Why Do Policies Matter?

This six-part Policy Management Illustrated series is part of the larger GRC Illustrated Series presented by OCEG and Compliance Week periodically in the pages of this magazine and on the Compliance Week and OCEG Websites. For a downloadable version of the illustration on the facing-page fold-out and for all prior illustrations in the GRC Illustrated series, please go to www.complianceweek.com and select “GRC Illustrated” from the “Topics” pull-down menu on the toolbar.

By Michael Rasmussen

From time to time, to my surprise, I still hear people asking why policies matter. After all, they argue, aren’t the laws and regulations we have to follow enough guidance? Beyond those requirements, can’t we let managers decide how to run their own operations and have case-by-case flexibility? Don’t policies create liability when they aren’t followed? Isn’t it just more unnecessary bureaucracy?

My answer, at its most basic, is that when an organization fails to establish strong policies, the organization quickly becomes something it never intended. Good policies define the organization’s governance culture and objectives. Without the guidance provided by well-written and effectively managed policies, corporate culture may morph and take the organization down unintended paths.

The longer answer is a bit more complex. Policies set the standard for acceptable and unacceptable conduct by defining boundaries for the behavior of individuals, the operation of business processes, and the establishment of relationships. Starting with a code of conduct defining ethics and values across the organization—and filtering down into specific policies for business units, departments, and individual processes—the organization states what it will and will not accept and defines the culture of integrity and compliance it expects.

Policies, done right, articulate and build the desired corporate culture and drive standards for individual and business conduct. Consider that:

» Policies articulate the governance culture: Policies address more than how to meet legal requirements, they also drive the performance objectives of the organization. Without policies the organization has not made clear what people or business units may or may not do in seeking to meet those objectives. Individuals are left to make decisions and may take the organization where management does not want it to go. Governance is not really taking place.

» Policies articulate the risk culture: This includes establishment of risk-management responsibilities, communication, appetite, tolerance levels, and risk ownership. Every organization takes risk—it is part of business and sometimes helps to get the business where it wants to be. Without clearly written guidance and ownership, however, risk governance will be ineffective and risk decisions will be made by each individual based on his or her personal appetite for risk.

» Policies articulate a culture of compliance: Policies define what is acceptable and unacceptable. This starts with legal and regulatory requirements: communicating how the organization will stay within legal boundaries given the various jurisdictions in which it operates. Policies also establish the values, ethics, commitments, and social responsibility of the organization, when it comes to matters of discretion.

Let’s be clear. Policies in and of themselves do not ensure the right corporate culture, nor do they resolve all the complex issues that arise in addressing performance, risk, and compliance. Merely creating thousands of policies is not the answer; in the case of policies often “less is more.” Even when well-written policies are issued, the game isn’t over. An organization can have a wide array of policies that “sit on the shelf” or are not adhered to and end up in very hot water. We know that an organization may develop a corrupt culture even with the right policies in place; but we also know that it cannot have a strong effective culture without them.

Issuing, well-crafted and appropriately targeted policies is a necessary first step in clearly defining and communicating the organization's boundaries, practices, and expectations. Policies are the vehicles that communicate and define values, goals, and objectives so that culture does not morph out of control. But the policies also must be well managed so that they are both effective and efficient tools to help the organization stay on the path it chooses.

Michael K. Rasmussen is a Principal Analyst with GRC360° Research. He also chairs the OCEG GRC Solutions and Policy Management Councils and serves as an OCEG Fellow. GRC360° Research is an information technology and analyst firm providing independent and objective research and analysis on topics related to Governance, Risk Management, and Compliance (GRC). www.grc360.com
The continual growth of regulatory requirements, complex business operations, and global expansion demand a well thought-out and implemented approach to policy management. This illustration defines each step.

**Why Do Policies Matter?**
Strong, well managed policies that are integrated across the business help to:
- Define, articulate, and communicate boundaries and expectations
- Communicate risk limits
- Establish a culture of compliance
- Guide desired conduct
- Protect the organization
- Achieve business objectives
- Explain governance and accountability structures

**Why Does Policy Management Matter?**
In many organizations, policies are scattered throughout the entity with no central repository and suffer from:
- Inconsistent styles
- Unauthorized issuance
- Lack of ownership
- Poor lifecycle management
- No mapping to exceptions or incidents
- No cross-reference to standards, rules, or regulations

**Effective Policy Management**

1. **DETERMINE NEED**
   Only create policies when they define organizational values or mandates, address regulatory obligations, or manage potential risk or liability. Too many policies burden the organization and too few expose it to unnecessary risk. To identify when a policy is needed, monitor drivers and changes.

2. **DEVELOP AND UPDATE**
   Policy development is continual, whether creating new policies or revising existing ones in response to change. Establish and document methods to track conformance with the policy and continued relevance of each policy. Implement controls that enable enforcement. Monitor those controls for effectiveness and adherence. Document and remediate violations, while considering what policy improvements should be made.

3. **COMMUNICATE AND TRAIN**
   A policy is only as good as its communication and understanding. Establish a policy repository and inform all intended audiences of how to access each policy. Consider the importance of each policy and determine the level of communication based on the content, context and audience. Periodically review each policy to ensure it remains relevant and correct. Design and implement standardized steps to determine need for revision, reauthorization or retirement. Maintain the version control and archives of each version and related management steps.

4. **IMPLEMENT & ENFORCE**
   Even with good communication, policies aren’t always followed. Implement controls that enable enforcement. Monitor those controls for effectiveness and adherence. Document and remediate violations, while considering what policy improvements should be made.

5. **MEASURE AND RE-EVALUATE**
   Periodically review each policy to ensure it remains relevant and correct. Design and implement standardized steps to determine need for revision, reauthorization or retirement. Maintain the version control and archives of each version and related management steps.

**Benefits of an Integrated Process and Technology Architecture**
- Consistently manage the policy life cycle
- Notify when changes to regulations, laws, standards and procedures affect policies
- Link policies to drivers, controls, owners, reporting pathways and training
- Provide a user-friendly portal for employees and other stakeholders
- Enable cross-referencing and linking of policies and procedures
- Provide a robust system of record for access/identification/training
- Establish a calendar view to streamline communications
- Restrict access and rights to individual policies
- Assign relevant policies based on target group
- Keep a record of all policy versions and histories
- Maintain accountable workflow
- Deliver comprehensive reporting

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests ©2012 OCEG. Visit www.oceg.org for other installments in the Policy Management Illustrated Series
Effective Policy Management: An OCEG Roundtable

Rasmussen: Let’s start at the beginning. What is effective policy management and how do organizations achieve it? What steps should you take first to gain improvement?

Campbell: Let’s state the obvious first. Policies and procedures are often required by laws and regulations, they help to manage risk and improve efficiency, and they help defend against legal and regulatory actions. The complexity comes about because of the very nature of organizations and the need to collaborate on policy development and understand which risks demand policies, as well as difficulty communicating the letter and spirit of policies across cultures and geography. Effective policy management delivers all these elements efficiently and with an auditable trail. Many organizations have “young” or insufficiently developed business processes around policy management so the first step might be to identify the areas that can provide early and important “wins.” For some it might be workflow and activity management; for others it might be version control, cultural alignment, or alignment with risks.

Daie: Many organizations view an effective policy management system as the cornerstone of their enterprise compliance programs, because it enables the cornerstone of their enterprise policy management process to be effective policy management system as you would expect them to be.

Rasmussen: What is the role of technology in effective policy management? Can you share a few examples?

Tietjen: Most organizations spend an inordinate amount of time “running down” every employee to get signatures on each applicable document every once in awhile. Unfortunately, after spending weeks, or months, collecting everyone’s attestations, the managers then file the signed documents away, rarely in the designated location, and forget about them. Then new employees start entering the system within the next few days or weeks and are trained on the policy, but not asked for attestation—a huge legal and compliance hole. Technology can eliminate this issue by allowing you to assign documents to specific job titles or departments, and then automatically notify current and new employees of policies or procedures they are required to read and sign. It can continue to nag them until they actually electronically sign—thus removing this task from the manager, and allowing administration to quickly see reports of attestation compliance.

Technology aids policy management by speeding up the review and approval process, and enforcing standardization with predefined templates and metadata options. Instead of manually routing paper copies or e-mails that get lost in the shuffle, policy software is used to send reminders of review tasks and maintain a centralized repository that all use for policy collaboration and commenting. Software can detect when a new policy has been approved, and automatically archive the outdated version. Those with policy management software note that what used to take them 2 or 3 months to accomplish is now reduced to 2 or 3 weeks.

Daie: For all these reasons, technology should be the foundation of any policy management program. It gives you the consistent, repeatable, auditable mechanism that you need for effective policy management. Technology facilitates the interaction, distribution, tracking, monitoring, and exception management components of your policy management program. In addition, policy, training & certification systems are essential in distributing policies to employees, contractors, and vendors that may be widely dispersed. These systems provide the ability to determine if a policy simply needs to be published, needs certification, and/or needs online training. Lastly, you’ll need technology to store, validate, and redact the controls that you have in place for each policy. Ideally, you’ll have one enterprise compliance solution that can support all of your policy management needs as well as your other compliance initiatives. This eliminates redundant systems and reduces the need for integration.

Tietjen: Technology plays a number of roles in building an effective policy management solution. Workflow automation can manage the lifecycle from policy initiation to creation, approval, certification, and ongoing monitoring by delivering timely notifications to key stakeholders and provide a security layer to ensure the right individuals have access to the appropriate policies. In addition, the integration of subscriber services and linking of those to the relevant policies helps to ensure updates to the regulations, standards, procedures, and risks can be monitored with actionable workflow to notify and manage changes to policies as a result.

Rasmussen: Many organizations just use spreadsheets and collaboration software to manage their policies. Is this a good solution for effectively managing policies? What are the limitations of this approach? Sometimes, technology can manage the lifecycle from design to creation, distribution, tracking, monitoring, and exception management components of your policy management program. In addition, policy, training & certification systems are essential in distributing policies to employees, contractors, and vendors that may be widely dispersed. These systems provide the ability to determine if a policy simply needs to be published, needs certification, and/or needs online training. Lastly, you’ll need technology to store, validate, and redact the controls that you have in place for each policy. Ideally, you’ll have one enterprise compliance solution that can support all of your policy management needs as well as your other compliance initiatives. This eliminates redundant systems and reduces the need for integration.

Tietjen: Technology plays a number of roles in building an effective policy management solution. Workflow automation can manage the lifecycle from policy initiation to creation, approval, certification, and ongoing monitoring by delivering timely notifications to key stakeholders and provide a security layer to ensure the right individuals have access to the appropriate policies. In addition, the integration of subscriber services and linking of those to the relevant policies helps to ensure updates to the regulations, standards, procedures, and risks can be monitored with actionable workflow to notify and manage changes to policies as a result.

Daie: Often spreadsheets, network drives, and collaboration software are used to manage policies because they are readily available and may even be already paid for by the IT organization. While these solutions have strong purpose and value, they fall short in providing you with the rigor, version control, audit trail, and consistent workflow that you will need as part of an effective policy management program. With more than 3,500 new regulations issued annually at the federal level in the U.S. alone, many organizations find these systems can’t meet their requirements for distribution, certification, and training of policies. These systems don’t capture best practices, build-in operational efficiencies, or provide the evidence required to defend their compliance practices which leave companies re-inventing the wheel as new policies are put in place which costs the organization time and money and possibly compliance with a new regulation. Lastly, many organizations implement policy management programs for their contractors and vendors. Internal systems are often unavailable to any external constituents, limiting your ability to leverage any internal solutions.

Campbell: Let’s think about one example of a particular issue in policy management: the updating of a social media policy. Maybe such a policy was initially created 3 years ago when the landscape was far different than it is today. Updating this policy requires input from business owners in multiple disciplines (marketing, sales, data privacy, employment law, HR, security, public relations, etc) across multiple jurisdictions. Global organizations realistically may need to involve 20 to 50 people in such a discussion. E-mail comments that are cut and pasted onto spreadsheets lose the historical trail of conversation, and file sharing sites can’t properly account for edits that are made simultaneously. The compliance office ends up with a paper trail, with incomplete commentary and edits, with e-mail conversations that are difficult to document, and with hours of manual effort. It’s a step up from paper binders but it’s an answer that’s both incomplete and inefficient.

Tietjen: Trying to manage thousands of policies and procedures with spreadsheets and collaboration tools can require a large team to keep a system clean and up-to-date. And there are several other costly scenarios that they won’t address. For example:

1. Assigning readers by job titles and electronically notifying them of their need to attest, or prove comprehension.
2. Accurate versioning and archival.
3. Creation of multiple templates and formatting for standardization.
4. Linking documents to a regulatory library
5. Automatically moving documents forward in the review process based on escalation and time requirements.
6. The ability to report on all tasks and statuses related to the document.

There are many more reasons that tools and systems not designed specifically for policy management are inefficient and ultimately cost prohibitive. But the most important reason for using a system that is designed for the policy management process is a user-friendly experience—which enables actual implementation and use.