

Prepared By:



**Michael Rasmussen**  
Risk & Compliance  
Lecturer, Writer, & Advisor

*“Collaborative Accountability brings integrity and value to policy management. It provides collaboration and accountability to policy management processes that are often scattered across the organization. It enables policy management to work in harmony across organization functions delivering efficiency, effectiveness, and agility.”*

www.Corp-Integrity.com  
research@Corp-Integrity.com  
+1.888.365.4560

## Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

### Corporate Policies in Disarray

#### Why Policy Matters

Policy, done right, can articulate corporate culture, the boundaries of individual and business behavior, and personal conduct. Consider that:

- **Policies articulate the governance culture and structure:** Most organizations do not connect policy with how they influence and establish corporate culture and align governance activities. Granted, corporate culture is present with or without policies. However, without policies there are no written standards about acceptable and unacceptable conduct. Without good policy, culture morphs, changes, and takes unintended paths without a compass to guide its way.
- **Policies articulate a culture of risk:** This includes risk responsibilities, communication, appetite, tolerance levels, and risk ownership. Every organization takes risk — it is part of business. Without clearly written guidance and ownership, risk governance policy will be ineffective.

### Table of Contents

Corporate Policies in Disarray .....	1
Why Policy Matters .....	1
Hordes of Policies Scattered Across the Organization .....	2
Lack of Accountability in Policy Management .....	3
A Collaborative Accountability Approach to Policy Management .....	4
Collaborative Accountability Policy Lifecycle Management .....	4
1 — Environment Change .....	5
2 — Policy Development .....	5
3 — Policy Communication .....	6
4 — Policy Management .....	6
5 — Policy Maintenance .....	6
Collaborative Accountability in Policy Oversight and Management .....	7
Technology Enables Collaborative Accountability in Policy Management .....	7
Mitratech Provides Collaborative Accountability in Policy Management .....	9
RPEC Unites GRC Efforts and Optimizes Policy Management Across Teams .....	10
Components of Collaborative Accountability .....	13
Corporate Policies No Longer in Disarray .....	13
About this Paper . . . . .	14
About Corporate Integrity . . . . .	14
About Michael Rasmussen . . . . .	14

# Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

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

Within policies, the organization defines boundaries for behavior of business processes, relationships, systems, and individuals. At the highest level, policies start with the Code of Conduct, laying forth ethics and values that extend across the enterprise. These filter down into specific policies at the enterprise level, into the business unit, department, and individual business processes. Expectations of conduct are written into policies, so individuals know what is acceptable and unacceptable.

**Policies are supported by procedures:** Procedures<sup>1</sup> articulate how the boundaries within policies are carried out in the form of actions. Policies and procedures should not be open to broad discretion and interpretation. Policy and procedures, at the statement level, establish and authorize controls by which the organization is managed, monitored and measured.

**It is important to be clear:** Policy does not provide corporate culture, nor does it resolve the issues of governance, risk management, or compliance (GRC). An organization can have a wide array of policies that are not adhered to, and end up in very hot water. However, policies are a necessary means to clearly define, articulate, and communicate the organization's boundaries, practices, and expectations. An organization can have a corrupt and convoluted culture with good policy in place, though it cannot have a strong and established culture without it. The right policy is necessary to define and communicate what the organization is about.

Recognize also that culture itself is broader than policies. Policies are the vehicle that communicates and defines culture so culture does not morph out of control. This requires policy is adhered to at every level and as appropriate to given roles, that exceptions be closely managed, and that violations be dealt with consistently and responsively. Because policy can establish liability, mismanagement of policy and procedures can introduce liability to the organization as a policy or procedure establishes a duty of care for the organization. This reliance upon duty of care can be used by regulators, prosecuting and plaintiff attorneys, and others to place culpability on an organization. It is paramount for an organization to establish policy it is willing to enforce.

## *Hordes of Policies Scattered Across the Organization*

Policy is a critical component of a GRC strategy because it describes the practices and behaviors of the company under specific circumstances — but is often the most overlooked or neglected component of directing desired or acceptable actions. The typical organizational approach to managing corporate policy and procedure is in complete disarray and chaos. The breadth and depth of the voluminous increase in laws and regulations that describe acceptable practices are in contrast with the inept manner in which enterprise behaviors are directed and coordinated.

The typical organization suffers with ineffective policy structures, content, coordination, lifecycle management, accessibility, accountability, and communication. As a result, organizations have:

- **Policies scattered across dozens of places:** There is no single authoritative source where all policies and procedures are consolidated, maintained, and managed. There is no single place where an individual can see all the policies that apply to specific roles or structured in a manner conducive to supporting efficient access.
- **Policies bound by paper:** With numerous policy manuals in print, the typical organization has not fully embraced online publishing and ubiquitous access to policies and procedures.

<sup>1</sup> Additional forms of governance documents include standards and guidelines. Standards provide the specifications for how a policy will be complied with — while procedures provide the how they will be complied with. Guidelines are permissive by nature and are not mandatory. All four, policies, procedures, standards, and guidelines are relevant throughout this document — for simplicity and clarity we focus terms on policies and procedures.

# Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

- **Policies grossly out of date:** In most cases, published policy is not reviewed and maintained on a regular basis. In fact, organizations have policies that have not been reviewed in years for applicability, appropriateness, and effectiveness.
- **Policies that lack an owner:** The typical organization has numerous policies and procedures that lack an owner responsible for managing them and keeping them current.
- **Policies that lack any lifecycle management:** Most organizations maintain an ad hoc approach to writing, approving, and maintaining policy with no defined system for managing the workflow, tasks, versions, approvals, and maintenance process.
- **Policies that do not map to exceptions or incidents:** Typically, an established system to document and manage exceptions to policy is missing. Further, there is a lack of a system to map incidents, issues, and investigations to policy — the organization is ignorant of where policy is breaking down and needs to be addressed.
- **Policies that do not map to standards, rules, or regulations:** The typical organization does not have the ability to define and maintain a record of policies that address legal, regulatory, or contractual requirements. This makes it virtually impossible to produce a compliance manual for a particular regulation. It is a time-consuming, labor-intensive and error-prone effort to validate compliance for auditors, regulators or other stakeholders. The organization does not have the ability to easily assess the impact of new or changing regulations that affect policy.
- **Policies lack adherence to a consistent style guide:** The typical organization has policy that does not conform to a corporate style guide and template. Policies often use language used only by the individual or department that created them, rather than terms commonly used across all policies and procedures.

## *Lack of Accountability in Policy Management*

Adding to these issues, organizations often lack an auditable means of policy communication, attestation and training. There are various processes and approaches to tracking policy attestation and certification (making sure policy documents are read and understood), and corresponding quizzing and training. The organization must provide full visibility into who accessed a policy, accepted it, was trained on it, and passed or failed quizzes to gauge understanding — all things that provide the organization with a stronger defensible situation with regulators and in legal actions.

Organizations that approach policy without clear accountability face significant risk to their business. This accountability applies to policy owners for their ongoing review and maintenance of policy, the process of granting exceptions, monitoring incidents and violations of policies and extends to policy governance to track reading, acceptance, and training on an individual basis.

When the organization is under a microscope, having a detailed trail of what policy was in effect, how it was communicated, who read it, who was trained on it, who attested to it, what exceptions were granted, what other incidents violated the policies all provide grounds for defending the organization. An ad hoc “dust in the wind” approach to policy management may expose the organization to significant liability. This liability is further exacerbated by the fact that today’s compliance programs affect every person involved in supporting the business both internally, and for third parties. If policies look different, use words with different meanings, are located in different places and don’t offer a mechanism to gain clarity (e.g., a policy helpline), organizations are not positioned to drive desired behaviors or enforce accountability which aid to improve performance, produce predictable outcomes, mitigate compliance risk, and avoid incidents and loss.

# Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise

## A Collaborative Accountability Approach to Policy Management

Collaborative Accountability brings integrity and value to policy management. It provides collaboration and accountability to policy management processes that are often scattered across the organization. It enables policy management to work in harmony across organization functions delivering efficiency, effectiveness, and agility.

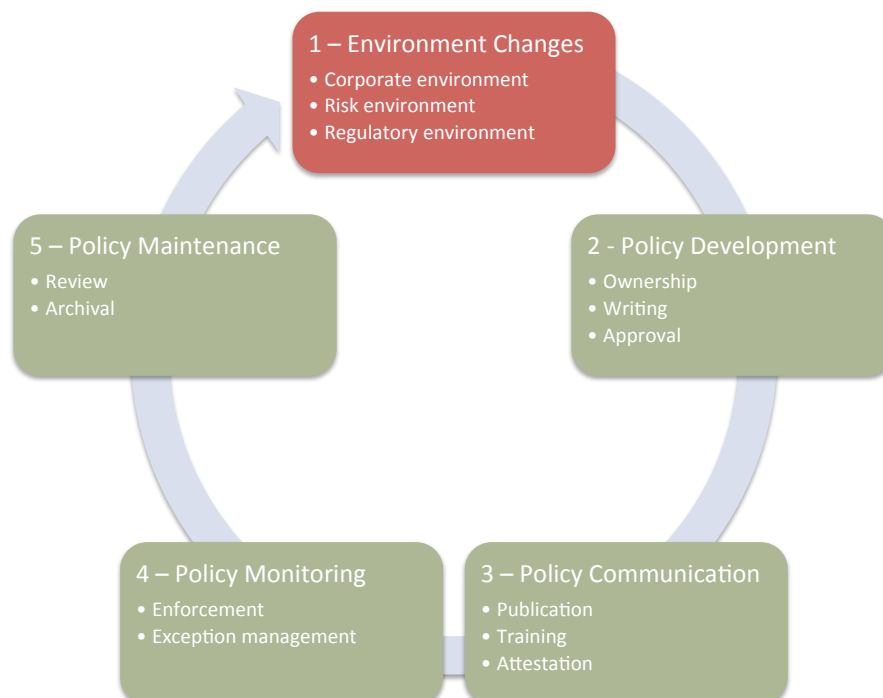
In today's environment, ignoring a Collaborative Accountability view of GRC means processes, partners, employees, and systems that behave like leaves blowing in the wind. Policy management processes are constantly in disarray when operating autonomously, introducing risk in today's complex, dynamic, and distributed business environment. Organizations require an enterprise view of policy accountability and collaboration that not only brings together silos, but integrates them into a common policy-management process.

### Collaborative Accountability Policy Lifecycle Management

Most organizations fail to manage the lifecycle of policy, resulting in policies that are out-of-date, ineffective, and not aligned to business needs. It opens the doors of liability, as an organization may be held accountable for policy in place that is not appropriate or properly enforced. Organizations require a consistent process to develop, communicate, monitor, and maintain corporate policy and procedures. This requires collaboration across business roles with clear accountability throughout the process.

Collaborative Accountability Policy Lifecycle Management is the process of managing and maintaining policies throughout their effective use within the organization. It involves defined stages of monitoring business change for policy development, communication, and maintenance.

Implementation of the Collaborative Accountability Policy Lifecycle Management requires a technology architecture that is rich in content management, workflow management, process management, task management, notifications, and has a robust accountability audit trail. The lifecycle is defined in five primary stages: Environment Change, Policy Development, Policy Communication, Policy Management, and Policy Maintenance (see Figure 1, below).



**Figure 1: Collaborative Accountability Policy Lifecycle Management.**

# Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

## 1 — Environment Changes

Something has happened and the organization is faced with the question — should we write or revise a policy? The organization needs a clear guide to determine when a policy should be written. Policy should not be taken lightly, and should be only created when necessary. Drivers to write policy include: regulatory requirements, establishing the values and ethics of the corporation, outlining business partner requirements, best or industry practices, awareness of potential liability, and a host of others. An organization needs an active risk and regulatory-intelligence process to identify when a policy needs to be created. This includes the ability to monitor:

- **Corporate environment:** An organization may have changed in response to new strategies, objectives, mergers, and acquisitions. Changes in corporate commitments, contracts, values, ethics, and social responsibility statements also drive policies.
- **Risk environment:** The risk environment changes continuously. This requires ongoing risk intelligence processes to monitor geopolitical, environmental, economic, strategic, and operational risks that impact policies.
- **Regulatory environment:** New laws, changing regulations, litigation, and court rulings (case law) impact organizations and drive policy adoption and changes. Organizations need regulatory intelligence processes in place to monitor the dynamic and changing legal and regulatory environment in all jurisdictions where the organization conducts business.

## 2 — Policy Development

Upon identification of a change in the corporate, risk, and regulatory environments, with a determination that a policy is needed, the organization enters the Policy Development phase. This includes:

- **Policy ownership:** The first step is to assign a policy owner. Every policy in the organization should have an individual or business role that owns the policy. Even if the policy is applied across the entire organization, such as with a Code of Conduct, it is necessary that someone or some committee be established as the owner of the policy to oversee its implementation and monitoring within the environment.
- **Policy writing:** Once an owner is established, the next step is to write the policy. All policy should be written in a consistent style, format, and language organization-wide. Policies must be clear and easily understood by the intended audience. Who the policy applies to, what standards, rules, regulations or laws it intends to address; and what if any, larger program it will be associated with should be clearly articulated.
- **Policy approval:** Once the initial draft of the policy is written, it moves into the approval process. The owner sends the draft policy to identified stakeholders to approve the policy before going to publication. Some stakeholders may be in the approval stage for every policy written (e.g., legal). Other stakeholders are approvers because the subject matter touches on their area of the business and they must serve as subject matter and process experts. This stage confirms the roles, users, departments, etc., that the policy applies to, to establish training requirements and accountabilities for execution. It also identifies the criteria for the next phase -- communications and publication -- and considers the timing of other events, such as other significant changes in the business, and other related policies not yet developed or approved. This phase is iterative, as the approvers may send back the policy requiring changes before it is approved and everyone comes to agreement that it is the right policy for the organization.

# Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise

## 3 — Policy Communication

After the Creation phase, comes the Policy Communication phase. This includes:

- **Policy publication:** After approval, the policy must be published. Publication is effectively performed using a single Web-based technology platform. Unfortunately, many organizations have scattered systems that publish policies and procedures and lack a single authoritative system for all policies. This complicates the management of policies as multiple publication media add to the number of policies that will become out of date. Best practice is to have a single policy system in which any individual within the environment can login and see all of the policies that apply to a specific job role in the organization and receive automated notification of the changed or new policy. This event relies heavily upon the previous Approval step, as it supplies time frames for publication and the required recipients.
- **Policy training:** These are the times of Internet video: It is no longer good enough to use only written policy. Organizations must actively ensure that individuals understand the policy and understand what is required of them. This requires that certain policies have associated training in either online or classroom formats to validate that they understand the policy. Surveys and testing are an integral part of training. It is important that classroom and e-learning courses are linked to specific policies and that they are as easily accessible as the policies themselves.
- **Policy attestation:** Once an individual has read a policy and taken associated training, it is important to track their attestation (e.g., certification, assurance that the policy is read and understood) that they read it, understand it, and will adhere to it. Some policies such as the Code of Conduct by their nature require specific attestation on a regular basis (e.g., annual). Other policies may be grouped together in an attestation, although this should be less common. Some policies will not need specific attestation. Attestations should be date and time stamped and preserved with the version of the policy and should be easily accessible by oversight personnel.

## 4 — Policy Monitoring

After a policy is communicated, it enters the Policy Management phase. This includes:

- **Enforcement:** The policy then enters ongoing monitoring for enforcement and compliance within the organization. Specific controls are established and monitored to determine if the policy is being complied with. Incidents of noncompliance and violations are noted to provide feedback when the policy is next reviewed. The enforcement section of a policy is critical in that it defines levels of infractions and associated actions given the severity, repeat offenses and other criteria to support enforcement. These actions protect everyone involved, including the employee who violated it, the manager who imposed disciplinary action, and the company, so as not to exhibit signs of favoritism or bias.
- **Exception management:** While policies must be complied with, there are instances that arise in which the organization accepts noncompliance. These exceptions have to be documented and managed. An exception may be appropriate for a given time period or until a certain event occurs and must be reviewed to validate that the exception is still needed with appropriate levels of approval at each stage — approval, extension, and expiration.

## 5 — Policy Maintenance

The final phase of the Collaborative Accountability Policy Lifecycle Management is Policy Maintenance. This includes:

- **Review:** Every policy must have a regular review cycle. The review of a policy should be done at least annually. It is during the review process that the policy owner looks at the incidents of noncompliance and exceptions granted alongside the business requirements driving the policy. In this process, the policy is either authorized as-is for another management cycle, goes back into the Policy Development phase to update and approve the policy, or

# Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

is archived for retention. Review cycles can be initiated prior to a scheduled review, such as when a new law or regulation is issued and a policy change is needed to address the requirement.

- **Archival:** Every policy and every version of a policy must be archived for referral at a later point in time. The retention period for superseded or expired policies should be managed in accordance with the organization's document and records-retention policies and schedules. When an organization becomes aware of an incident, or a regulator has a question, it is necessary to have a full view into the accountability history of a policy — the owner, who read it, who was trained, and who attested and on what version of the policy at a particular date in the past.

## *Collaborative Accountability in Policy Oversight and Management*

Accountability in policy compliance and enforcement is made possible by three primary key functional capabilities:

- A well designed **Collaborative Accountability Policy Lifecycle Management** process.
- An organized **Policy Management Committee** to govern the oversight and guidance of policies and ensure policy collaboration across the enterprise.
- An individual assigned to the role of **Policy Manager** to assure accountability across the policy lifecycle to the standards, style, and process defined by the Policy Management Committee.

The Policy Management Committee provides the structure and connective tissue to coordinate and drive consistency across the organization and is comprised of team members that represent the best interest and expertise of the different parts of the organization. They leverage the knowledge, charter and the authority of the committee to benefit their business areas and, at the same time, benefit other business areas and the organization as a whole.

This organization carries out its execution responsibilities by leveraging the commonly developed and agreed-upon policies and technologies that form the Collaborative Accountability Policy Management program.

The policies and procedures contained within the system cover every aspect of the business addressed within the policy lifecycle management system which in and of itself, documents accountabilities, provides audit trails, links to internal and external mandates, manages training and attestations, and specifies monitoring activities, review cycles, enforcement policies and responsibilities over time.

## Technology Enables Collaborative Accountability in Policy Management

A strategy that addresses policy management through common technology architecture gets to the root of the problem, and delivers cost savings and efficiency. Common policy management architecture provides Collaborative Accountability and delivers on business agility, efficiency in human and financial resources, and effectiveness in meeting requirements.

The goal is to enable organizations to proactively protect the organization by aggregating and reconciling compliance with multiple regulations and requirements, the policies that result from them, and the processes that ultimately monitor and control them.

Policy management applications designed for Collaborative Accountability are intended from inception to manage all departments, divisions and related companies in one common framework. A well-conceived and soundly engineered policy management platform enables policies and procedures to be shared and managed across multiple entities (companies, divisions and departments) as needed, or restricted to just one entity when appropriate.

# Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

Business today requires a policy management platform designed for Collaborative Accountability that is context-driven and adaptable to a dynamic and changing business environment. Simply put, a Collaborative Accountability approach to policy management enables a better-performing, less costly, more flexible solution.

Technology issues that affect Collaborative Accountability include:

- **Organization management:** Policies apply to something within the organization — whether a business process, a physical asset, an information asset, a business relationship, or the entire organization. A policy management system needs the ability to model the organization and map policies to what they apply to in the organization.
- **Technology integration:** Policy management systems often require information from human resources, contact management, vendor management systems, and other sources to automatically maintain a single record. Policy management applications provide the capability to integrate with other systems.
- **Accessibility:** Policies are only of value if they are accessible. A policy management system must provide a complete system of record that any individual can log into and find the policies that apply to their role in the organization as well as required tasks, attestations, and training they have to complete. The system should be available in the official languages recognized by the organization, as well as support means for those with handicaps to access policies (e.g., vision impaired).
- **Workflow:** Workflow capabilities are a necessary component of policy management systems. The important consideration here is that the workflow functionality be flexible and integrated so the policies, people and process elements exist as part of the overall system. Automating workflow activities for policy and procedure management help the company to manage and monitor accountabilities and workloads associated with all phases of Policy Lifecycle Management and coordinate responsibilities and the contributions needed from distributed members of the process. Automated workflow management is also valuable for creating audit trails and provides metrics that show workloads, delays, assignments and other measures to help manage resources, cost and risk.
- **Task management:** A policy management system delivers the ability to track a variety of activities at different stages of execution. Policy management roles are responsible for drafting policies or procedures, providing approvals, handling exceptions, and performing policy reviews. Individuals receive notifications of training that have been assigned, policies and procedures that must be read and attested to, surveys they must complete, and other related activities. Policy management systems provide a collective overview of each individual's respective task list of outstanding work items and due dates, and prompts individuals with reminders of upcoming activities. It will also escalate overdue tasks to appropriate oversight and management personnel.
- **Content management:** Content management is a cornerstone of policy management. The content management component of the policy management system provides support for a range of document types as well as metadata (i.e., relevant dates, jurisdictions, programs, business units, vendors, status, and retention criteria). Content management capabilities provide check-in, check-out, version controls, audit trails, linking documents, and searches which enable users to easily complete their duties.
- **Training management:** Training management includes support for classroom, offsite or vendor training, e-learning programs, recorded presentations, simple document delivery and attestation, registrations and attendance completions. The challenge for companies is integrating learning management systems with policy management systems, which can be managed by adopting a policy management solution that provides training management. In this model, the courses, scheduling, attestations, and automatic assignment of policies and training based upon the organization matrix are integrated with workflow, task management and monitoring. Mature policy management systems automatically reschedule training if a policy is updated and assigns additional training if a person is promoted or changes roles that require additional training. This can be driven from the new hire or transfer process, or by the introduction of a new or changed policy, greatly simplifying administration and maximizing accountability and measurability.

# Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise

- **Notifications:** The most effective means of providing Collaborative Accountability in policy management includes notification capabilities. Notification is needed when policy authors receive word of a new work assignment. If the due date is nearing, they should receive a reminder notification. It might even be appropriate that if a task is overdue, an escalation notice is sent to management. If a person, or perhaps a whole business unit, need to read and attest to a revised policy, this must be communicated and can require reminders and escalation. Policy management systems provide configuration capabilities to customize messages, provide links to the task at hand, consolidate notifications if desired and help to enforce the goals, plans and accountabilities of the business. Notifications need to be able to integrate with the organization's e-mail system to deliver the messages and drive accountability.
- **Audit trail:** If it is not documented, it's not done. Every assignment, person, piece of content collected, developed, changed, distributed, archived, surveyed, trained, notified, and read should be accompanied by an audit trail to document every who, what, where, and when. The level of audit trail needed for policy management cannot be maintained with manual processes and ad hoc systems spread across an organization. When an incident occurs, an audit takes place, or a regulatory exam or investigation happens, you will be prepared with accurate and timely evidence of who did or didn't do what and when.
- **Interaction with other GRC applications:** Policies, training and communications serve to drive desired behaviors. However, there will still be investigations into business matters that, at some point, identify policy that needs to be changed or created. When incidents or investigations occur, it is important to identify not only what went wrong but to make changes that can prevent future similar occurrences. Noting within the investigation which associated policies were violated (and should be reviewed or revised) helps close the loop and drive continuous improvement. The investigations management system should integrate with the policy system to identify which policy was violated. Additionally, risk, control, and compliance applications are to be cross-referenced to policies they interact with.

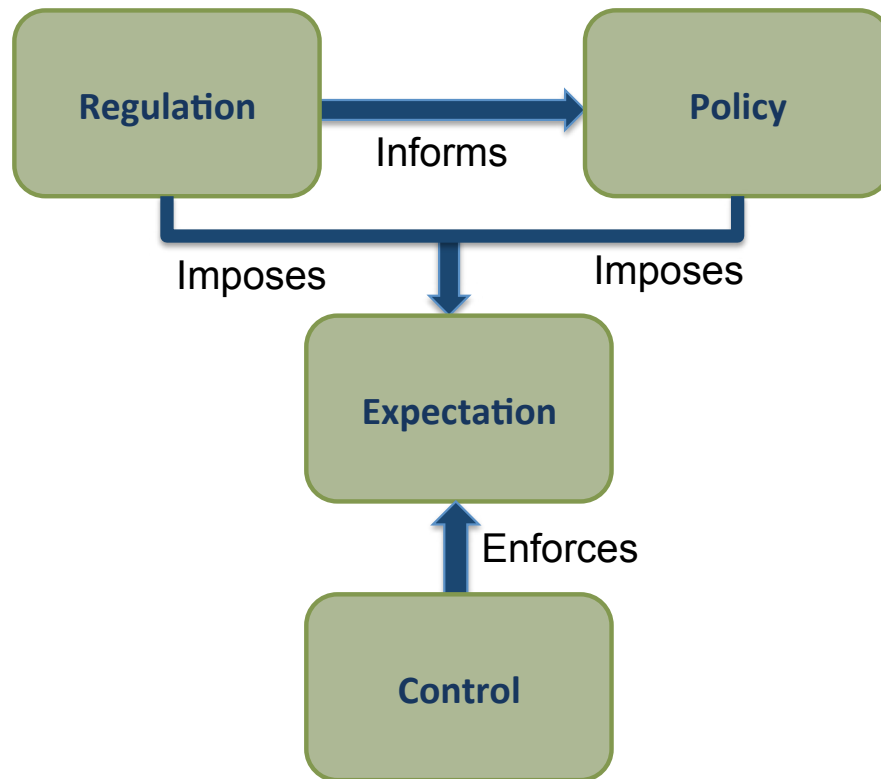
## Mitratech Provides Collaborative Accountability in Policy Management

Mitratech is a technology provider in the GRC market that Corporate Integrity has researched and evaluated. Through collaboration, accountability, and process automation, Mitratech's TeamConnect GRC eases the policy management burden by delivering agility, consistency, efficiency, transparency, and accountability to policy management processes. The company provides Collaborative Accountability for policy management using a strategic model called Regulation-Policy-Expectation-Control or RPEC (see Figure 2, below). When implemented via TeamConnect GRC, it manages the relationship among the four RPEC components:

- **Regulation:** Regulations include statutes or regulations imposed by government bodies; requirements from private industry associations, such as payment card associations; and obligations imposed by third parties, such as those imposed by healthcare providers on business associates.
- **Policy:** Regulations are translated into or inform one or more policies, which are then disseminated throughout the organization through a central medium or forum and are presented in a common view or format.
- **Expectation:** An expectation (or control objective) is a specific mandate that is identified in the applicable regulation and imposed by that regulation and the associated policy.
- **Control:** A control<sup>2</sup> (or internal control), broadly defined, is a mechanism to enforce a policy.

<sup>2</sup> The COSO Framework defined internal control as "a process, effected by an entity's board of directors, management and other personnel... [that] is designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations." See <http://www.coso.org/resources.htm> (last visited August 10, 2010).

# Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise



**Figure 2: The Regulation-Policy-Expectation-Control (RPEC) model.**

Even enterprises that are not in highly-regulated industries are subject to regulatory and contractual obligations, and the interplay among the RPEC components can be fiercely complex. Collaborative Policy Lifecycle Management (PLCM) uses a common backbone to unite policy management contributors, giving all parties a common view of the state of a given policy, along with potential and existing regulatory changes that directly impact and inform those policies. Policy managers use RPEC to automatically flag the list of impacted policy areas for review and to assist in the translation of those changes into expectations. TeamConnect's event forensics function provides accountability by enabling auditors to determine who was responsible for particular policies and whether they properly addressed changes in regulatory obligations in a timely manner. Finally, team members responsible for the creation and maintenance of controls can determine what changes are necessary, if any, to address changes in expectations. A native reporting capability enables auditors to evaluate the effectiveness of those controls, providing accountability and assisting in their improvement.

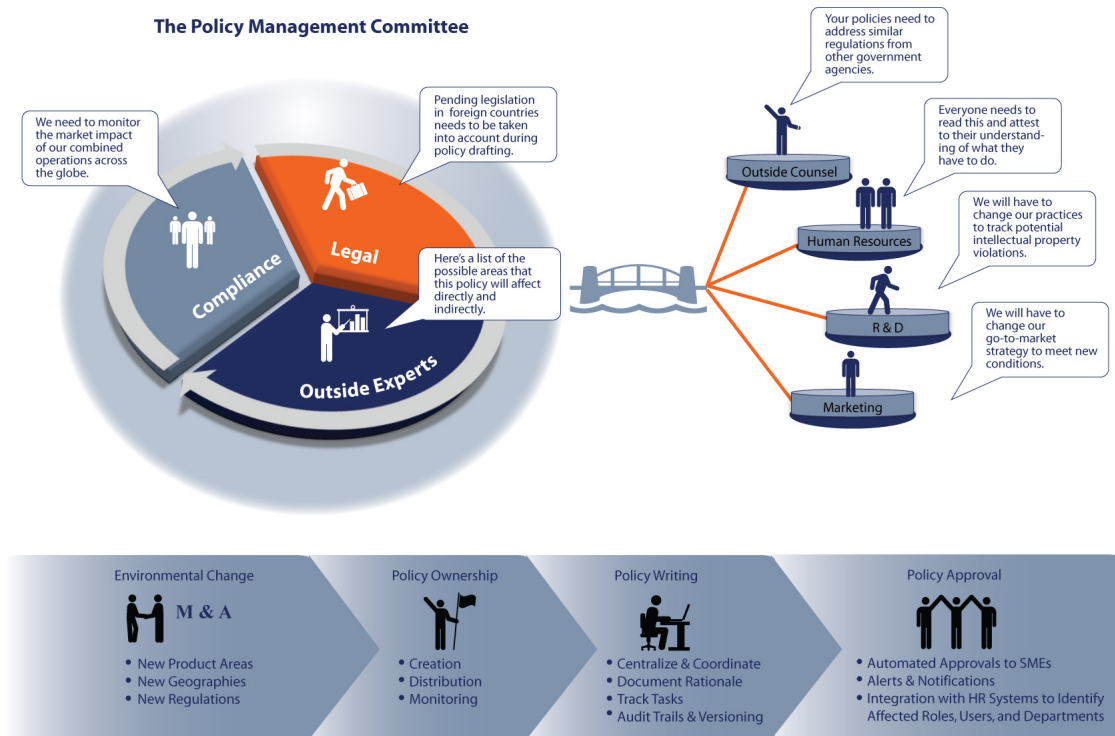
The value of RPEC lies in its provision of a comprehensive and extensible framework to address all aspects of enterprise governance, risk, and compliance management. The power of using RPEC becomes apparent when an enterprise has multiple regulations from different functional areas that can be addressed with the same policies or that results in the same or similar expectations. By giving visibility to all expectations as a whole, economies of scale can be achieved by building solutions that fulfill a variety of similar or related expectations.

## *RPEC Unites GRC Efforts and Optimizes Policy Management Across Teams*

Companies that wish to manage policies using a process that is automated, repeatable, and defensible employ virtual policy lifecycle management committees comprised of members from legal, compliance, and risk management departments to address every component of PLCM and to determine how policies interact with other RPEC components. Such committees or teams implement PLCM for the enterprise and extraprise (players outside the corporate firewall — outside counsel, experts, insurance carriers, and business partners) using Collaborative Accountability in the following way:

# Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise

- **Analyze environmental changes:** Environmental changes — changes in the corporate, regulatory, and risk environments — are identified and analyzed best through the use of a regulatory intelligence (RI) system. An RI system is a critical component of any policy management system and is used to analyze the many streams of environmental data. When necessary, it flags potential issues for review by the policy managers. Policy managers can then collaborate on appropriate issues with other members of the PLCM team, using workflows and task management, to determine when a new policy needs to be written.
- **Define and categorize policies:** A threshold task for defining and categorizing policies is determining policy scope, which asks the question, “What regulation is driving this policy and to whom does it apply?” Once complete, the PLCM team defines a hierarchy and structure to manage policies across the organization, inventories their policies, and structures them in an interactive policy and procedure dashboard that is available to and accessible by the entire organization.
- **Collaboratively develop and approve new policies:** Organizations create new policies with regularity. This requires a defined process for writing the policy and going through stages of policy draft approval and review, so that the policy can be published. PLCM teams are linked together with stakeholders through a centralized platform that enables a complete view of policy drivers, environmental changes, and policy goals. This forum also tracks the task list at each stage, greatly speeding the development process as well as documenting the rationale and responsibility for policy decisions. Centralized access to existing policies and content management tools help ensure standard formats and language across policies. Audit trails and versioning keep a complete history of the policy throughout its stages, while alerts and notifications keep policy creation on track.



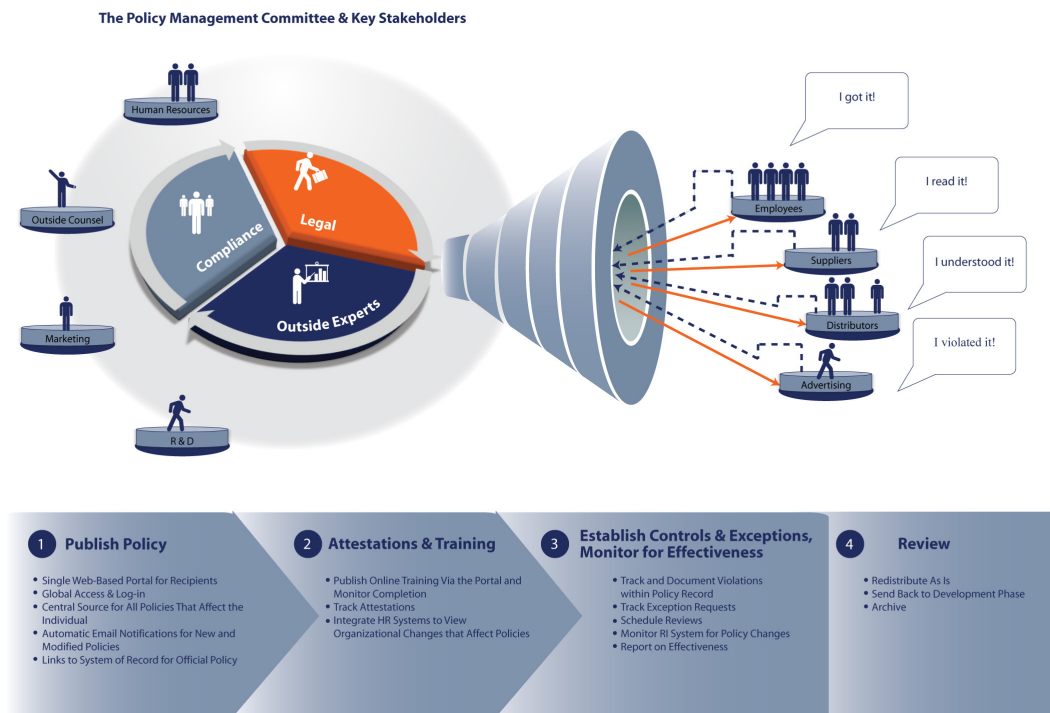
**Figure 3: Successful Policy Lifecycle Management requires participation from the entire enterprise, including input from outside parties.**

- **Establish principle relationships among RPEC components:** A particular regulation may precipitate a list of policies to address multiple implications, and those implications will precipitate a longer list of expectations that map to responsible parties. An internal control team, distinct from the PLCM team, establishes the necessary phys-

# Collaborative Accountability in Policy Management: Effectively Managing Policies across the Enterprise

ical, technical, and administrative controls for enforcing those expectations and metrics for determining control effectiveness. The team maps those controls to the expectations within the system, using guidance documents that are in many cases utilized industry-wide. The entire RPEC map then lives within the system and is available for publishing in a variety of forms throughout the organization.

- **Publish policies:** Policies and their attendant expectations are then published to responsible parties throughout the enterprise and to a collection of external parties using a common format that is available globally via Web browser. The need for integration with the organization's technology infrastructure cited earlier is perhaps illustrated best here. For example, the attestation Web portal enables all responsible parties to acknowledge receipt of the policy and expectations, and to attest to their understanding of their duties and consequences for noncompliance. Additionally, training management occurs directly within the system. Workflow and task management capabilities ensure that all responsible team members complete training. Attestation for training completion is tracked within the system and is both reportable and auditable. Finally, integration with HR systems ensures that training administrators are aware of any organizational changes (new hires, promotions) that result in the need to schedule additional trainings for any particular policy.



**Figure 4: Policy management integration with the organization's technological infrastructure is crucial for global policy publishing and monitoring as well as policy-specific training and compliance enforcement.**

- **Monitor and maintain:** Policies require regular review to assure they remain relevant to the organization. Changes in regulatory expectations are the most likely driver for policy changes, and the task of monitoring for potential changes falls to the policy managers, who utilize the regulatory intelligence (RI) system as part of the review process. Policies that require regular reviews can be scheduled within the system, with alerts and notifications sent to the policy manager as the new cycle approaches. If a policy needs to go back to the Policy Development phase, all appropriate parties once again collaborate on policy creation with the policy manager assigning appropriate roles through workflow and task management capabilities. The policies and attendant expectations can be updated directly within the system, if necessary, as well as changes in the control infrastructure by the appropriate team. A complete audit trail tracks the policy history.

# Collaborative Accountability in Policy Management: *Effectively Managing Policies across the Enterprise*

- **Test for effectiveness:** The reporting functions are used periodically to test for effectiveness and reductions in violations and resulting sanctions. If a violation or negative event takes place, the event forensics function can be used to unwind specific transactions to determine with precision what happened and who the responsible parties are.

All of these steps use three core functionalities:

1. Linking team members, wherever in the world they might be, into a virtual forum that offers the same view of the same data, such as RI, policy hierarchies, and the relationship among RPEC components.
2. A means to review and examine PLCM-related processes, controls, and events.
3. A secure infrastructure that can unite the enterprise and extraprise, and safely moderate access to all team members, minimizing the company's exposure to threat.

These components form the foundation of Collaborative Accountability.

## Components of Collaborative Accountability

Collaborative Accountability enables Policy Management Committees to realize PLCM and other teams to realize their respective efforts through the establishment of three distinct yet interrelated components:

1. **Enterprise and extraprise teamwork:** Many, if not most, enterprises today function in a geographically dispersed environment yet require close cooperation in order to fulfill their missions. That same close cooperation is necessary for GRC teams to manage policy lifecycles and for the rest of the enterprise to meet policy-driven expectations. The enterprise team must have access to much of the same information as others, and is subject to the same expectations. Collaborative Accountability makes extraprise participation transparent to the rest of the team.
2. **Event forensics:** Event forensics allows an organization to unwind an event or transaction in order to determine who did what, and when, and perhaps who knew what, and when. Having such capability built into PCLM is crucial for identifying details of a violation and the attendant circumstances, such as the failure of a particular control. Event forensics is a powerful tool for promoting accountability for all enterprise and extraprise team members, and offers exculpatory potential for the enterprise in cases where another organization was at fault. This feature distinguishes TeamConnect from mere collaboration tools.
3. **Flexible security:** Team members require access to certain types of information to perform their respective duties, yet access must be limited to protect the integrity of the enterprise. Outside counsel, for example, should be accessing only company matters to which they are assigned. Furthermore, members of the firm that have a more limited role, such as paralegals, should have access narrowed further. TeamConnect uses a flexible role-based access control (RBAC) security model that can limit access down to the field level according to predefined roles, and create exceptions or additional restrictions using business rules.

Collaborative Accountability represents a fusion of the features of modern groupware tools with granular tracking of tasks, events and communications and is enabled by multifaceted access control.

### *Corporate Policies No Longer in Disarray*

Collaborative Accountability addresses the many problems surrounding effective promulgation of policies, such as ineffective policy structures, lifecycle management, communication, and accountability. Corporate policies are no longer in disarray because their location, content, ownership, lifecycle phase and relationship to other RPEC components is securely and dynamically managed by responsible teams with a holistic view of policy and the implications of policy changes

and violations. Policies and policy-driven expectations are pushed out to team members regardless of geographic location and attestation to the members' understanding of them is checked using periodic reporting. In the event that a policy failure occurs, accountability for all involved is achieved using event forensics to unwind the event or transaction in question and to determine what went wrong. As such, event forensics can apply in a variety of contexts and has strong exculpatory potential for the entire organization.

Effective PLCM is crucial for the modern organization to function within the bounds of the legions of mandated obligations, such as the FCPA, information security statutes, and the federal sentencing guidelines. It is also crucial for self-imposed obligations, such as those agreed upon with business partners. A Collaborative Accountability approach to policy management addresses the principle challenges of managing the litany of policies needed to function within these bounds — uniting team members from around the world, giving them access to the information and tools they need to carry out their duties, and doing so in a way that protects the organization from harm.

## About this Paper . . .

This white paper is brought to you by Mitratesch.

Mitratesch provides market-leading Collaborative Accountability Applications for businesses and their trusted partners. With team-oriented domain applications in legal process automation, governance, risk, compliance and security, Mitratesch's TeamConnect® Collaborative Accountability Suite improves transparency of financial reporting, reduces exposure to risk, sharpens operating discipline, improves information security and the efficiency of enterprise processes.

Our Collaborati browser application also meets the accountability and collaboration needs of proliferating extraprise teams, wherein vendors, partners and service providers often have to be included in sensitive teamwork projects such as electronic billing, legal hold and collaborative budgeting, or those which expose your business to liability. To learn more, visit [www.mitratesch.com](http://www.mitratesch.com).

## About Corporate Integrity . . .


Corporate Integrity, LLC is a GRC strategy advisory firm providing leadership in education, research, analysis, and advisory services by monitoring the challenges and trends of the business roles accountable for corporate governance, enterprise risk management, and compliance (GRC).

Through ongoing research, interactions, and analytics Corporate Integrity is the authority in understanding how organizations can foster a culture that "walks the talk" - where integrity is central to governance, risk, and compliance (GRC) practices. Corporate Integrity educates organizations - and GRC professionals within those organizations - on achieving sustainability, consistency, efficiency, and transparency in their corporate GRC practices so they maintain a position of integrity aligned with corporate values and business performance..

## About Michael Rasmussen . . .

*J.D., CCEP, OCEG Fellow: Risk & Compliance Lecturer, Writer, & Advisor*

Michael Rasmussen is an authority in understanding Governance, Risk, and Compliance (GRC) processes. He is a sought-after keynote speaker, author, and advisor on risk and compliance issues around the world and is noted for being one of the earliest advocates for GRC.



With more than 15 years of experience, Michael's objective is to assist organizations in defining GRC processes that are efficient, agile, effective, accountable, and transparent.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, and currently serves on the Leadership Council of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in "Governance and Compliance: Saving the Planet and the Corporation." Most recently, in October 2008, he was recognized as a "Rising Star in Rocky Times: Corporate America's Outstanding Executives Under the Age of 40."

During his career, Michael has worked in market research, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and 'top analyst' at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael's educational experience consists of a Juris Doctorate and a Bachelor of Science in Business. Michael is currently in the Master of Divinity program at Trinity Evangelical Divinity School.