outside services. Indicate on your timeline when the company is likely to incur these costs.
- Use actual examples of privacy data found on a public fileshare, the impact of when an employee had the wrong version of a document, or historical ediscovery costs.
- Set target metrics and commit to providing updates by measuring your success against these metrics.
- Employee productivity and reducing the impact of turnover is your money slide. This is the driver most likely to carry the day.
- Conclude with the big picture view: Poor information governance practices can tie down and hold a business back. Good information practices enable the employees to be more productive and the business more agile.

A word of caution: Resist the temptation to set expectations for a specific return on investment (ROI). While these information governance pro-

Generating feedback and buy-in from stakeholders

Your invitation to stakeholders for this initial brainstorming session should briefly explain the purpose of the meeting (i.e., to explore the state of information governance across the organization), and request that each participant review and consider the following questions ahead of time in preparation for sharing with the larger group:

1. **How do you personally define information governance here at Company X, and what part does your group play?**
2. **What are some of the risks you have observed related to Company X's collection, use, management, storage or destruction of data, and who owns the mitigation plans related to those risks?**
3. **What are some of the risks you have observed related to Company X's use of new technologies, media and/or devices?**
4. **Where do you see gaps in our overall governance of information (e.g., policies, processes, implementation, training, auditing, etc.)?**
5. **Are there challenges you face implementing your group's documentation/data/technology initiatives (e.g., legal/ compliance support, training, communication, technical support, etc.), and how would collaborating with others help?**
6. **What successes have you had collaborating with other groups when facing a documentation/data/technology challenge?**
7. **What challenges do our employees face with the use, manipulation, storage and destruction of documents (both paper and electronic)?**
8. **What challenges do our employees face with our current technology solutions, and are there new technologies that Company X should consider?**
9. **Can you think of a current documentation/data/technology issue that is best addressed by a cross-functional team?**

grams clearly reduce costs, creating a detailed ROI depends on unforeseen situations, such as litigation, regulatory changes, regulatory sweeps or other unknown events. You could create a hard ROI, but it is built on so many assumptions, it is not likely to be credible. Better to sell your program as a basket of individual wins for a number of stakeholders and the business units.

Final thoughts

An information governance program should not change the way you do business. Rather, a good program will implement best practices with how you do business today.

Think big, but execute in pieces; realize that progress is best measured in the long term, over a multiple-year horizon. Once the elements of an information governance program are in place, frequent evaluation and oversight are critical. Focus initially on areas where a high payoff is likely.

Don't let perfect be the enemy of good. These are inherently imperfect programs and processes. That's expected and a consistent issue, as the legal and compliance standard is often "reasonable and good faith efforts." Put the right program in place that makes sense for your organization and its risk tolerance profile and be prepared to follow it. You will be much better off than waiting for a never-to-arrive perfect program.

Finally, an information governance program can seem, quite frankly, overwhelming. The hardest part is getting started by seeking out the right stakeholders for the steering committee, crafting a problem specific and action oriented charter, and convincing senior management of the value of your initiative. Keep in mind two things as you build your business case: First, the approaches discussed work, even for companies who believe it will never work for them. Second, the effort, expense and time required to drive a successful information governance program is much less than aggregate effort of current piece-meal approaches. With a strong foundation built on buy-in from across the organization, the program will be sized and structured appropriately for immediate and long term successes. **ACC**

ACC EXTRAS ON… Information governance

ACC Docket
Hoarders Beware: Defensible Data Disposal Is Good Business (May 2013). *www.acc.com/docket/data-disposal_may13*

QuickCounsel
Cloud Computing in Ediscovery and Information Governance (Jan. 2012). *www.acc.com/quickcoun/info-governance_jan12*

Top Ten
Top Ten Basics for Issuing Corporate Policies (Apr. 2012). *www.acc.com/topten/pol_apr12*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

NOTES

1 Unpublished survey data from Osterman Research, Inc.
2 Discovery Subcommittee of the Advisory Committee on Civil Rules, Sept. 9, 2011, Dallas, Texas.
3 Gartner Group.
4 ARMA The Generally Accepted Recordkeeping Principles.®
5 Steering Committee for The Sedona Conference® Working Group 1 on Electronic Document Retention and Production.
6 International Association of Privacy Professionals Privacy Program Framework.
7 Gartner ECM Maturity Model.