CIGP

CORPORATE INFORMATION GOVERNANCE PROGRAM

Implement an Information Governance Program

Written by Rick Wilson, Sherpa Software

www.sherpasoftware.com

SHERPA SOFTWARE

Preface

It has been gratifying to see how well Sherpa Software's white paper series on establishing a Corporate Information Governance Program (CIGP) has been received. I'd like to extend my thanks to everyone who has taken time to read each installment and particularly to those of you who have offered such kind comments on the series to me personally.

Collectively, we've all learned a lot since the series was conceived. Within the records management, IT and legal communities there is a broader understanding of what the term information governance implies and the value that it can to bring to an organization in the form of improved operational efficiency and reduced risk. Over the past year, I've spoken with dozens of practitioners and it's clear that many of them are struggling in their efforts to launch an information governance project. Sometimes those struggles involve framing the economic justification for a program to senior management and often the all-encompassing nature of information governance makes it difficult to know just where to get started. If either of these situations describes your position then I have some good news, these are exactly the reasons why we created the CIGP series!

Over the four parts of the program outlined in this eBook, we attempt to break the governance journey down into logical steps designed to help you get started. From understanding the compelling need to selecting and building a team to creating a repetitive process, each of the four phases contains advice that will help you move from analysis to action.

If we've learned anything over the past year, it's that doing nothing is not an option. High profile data breeches have become regular news events, the volume of unstructured data created by technology trends like the Internet of Things (IoT) continues to expand, and employees are saving more email than ever before. Now is the time to start with your governance program with three easy steps:

- Focus on selecting a project that can offer you a quick win.
- Follow the steps outlined in the CIGP for a successful implementation.
- Promote that success throughout the organization.

Need help along the way? Feel free to contact us - the team at Sherpa Software is dedicated to helping our clients succeed with their information governance projects.

By Rick Wilson
Author of CIGP
VP of solutions &support
Sherpa Software

Table of Contents

Meet the Author

Rick Wilson, VP Strategy & Solutions

rwilson@sherpasoftware.com

(412) 206-0005 x218 | @SherpaRick

Rick collaborates with Sherpa's senior management team to establish the organization's strategic direction and formulate specific tactical steps to achieve those goals. As a certified information governance professional through AIIM and ARMA, he also works closely with Sherpa partners and clients to shape the roadmap for Altitude IG, Sherpa's signature platform for policy-driven information governance.

Rick joined the organization in 2008 and served for several years as a product manager, during which he participated in the overall design of Sherpa's Microsoft Exchange products such as Archive Attender, Mail Attender and PST Backup Attender. Subsequent to that, he was a solutions architect in Sherpa's sales department, working closely with the account managers in formulating solutions to address each client's unique business and technical needs.

Rick holds a Bachelor of Science degree in business administration from Geneva College. He is also a certified scuba diver and likes to get underwater as often as possible. He and his wife Debbie reside in the Pittsburgh area, but love traveling to Japan to visit their son, daughter-in-law, and granddaughter in Tokyo.

The Planning Process

What is Information Governance?

Nearly fifty years ago, Peter Drucker coined the term *"Knowledge Worker."* At that time, he asserted that the rise of information in the workplace (and society at large) would create demand for a different type of worker:

> "Finally, these new industries differ from the traditional 'modern' industry in that they will employ predominately knowledge workers rather than manual workers."
>
> – Peter Drucker in *The Age of Discontinuity* (1969)

In today's world of interconnected devices and ubiquitous connectivity, it's easy to see just how prescient Drucker really was for his time. Many of us are engaged as knowledge (or information) workers - routinely creating, processing or disseminating information as our primary job function. As a result, information has become an essential corporate asset. If you accept the assertion that information is an asset, then like any other corporate asset, information must be tracked, managed and disposed of at the end of its useful life. Instituting this type of lifecycle management is the premise behind information governance and it is an important effort since effective information governance not only helps make business operations more efficient, but also mitigates risk.

In this eBook, we describe a proven process for undertaking an information governance project: we call that process the Corporate Information Governance Program (CIGP).

Sherpa Software's Information Governance Methodology

The information governance (IG) methodology detailed in this eBook has its roots in ARMA's Generally Accepted Recordkeeping Principles® (ARMA Principles), EDRM's Information Governance Reference Model (IGRM) and Sherpa Software's industry experience. Sherpa's CIGP approach to IG begins with incorporating the ARMA Principles as a guideline to ensure information accountability, integrity, protection, compliance, availability, retention, disposition and transparency throughout the process. To complement ARMA's Principles, we also factored in IGRM because it adds an organizational element by recognizing the comparable (and sometimes conflicting) needs of various stakeholder groups including:

- Business users who need information to operate the organization
- IT departments who must implement the mechanics of information management
- Legal, risk and regulatory departments who understand the organization's duty to preserve information beyond its immediate business value

While the ARMA Principles and IGRM offer a sound structural framework, the CIGP methodology also factors in real-world expertise in execution, a perspective earned through over a decade of working with clients on complex information management projects. Sherpa has combined all of these influences to

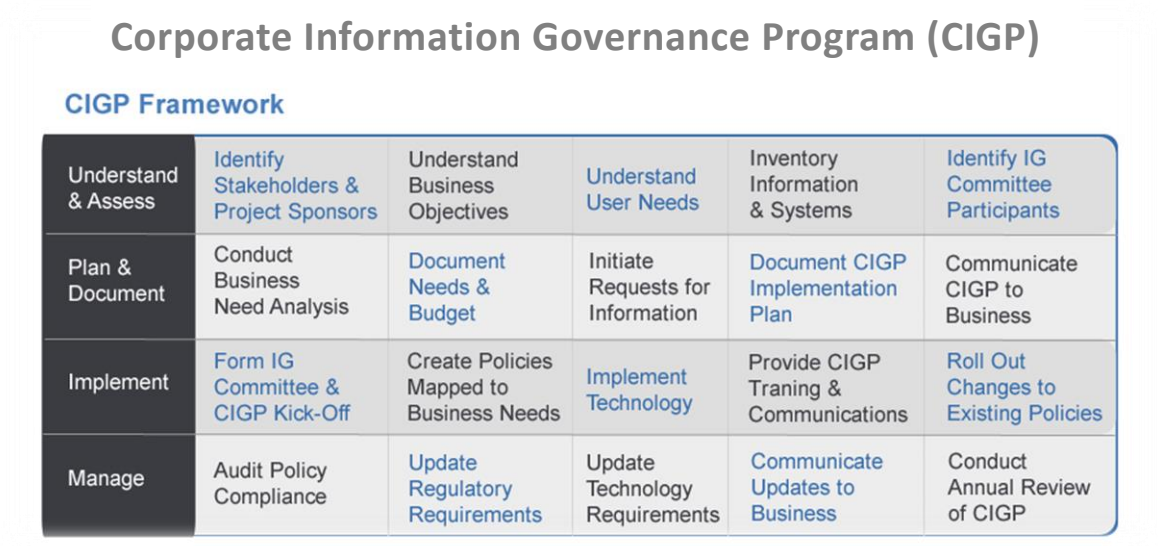

Figure 1: The Four Phases of the CIGP Framework

formulate the CIGP. The progression outlined in the CIGP (see Figure 1 below) is intended to serve as a template that will guide you through the process of implementing a formalized information governance program within your own organization.

This document will be delving into each of the distinct phases of the CIGP framework; Understand & Assess, Plan & Document, Implement and Manage. Let's get started by examining the five steps that comprise the Understand and Assess phase.

Identify Stakeholders & Project Sponsors

In order to be successful, an information governance program should be viewed as an enterprise-wide initiative that is endorsed by senior management and supports the overall business objectives of the organization. Since the CIGP process touches many different areas within the organization, we suggest recruiting project sponsors as the first step in this phase. Sponsors are typically C-level executives who understand that a governance program will help protect the organization by mitigating risk. While their hands-on involvement with the process is minimal, we recommend that organizations keep their sponsors apprised of progress with regular status reports or briefings and rely on their expertise to smooth any resistance raised by the next group of constituents, the stakeholders.

In the context of the CIGP, stakeholders are the parties who have some hands-on involvement with the project. In most cases, they will fall into the category of data owners and therefore are either responsible for, or directly involved with, managing information from a particular source. For example, the director of sales is likely to be the stakeholder responsible for CRM data within the organization. If possible, we suggest introducing your stakeholders to the CIGP process by conducting a group meeting.

The content for that session should be concise: help the stakeholders understand why the CIGP is being undertaken, what you require from them in order to be successful and make it easy for them to participate in the process (after all, they do have other responsibilities). Depending upon the size and complexity of your organization, additional one-on-one stakeholder meetings may be required in order to gain a more thorough understanding of how information is gathered and managed in a particular business process.

Understand Business Objectives

Your organization's business objectives are what will be the underlying workings of your information governance initiative and CIGP. Business objectives will vary widely by industry, organizational requirements and governmental regulations; however, the stakeholders, sponsors and CIGP must work together to clearly define what the business objectives of the IG initiative are, so that specific strategic and tactical plans can be developed and executed for a successful IG plan. Regardless of the driving force behind your CIGP, IG touches nearly all aspects of an organization's data; therefore, it is critical that all parts of the organization know what the objectives are of the IG program and how they will be accomplished.

Ultimately the CIGP must support the organization without placing an undue burden on day-to-day operations, so it is important to thoroughly understand the business objectives of the organization and align the program to support those goals. In most cases, business objectives can be related directly by your project sponsor(s). Since a CIGP effort may span a considerable amount of time, pay special attention to any planned operational changes that may occur during the time horizon of the project (i.e. opening an international manufacturing facility). At this point in your planning, it is key to uncover any factors that may influence the later design and implementation stages of the program.

Understand User Needs

In addition to an understanding of the business objectives, it is important to consider the specific needs of your user community. There is a tendency to limit this analysis to an assessment of the technology that your user community employs (i.e. mobile device types or base system images) but that is only one aspect of this stage. It is also advisable to consider a baseline training level for various types of users within the organization. Instituting an ongoing user training curriculum will be another key success factor in your CIGP effort. Not only should users understand the lifecycle involved with particular types of information that they generate, they should be aware of its classification. For example, what it is that characterizes a piece of electronic content as confidential or the need to tag particular types of communication as those which contain private data (PII, PHI, etc.).

Inventory Information & Systems

Undoubtedly, one of the most daunting portions of the assessment process is conducting an inventory of the information and systems that are being used throughout the organization. Our best advice for this

phase of the process is to rely on the expertise of your stakeholders. They typically have the best knowledge of the various systems being used within their sphere of influence, and if they don't have firsthand knowledge, they should be able to reliably direct you to the parties that do. Trusting their expertise in this area not only shortens the process, it helps avoid oversights that can manifest as gaps in the program at a later stage. Remember: you don't have to address the recordkeeping requirements of the information at this point – just identify the type of data, where it resides and the systems that create it. Determining how to deal with that information will be addressed in a later stage.

Identify IG Committee Participants

The information governance committee serves a slightly different purpose than your project sponsors and stakeholders; those groups are concerned with providing the authority to conduct the CIGP and the knowledge to evaluate what information exists within the organization. The IG committee, on the other hand, will be responsible for helping assess the importance of the information (i.e. what is business-critical and what can be disposed of), providing input on information lifecycles and policies, consulting on user training and any number of other details that will be encountered throughout the CIGP process. In other words, they will become your trusted advisors. Recruiting committee members from different tiers of the organization and various business units will help provide a more holistic perspective on the CIGP since they will have a more diverse set of views, experience and aptitude. We recommend limiting the size of the committee (perhaps ten participants at most, depending upon organization size) in order to keep the team manageable.

Review[DY1]: The Planning Process

Next, we will examine the planning phase of the CIGP process. In the meantime, here are some key takeaways from the Understand & Assess phase:

- Effectively managing corporate information assets is an important strategic objective for most organizations in general and especially for those operating in highly-regulated industries
- This phase of your CIGP process is all about establishing a project structure, establishing relationships and gathering preliminary information
- Don't be too concerned with the 'how' of your governance effort at this stage; focus more on establishing the right team and gathering all of the pertinent information

Building Your IG Roadmap

Exploring the Plan & Document phase

Moving through the information governance planning process typically involves a progression that begins with understanding the current state of existing processes, defining a desired future state for those processes and then establishing a roadmap to bridge that gap. Completing the Understand & Assess phase will have provided some insight into the current state of your organization with regard to overall business objectives, user needs and current systems. The *Business Needs Analysis* within the CIGP Plan & Document phase will complete that picture by providing insight into how information is currently generated, consumed and disposed of within the organization. These insights are normally uncovered by interviewing stakeholders within each business process area. During that information gathering process, there are some governance-related considerations to include.

Conduct Business Needs Analysis

One of the main objectives of this eBook - is to provide actionable advice for completing your IG project. With that in mind, Figure 2 illustrates governance-related future state objectives that should be included as part of the *Business Needs Analysis*.

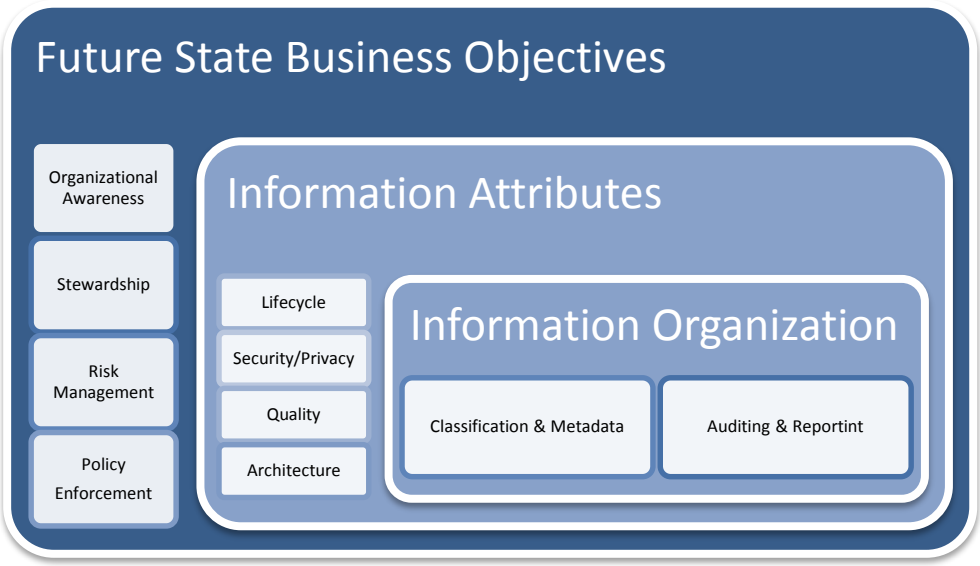

Figure 2: IG Focus Areas for Business Needs Analysis

Depending upon the size and complexity of your organization, some of the areas shown in the diagram may not apply; so, let's consider each in more detail.

Organizational Awareness

Providing regular feedback to the organization, while the IG program is underway, is critical to the visibility of the program. This is the perfect opportunity to solicit feedback from various constituents on what governance-related reporting requirements are important to them, and how to supply them with reporting criteria that will demonstrate the effectiveness of the IG program.

Stewardship

Information assets have an inherent value to the organization, so it is important to establish accountability for those assets. Ensuring that all parties have a clear definition of what constitutes an information asset will help improve stewardship and accountability. As you identify information assets, make sure those assets are linked to an accountable individual. Creating a responsibility assignment matrix, or RACI chart[1], will help you track responsible and accountable parties for each information asset type.

Risk Management

Regulatory requirements often dictate how various types of information must be treated throughout the organization. A continuous review of the latest regulations applicable to your jurisdiction will help ensure that current rules are being adhered to and mitigate the risk of non-compliance. In addition, look for information which may be subject to unauthorized or anomalous access as potentially high risk content.

Policy Enforcement

Consider how your company will enforce policies and how you will monitor compliance with those policies. Strong policy management helps build stakeholder confidence that governance practices are being applied uniformly throughout the organization. Additionally, consistent policy enforcement is one of the control criteria examined by regulators and auditors.

Information-Related Attributes

There are discrete information-related attributes to consider as you assess each business process area, which may significantly impact your IG project. They include:

> **Lifecycle**- Establish a systematic structure that balances information availability with business requirements and regulatory mandates. There are measurable economic benefits to be gained from enforcing lifecycle guidelines, including lower storage costs and reduced risk exposure.

[1] For more information on RACI see: http://en.wikipedia.org/wiki/Responsibility_assignment_matrix

Security & Privacy – Categorize information with regard to its sensitivity and risk profile. If, for example, the systems used by this business unit include personally-identifiable information (PII), they carry a much higher risk rating than routine marketing communications.

Quality –Look for an element of consistency to the information being generated within this business area (usually enforced by business rules). For example, address fields should be utilizing standard USPS state abbreviations.

Architecture- Information should be stored in a standard format that is accessible to other users or applications within the organization, so it can become a common asset.

Information Organization

Establishing a coherent means of organizing information assets can help employees locate information faster, preserve institutional memory and aid in identifying redundancies. These attributes will increase your organizations utilization of relevant versus non-relevant assets, as well as increase the effectiveness of locating and categorizing data that is business appropriate.

Classification & Metadata - The key to organizing assets is a well-thought-out classification scheme and/or consistent metadata elements. As you uncover information within a business unit, ask about what metadata it contains natively and the possibility of extending or customizing those attributes. In some cases, the data may be classified based on business use (for example, contracts) in addition to metadata elements.

Monitoring & Auditing - Establishing a sustainable process for collecting and storing audit information is key to a successful compliance strategy. The goal is to find a consistent method of gathering data across the organization. This will help reduce the cost of collecting and storing the audit information, and also minimize compliance costs.

Document Needs & Budget

The information gathered during a *Business Needs Analysis* can be used to document your current state business processes and map them to the future state objectives. We recommend visually mapping these processes in order to develop a succinct list of gaps that you can prioritize. The mapping exercise can be performed using a graphic format (see Figure 3), an Excel spreadsheet or even a series of Post-it notes on the wall.

Use the GAP analysis to help prioritize initiatives that are achievable both in terms of budget and organizational effort.

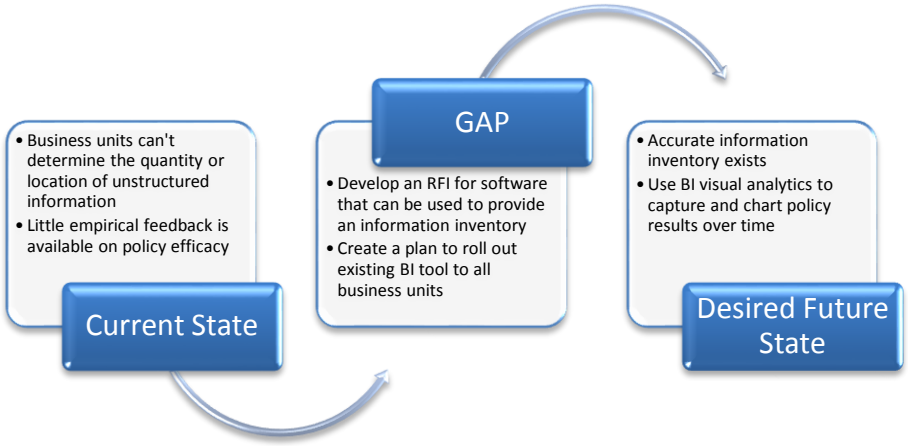

Figure 3: Sample GAP Analysis

It's important to be realistic in this effort; in most cases, a substantial amount of information is gathered during the business analysis. In order to address all of the proposed gaps, it may take a long period of time and a staged investment. For that reason, we advocate selecting a few high-visibility future state objectives to work on at a time as you move toward a comprehensive IG implementation. This prioritization becomes particularly important when you factor budgeting into the analysis. Although many IG initiatives result in significant cost savings over time (i.e. reductions in storage capacity), they typically require up-front investment. Use the GAP analysis to help prioritize initiatives that are achievable both in terms of budget and organizational effort.

Initiate Requests for Information

In many cases, bridging the implementation gaps (to reach the information governance objectives that you have defined) will require additional resources in the form of hardware, application software or consulting services. Creating RFI (Request for Information) documents is a useful tool in soliciting feedback from third parties with regard to how their products or services can help you achieve the project goals – this effort can also help you determine if your budgetary constraints are realistic.

At a minimum, the RFI itself should briefly describe your organization, the purpose of the proposed project, the requirements for the solution that you would like the vendor to propose and a projected timeline. Be precise with your requirements, but don't include more information than is necessary in the RFI. Too much extraneous detail may confuse the responding parties resulting in delayed responses or vague and inaccurate proposals.

While you wait for the RFI response documents, select a scoring mechanism that will help you rate and compare responses. It becomes much easier to score vendors across a level playing field if you dictate the format of their response (for example, a pre-defined Excel response template) as part of the RFI. After scoring responses, select the top three and conduct interviews or demonstrations with the finalists.

Document the CIGP Implementation Plan

Like any other enterprise-wide initiative, taking the time to develop a comprehensive project plan will improve your odds of implementing an IG program on time and on budget. Project plans serve as excellent guides for resource planning and tracking those all important project milestones. Effective project management with a focus on leading (rather than lagging) milestone indicators is often cited as a key factor by successful IG programs.

Communicate CIGP to Business

From a transparency point of view, socializing the IG initiative is an important step in encouraging accountability for information assets throughout the organization. Concentrate on establishing appropriate channels to regularly communicate the progress of the IG effort as it rolls out. Avenues such as internal newsletters, blogs or enterprise social software wikis can all be helpful ways to reach the organization and build support for the project.

Review: Building your IG Roadmap

Here are key takeaway points from the Plan & Document phase:

- Developing a clear picture of current and future state objectives is a critical element of the planning process.
- When conducting your *Business Needs Analysis*, steer toward governance-related future state objectives.
- Prioritize your future state objectives carefully. Undertake those that are budget-friendly and have a high probability of success first in order to build support for the longer-term objectives.
- When soliciting outside support, keep your RFI documents succinct.
- Work from a project plan that will help you spot problem areas with leading indicators.
- Keep the organization involved – communicate regularly.

Exploring the Implementation Phase

Exploring the Implementation Phase

Effectively moving from planning to production is the emphasis of the CIGP implementation phase. This eBook describes four processes that can help safeguard corporate information assets by moving a governance program off the drawing board and into daily operations.

Form IG committee and CIGP kick-off

As mentioned in the first section, the IG committee members that you recruit should represent a cross-section of the organization in order to bring diverse expertise and knowledge to the project. Typically, the committee will be represented by various departments that have direct knowledge of, and potential responsibility for, handling your organization's internal and external data requirements. This may also include regulatory requirements. Most IG committees have representation from the executive team, compliance, IT, HR, legal, records, and/or security. The IG committee members should know where the organization's data is kept, what information needs stored, how long it should be stored, what information should be deleted, when it should be deleted and how information is accessed and moved within the organization. Treat your committee as a group of trusted advisors; they will have the knowledge to help you identify which areas of the business can benefit most from an information governance project, what the degree of difficulty will be to implement that initiative and how best to socialize the project within each segment of the business.

A project kick-off meeting is the ideal opportunity to bring your committee members together to underscore the importance of the project, prioritize the list of governance initiatives and solicit feedback on the best implementation approach. Keep in mind that your committee members have other responsibilities and priorities; remember to maintain clear and concise communication, so they understand exactly what information you need and how best to provide that to you during the course of the project. Often utilizing a portal like SharePoint (or similar tool) to centralize common documents and distribute meeting agendas helps to keep committee members involved and informed between regularly scheduled meetings.

Create policies mapped to business needs

One of the primary tools available to help enforce your governance rules is still the venerable policy. Policies, as defined by the dictionary, are a set of plans or actions agreed upon by an organization. Working with your committee to formulate these plans or actions is an important step in implementing your information governance controls. Since every type of electronic record in your organization will likely have different business and/or regulatory requirements, the committee may need to formulate a number of information governance policies. The grid below outlines some elements to consider when formulating a policy and suggests which committee members to consult for guidance:

Policy Formulation Elements	Governance Committee Advisor				
	Executive Team	Legal	Business Unit	IT	Records Management
Establish retention periods		✓			✓
Determine ultimate disposition			✓		✓
Validate compliance with controlling authorities		✓			
Select enforcement strategy				✓	✓
Sign off on official policy	✓				
Implement Policy			✓	✓	
Audit policy compliance		✓	✓	✓	✓

In some cases, policy controls will be dictated by industry best practices or regulatory requirements; however, outside of these constraints, organizations typically have a fair degree of latitude with regard to how their policy enforcement will occur. As your committee prepares to draft specific policies, it will be very helpful to have some baseline data about the current situation for the information repository in question. Obtain answers to questions such as:

- Who controls the information in question?
- How much storage space is the information occupying?
- How long is the information being retained?
- Where is the information being retained?

This will streamline the policy formation process for your committee by helping to identify unmanaged data silos or shortcomings in existing enforcement efforts. After selecting a particular content area, the committee can begin considering appropriate controls for that information and draft an appropriate governance policy. Policy formats vary widely from organization to organization but typically a policy will include the following sections:

1. Purpose – a narrative describing the intent of the policy
2. Scope – who the policy is applicable to
3. Definitions – explanation of any technical terms included in the policy
4. Responsibilities – who is responsible for policy implementation, enforcement and auditing
5. Designated Record Set – which data repositories the policy applies to
6. Minimum Policy – describe how the policy operates in detail
7. Training – how policy compliance will be communicated to the organization
8. Enforcement – how the policy will be applied
9. Sanctions – spell out the consequences of violating the policy

Once the policy has been drafted and approved by executive management, the focus turns to implementation. The next section offers some suggestions about using technology to enforce your newly-approved policies.

Implement technology

In simpler times, businesses could rely on written policies alone to determine how files, correspondence and other communications were handled, and the organizations' users were left in control of following these policies. Given the explosive growth of electronic communications, extensive regulatory compliance mandates and the ever-present threat of litigation, relying on written policies that organization users execute alone is simply not a defensible practice. Implementing automated policy enforcement tools is the best way to overcome the hurdles associated with written policies executed by users. Here are a couple of tips to consider as you evaluate the characteristics of a policy automation solution:

- Flexibility matters in a policy enforcement engine. It is tempting to focus on whatever the 'current' requirement is when evaluating solutions; though, that approach can sometimes be short-sighted. Perhaps you only need to perform defensible disposition using age-based criteria today – but as business needs evolve, the ability to supplement that age-based checking (with additional options like keywords or regular expressions) may be required; therefore, look for more capabilities than you currently require.
- The more content sources that a solution supports, the better. Investing in a policy tool for email may suit your current requirement, but what happens when legal extends the policy to
- Include SharePoint, file shares or some other content repository? Selecting a solution that features an open application architecture will help future-proof your implementation with regard to supporting multiple content sources.
- Limiting the degree of end-user interaction required for policy enforcement typically improves the probability of success for the initiative. Many traditional content management applications rely on the individual generating the content to apply the appropriate metadata tags required for administration. The technology to automatically tag or classify information based upon its semantic content is evolving rapidly - so look for classification capabilities in the technology that you evaluate. The ability to automatically classify content or uncover hidden relationships between various types of information promises to be an effective strategy for dealing with increasing volumes of electronically stored information (ESI).

Provide CIGP training and communications

In order to succeed in the long term, your information governance program needs to become an integral part of the organizational culture. Both training and communications are an important part of that integration.

Effectively communicating both the operational aspects of the policy and the rationale behind implementing it often helps foster adoption. In most cases, implementing a governance policy means that information will be retained for a shorter period of time or only available to a select group of users, and employees are often reluctant to accept these more restrictive types of controls. Taking time to explain how a policy will protect the organization (and ultimately their jobs) may ease the transition to a more controlled environment. The most effective way to communicate the IG policies will often need additional input from departments outside of the IG committee so that the committee can better understand what type of communication and training options will have the most impact across the organization.

In addition to communications, training is also a critical initiative for policy content. Instituting a formalized training program to help the end-user community understand how the governance policies operate is essential to the implementation effort. The training agenda should include a clear narrative of how the policy functions with an emphasis on any interaction that is expected (or required) by the end-user. Although the training sessions will need to be repeated periodically (perhaps quarterly) in order to include new employees, the initial sessions should be scheduled as close as possible to the policy 'go live date' so participants have the opportunity to apply their newly acquired knowledge. Ongoing training can also be supplemented with training video tutorials. These tutorials can be made a part of the IG process as required viewing to help reinforce in-person training.

Roll out changes to existing policies

Periodically, the policies that have been established will need to be modified or updated to reflect evolving business needs or regulatory requirements triggering the process described above to be repeated:

- The IG committee will meet to approve the updated policy constraints
- The technology tools that were selected should include the capability to schedule and roll-out new (or modified) policies
- Modified policy guidelines should be communicated to the community
- Training programs should be adjusted to reflect the new standards

The ongoing changes should be part of reoccurring meetings with the IG committee. Much of the work will be accomplished with the initial rollout; however, updating the existing policies is just as important as the initial roll out to keep evolving business needs and regulatory requirements in check. It is tempting to skip or combine steps in an attempt to streamline the process, but each of them serves an important purpose and is integral to the ongoing success of your information governance program.

Review: Exploring the Implementation Phase

Here are key takeaway points from the Implementation phase:

- Plan time to gather key metrics about your information prior to policy planning
- Leverage the expertise of your IG committee members when formulating policies
- Select policy enforcement tools that are flexible and extensible
- Let your user community know why the governance polices are being implemented
- Make provisions for initial and recurring training of the end user community
- When policies change, resist the temptation to take short cuts and be sure to repeat the implementation steps

The Management Phase

Exploring the Management Phase

The final phase of the CIGP process describes management activities that are essential to ongoing success since, like other corporate oversight activities, a governance program must be continually monitored, measured and adjusted in order to ensure it is relevant and effective.

Audit Policy Compliance

By this stage, your information governance (IG) committee has invested a substantial amount of time and effort in drafting a set of governance policies, and you have implemented a process for enforcing those policies. The role of auditing is to ensure that those policies are being consistently adhered to by the organization. Reactions to the term “audit” are almost universally negative, given its close association with taxes, but instituting a scheduled auditing process is an essential practice to validate governance policies are being adhered to.

Auditing does not need to be a complex process; in fact, some of the most effective tools can be relatively simple reports run against unstructured data. For example, if your policy prohibits mailbox owners from keeping messages older than 90 days, periodically select a set of random mailboxes and run a report checking for messages that exceed the threshold to ensure the process is running as planned. Of course, not every policy can be validated by a simple date check, but look for low impact ways to verify policy compliance. The simpler the audits are to perform, the more likely they are to be regularly conducted by your team. These audits should be executed across different departments and different data silos that fall under your information governance program. By implementing simple auditing practices that sample multiple aspects of your information governance program, you can create a process that supports and ensures that the policies implemented are being upheld.

Update Regulatory Requirements

Certain industries (healthcare, financial, etc.) must adhere to a fairly rigid set of regulations. In these industries, there is almost always a corporate department closely monitoring the regulations for changes and adjusting policies accordingly. Unfortunately, this is often not the case for organizations who are not accustomed to regulatory oversight. It is a good practice to annually review any changes to your business practices then revisit any regulatory compliance mandates those changes may have triggered. Here are some examples of how an operational change may introduce a new regulatory obligation:

- If your organization has moved from private to public ownership recently, that change may trigger a compliance requirement with some sections of the Sarbanes-Oxley Act, or other regulations required for public companies.
- You may inherit a new regulatory requirement from your customers. If you recently started doing business with a healthcare-related entity (hospital, clinic, outpatient facility, etc.), recent changes to the HIPAA statues may obligate you to execute a business associate agreement, and that document may impose new obligations to control certain types of electronic information generated internally.

To stay updated, there should be one or multiple members from different practices within your IG committee that are charged with reviewing the changes in regulatory requirements that may affect your information governance policies. Catching these new compliance obligations early gives you time to institute a remediation strategy and avoid potentially costly litigation.

Update Technology Requirements

There is little doubt about two topics related to technology: first, technology is a key component of any information governance strategy; second, it's a moving target. For those reasons alone, it is vital to revisit your information governance technology on a regular basis. As you perform that assessment, here are some focus areas where technology developments may necessitate changes to your strategy.

1. **Evolving business needs**. Both of the topics addressed in the previous section (Audit Policy Compliance and Update Regulatory Requirements) may trigger changes to the technology required to monitor and enforce your information governance practices. For example, if you have implemented new systems where data is used or stored, the technology you may be using to enforce polices must be able to access that information to bring it into compliance with your information governance policies.
2. **New content sources**. We've recently seen a tremendous expansion in the number of devices used by employees as part of the BYOD trend. By now, most corporate IT departments have instituted a strategy to manage, or at least remotely erase, cell phones or tablets - but the next wave of technology is right around the corner. New wearable devices are popping up every month, and there are already examples of personal data generated by wearable brands and similar personal technology being subject to legal discovery. In addition to wearables, industry experts are predicting an influx of electronic information generated by the IoT (Internet of Things) which can include anything from consumer electronics to industrial equipment. If your organization is likely to be capturing this type of electronic information, it may fall outside existing retention guidelines and require new enforcement technology.
3. **Keeping current platforms up to date**. An important part of your regular technology planning should include evaluating updates to existing systems. Staying current with operating systems, email and other environmental software makes it easier to enforce your IG policies. For example, many vendors who offer governance tools have already dropped support for Windows XP desktops, Windows 2003 servers and some Internet browser versions - many of these systems may still operate in your environment. If an unsupported system has technical issues and becomes undiscoverable, you may not be able to access the data you need to support your information governance policy initiatives.
4. **Investigating emerging technology**. Recent developments in machine learning are powering promising new tools for the automatic classification and categorization of electronic content. Since classification is so tightly integrated to most records retention strategies, technology advancements such as these promise to help your organization improve efficiency and control costs by allowing current staff to cope with larger volumes of information. Staying up to date on new technology will help keep your information governance program running efficiently while potentially increasing its return on investment.

Communicate Updates to the Business

The success of any information governance program requires the ongoing support of the entire organization. During the initial launch of the information governance program, this series discussed socializing the goals of an information governance project to make sure all levels of the company were aware of the program and their individual role in assuring it was successful. It is important to repeat this process on a regular basis, both to underscore the ongoing nature of an information governance initiative and to introduce new employees to the significance of the process. One effective way to accomplish this goal is to publish an "Information Governance Annual Report." This format provides an excellent way to recap the original goals of the project, highlight any changes that will be made in the coming year, and celebrate any successes that were attributable to governance-related processes. The report can then be presented and shared across the organization that will further reinforce it as part of the organization's vital initiatives.

Conduct an Annual CIGP Review

The annual CIGP review is an important step to ensure a governance project continues to be relevant and successful. It's typically a meeting dedicated to reviewing the progress of the information governance initiative over the past 12 months, and the specific activities discussed so far in this document are ideal agenda topics for that meeting. The annual review can also serve as a basis for creating the "IG Annual Report" that will further support your organization's information governance initiatives. It provides an opportunity to realign the governance strategy with the overall business needs, refresh the team by enlisting new committee members, and decommission any policies that are no longer relevant.

Conclusion

Ultimately, there are no guarantees with an information governance process, however the CIGP can help you with the planning and oversight tasks necessary to turn your program into a success story. As always, I welcome your comments on this article or the CIGP approach in general. You can find more information governance resources at www.sherpasoftware.com or contact me directly with the information below.