

## Preface

The *Policy Management Process™* and the associated *Effective Policy Management™ Best Practice* were developed in 2001, before the large accounting scandals became unfortunate news stories. Reaction from the government and securities industries was swift, and a new era of corporate governance was born. The words most commonly associated with corporate governance today are “Sarbanes-Oxley”, the Act designed to strengthen corporate governance for publicly traded companies in the U.S.

This white paper was first published in June 2002, after many scandals had surfaced but before the Sarbanes-Oxley Act was issued. At the time, the white paper provided a practical, logical process that companies could implement to help manage their policies and procedures. With this second edition, we update the best practice steps as they relate to the Sarbanes-Oxley requirements for internal control documentation and testing. Companies that are not subject to Sarbanes-Oxley will still find the original best practice steps useful for their internal policy and procedure management process.

Throughout this white paper, the term “policy” is used to represent all of the policies, procedures, internal controls, and any other reference information that employees need to understand and follow, not just the literal “policy” documents.

## Introduction

Today’s corporate crisis is destroying shareholder wealth, bankrupting companies, and putting tens of thousands out of work. The list of companies – Enron, WorldCom and Adelphia – will undoubtedly keep growing.

What is the crisis? The loss of investor confidence caused by accounting errors, shareholder lawsuits, and criminal investigations. These problems have always existed, but now that they are valued in “billions” they have become front-page news.

Many factors contribute to these types of problems – greed, fraud, personal pressure, even honest mistakes. However, underscoring all of these problems is a *fundamental lapse in clearly documented and communicated company policies* – how a company sells its goods and services, how it hires and manages employees, how it deals with vendors and makes expenditures, and how it accounts for those transactions.

*Policy Management* describes the activities necessary to document a company’s rules, illustrate how specific situations should be handled, and communicate this information to employees. While this may appear to be a basic concept, management, audit committees and auditors are waking up to

the fact that their companies have been operating in spite of a significant lack of clear company policies.

Most companies have experienced the *Negative Policy Cycle* caused by ineffective policy management: employees do not take the time to read company policies because the policies are outdated, and managers do not take the time to update the policies because employees do not read them. This negative cycle is the direct result of inadequate policy management.

Breaking this cycle is not simply a matter of updating policies and punishing those who don’t follow them. Discipline is required at every stage of policy management, from creation and issuance to communication and review.

Whether you are a small, entrepreneurial businesses or a Fortune 1000 company, the following 10 key steps will help your company develop an *Effective Policy Management* system for all of your departments and all of your activities.

**Sarbanes-Oxley Update:** While this introduction was written almost two years ago, the points are still valid. The accounting scandals showed the world that even the largest companies could be operating without proper internal controls. Sarbanes-Oxley forced companies to begin doing what they should have been doing all along: document, communicate, and continuously test and monitor an effective internal control structure.

## The Policy Management Process and Effective Policy Management Best Practice

The *Policy Management Process* treats policy and procedure information as a cycle, where every element of the cycle is critical to the operations of the cycle.



Within the steps of this cycle, there are 10 best practice steps that companies can benchmark their existing processes and existing technologies against.

1. Delegate responsibility
2. Be clear and concise
3. Document changes
4. Control issuing authority
5. Organize logically
6. Provide central access
7. Communicate updates timely
8. Document and test compliance
9. Encourage feedback
10. Force periodic review

The remainder of this white paper describes each step, with a Sarbanes-Oxley update at the end of each original section.

## 1. Delegate responsibilities and empower

While only management should have the authority to issue policies, *authoring* those policies can be delegated to other employees. For example, in the human resource department the manager should delegate policy sections to the staff to author. Delegation provides a number of benefits:

- employees feel empowered to suggest improvements
- the exercise can improve writing skills
- more people can provide different perspectives on the same activities
- policies can be completed faster

In addition to assigning staff authoring responsibilities, middle managers can also be assigned to review draft policies. This delegation provides new learning experiences for these middle managers, and increases the efficiency of the policy development process.

When managers do not delegate these responsibilities, the manager becomes the bottleneck and it becomes less likely that a set of quality policies, or any policies at all, will be completed.

**Sarbanes-Oxley Update:** Companies discovered that the cost of Sarbanes compliance was significantly more than they expected. One of the main cost drivers was the effort necessary to understand all of the company's processes and technologies, and then document the related risks and mitigating controls. Efficient documentation processes through a controlled delegation and review function has enabled the most successful companies to reduce the overall cost and ensure that documentation and testing deadlines are met.

## 2. Make the policies easy to read and understand

A policy might include valuable and important information, but if it is not easy to read it is unlikely that the reader will find what they are looking for.

The longer the policy, the less useful it will be to the readers that need it. For example, instead of a 20-page "Capitalization Policy" that includes every aspect of managing capital assets, create separate policies for

- the capitalization and approval process;
- periodic review of those assets
- the disposal or write-off process
- the depreciation rules for different asset types

A shorter, more concise policy will better direct readers to relevant information. Shorter policies can also be "shared" more easily with other departments, promoting communication across departments and sharing work more effectively.

For example, the above policies might have relevance in these other areas:

Capitalization and approval	➔	Budgeting
Periodic review	➔	Internal audit
Disposal or write-off	➔	Tax planning
Depreciation rules	➔	Monthly closing process

One long capitalization policy could not be shared among these activities and departments as easily as the four separate policies could.

**Sarbanes-Oxley Update:** An early decision companies and auditors needed to make was how to document their processes and controls and how detailed those documents should be. While the above recommendation of "shorter policies" provides for easier organization, faster acquisition, and better long-term management, documents can also be *too* short. A one-sentence description of a control will likely be inadequate, but a one-sentence control buried in a 4-page detailed desk procedure will be difficult to identify.

One successful documentation approach has been to consider whether a newly hired employee working in the relevant department could read the control document *and* supporting information for the first time and understand how to follow the control. Limiting a control document to "we reconcile our bank accounts" without any supporting information will not be

enough information – for your external auditors or for your own employees. However, with greater documentation comes the need to ensure that the critical controls are easily identified and the documentation is standardized.

### 3. Track all policy changes – when, why and by whom

A clear document trail of policy changes is important when questions or disputes arise relating to compliance with certain policies. Effective policy management requires the discipline to track all changes and record who made each change, why they made the change, and when. A company should clearly communicate to its managers that part of their policy management responsibilities is to clearly document policy changes.

This process can also discourage unethical behavior. For example, in a company with strict adherence to documented policies, the accounting staff will follow only the documented accounting policies. Changing an accounting policy requires a documented reason for the change, and internal audit, the audit committee, the board, and/or the external auditors will likely review those reasons. If the Controller wanted to manipulate earnings through accounting tricks, this process would discourage those actions.

This example shows not only the benefit of a strict policy for documenting and reviewing policy changes, but also gives an example of how documented policies – and a culture of following those policies – provides a solid internal control structure.

**Sarbanes-Oxley Update:** One of the most important requirements has also been one of the biggest deficiencies discovered in many software applications marketed as Sarbanes-Oxley tools. Change history is critical during the documentation stage when different people are creating and reviewing each document. Without a proper audit trail the documentation workflow lacks the proper controls to operate effectively, and documentation responsibilities default to a much smaller group than could otherwise be used.

After initial Sarbanes compliance, one of the most important management reports is a change report that can be used to understand the new controls, deleted controls, and control changes that have been implemented, and to evaluate necessary testing and/or disclosure of those changes. Unfortunately for some companies these requirements will not be apparent until after completion of the first year's compliance, and will require at that time implementation of new processes and/or new content management tools.

### 4. Control who has the authority to issue policies

Management should be the only ones authorized to issue policies. An appropriate review should be conducted before policies are issued, based on the nature of the policy and determined by the manager. For example:

- The Chief Financial Officer should be authorized to make and issue changes to the monthly closing process without other levels of review... but a new accounting policy should be reviewed by the company's auditors.
- The Human Resource Director should be authorized to update the hiring packages for new IRS tax forms... but changes to the Employee Manual should be reviewed by the company's legal counsel.
- The Treasurer should be authorized to update the internal policies for consolidating and reporting on investment activity... but the company's Investment Policy should be reviewed by the Board of Directors before it becomes effective.

A process that requires every new or changed policy to be reviewed by the Board of Directors or multiple levels of management will likely be too much control and therefore too inefficient. Management should have the experience and have earned the responsibility to determine what the appropriate review levels are for their new or changed policies. In instances where they have any doubts, they should know to consult the company's legal counsel to determine whether other reviews are necessary.

Internal audit, management or Board review of new policies and policy changes (as discussed in step 3) on a periodic basis will act as an additional control to ensure policies are appropriate and to discourage unethical behavior.

**Sarbanes-Oxley Update:** An efficient documentation process that relies on delegation to speed completion must have controls in place to limit publishing authority. Companies are falling into the dilemma described above for the Sarbanes documentation – their manual process requires *too few* people to publish controls making the process inefficient, or the software they are using allows *too many* people to publish controls because of inadequate authority level restrictions.

## 5. Organize policies in a logical way

Organizing policies may seem a simple task, but in fact most companies do a poor job of organization. Some examples of poor organization schemes include:

- Alphabetically
- In order of issue date
- By policy number
- No method at all

Organizing policies logically adds value to those policies. The right organization will depend on the nature of the policies:

- Accounting rules can be organized by balance sheet and income statement account
- Human resource policies can be organized by activity – hiring, compensation and benefits, personnel review, termination
- Sales policies can follow the sales cycle – marketing, processing leads, selling, delivering, and collecting payment

A well-organized set of policies will be easier to navigate and search through. Organization also improves the overall management of policies, as gaps or inconsistencies between policies can be more easily identified when they are logically organized.

**Sarbanes-Oxley Update:** Most Sarbanes-Oxley project teams have already concluded that risks and controls must be organized by account *and* by process. Those teams must also be able to report and filter on specific documents they want to view – only high significance risks, for example, or only controls impacting the IT area. Logical organization will provide many different ways to filter and find data, and will also provide easier employee access promoting process and other operational improvements in addition to greater control compliance.

## 6. Provide a central place to access all policies

Clear, well-organized policies provide little benefit if employees cannot access them. The greater the difficulty in finding relevant policies, the less likely an employee will take the time to look.

In this age of technology, companies can provide electronic copies of their policies via their Intranet site, portal, or policy management software. Without technology, hardcopy versions of policies can be provided, but for larger companies this can be a costly proposition. In this case a cost effective solution is to identify locations within the office space, plant floor, or distribution warehouse to store policies for easy access.

**Sarbanes-Oxley Update:** In determining the best way to publish internal control information, ease of use and technology platform are two important considerations. Ease-of-use will include such basic functions as searching, which makes finding information easier. In fact, the lack of a search capability by itself may keep employees from even bothering to look for information. Most companies choose web-based tools that can be easily incorporated into their Intranet sites so that employees have one central place to access both their controls as well as their other policies and procedures. The more seamless the communication of internal controls can be, the more of an effect they will have. If they are located in one place, easy to access, find, and read, then employees are more likely to follow them.

## 7. Communicate new policies and policy updates as they occur

New policies and policy updates should be communicated on a timely basis. In addition to ensuring that employees are operating with the most relevant information, timely communication of policy changes reinforces a company's culture of taking policy management seriously.

When policy changes are communicated in a timely manner, less time will be wasted addressing employee questions later. For example, a company's switch to a new 401k provider usually requires a number of employee actions. New paperwork needs to be completed, and in some cases a distribution check is sent to the employee that must be deposited with the new provider. There may also be changes in how 401k contributions are made, what investment options are available, or what the new hire eligibility standards are. There is also typically a delay during the switch, when employees are unable to make any changes to their current investment decisions.

Communication of the aspects of the change, what employees need to know about the change, and the answers to their expected questions will limit the number of questions asked by phone or by email and therefore limit the time spent answering those questions – in some cases answering the same questions over and over again.

**Sarbanes-Oxley Update:** Communication is a critical step in the management of internal control information – it is one of the six basic steps of the Policy Management Process. Still, many companies have not yet considered how they are going to communicate the thousands of pages that they have been creating for their Sarbanes compliance. For long-term compliance, there must be a process to communicate both the controls that employees are supposed to follow, as well as the control updates when they occur. Companies that have implemented technologies that were not designed for enterprise-wide use will have to develop their own

communication plans for providing employees with updated information.

## 8. Document and test employees' review and compliance with policies

There are typically a few policies that employers force their employees to review and sign attesting to their compliance, such as an employee handbook, a sexual harassment policy, and a code of ethics. However, these policies represent a small fraction of the total policies that a company would expect its employees to follow.

The more documentation an employer has for employee acknowledgement and compliance with policies, the better protected that employer is.

The company's policy for documenting employee compliance will depend on what type of policy management infrastructure they put into place. For electronic versions of policies, technology can be used to record which employees viewed which policies, proving that the employee did have knowledge of the appropriate policy in case of a later dispute.

Absent technology, manual procedures can be put in place to document compliance. For example, the accounting department could distribute complete closing and reporting guidelines semiannually to all location and division controllers and collect signed acknowledgements of receipt. Updates would be distributed as necessary, but acknowledgement of those updates would take the form of the next semiannual publication date.

In addition to acknowledgements, testing procedures must be used to ensure continued compliance with company policies. The internal audit group, external audit firm, and/or the company's compliance department should complete random cycle tests as well as more frequent tests of high-risk areas.

**Sarbanes-Oxley Update:** Compliance with internal controls is typically done both *independently* and through *self-assessments*. Independent testing is a critical element of Sarbanes compliance – both internal independent testing to validate that the controls are being followed, and external audit independent testing to support the auditor's opinion. Self-assessments support independent testing by having many individuals periodically acknowledge that they have been following certain controls and communicating any control issues that have occurred.

## 9. Provide a feedback mechanism for employee questions and comments

In some companies a culture exists that policies are "fixed and final", and not open to suggestion. Management dictates these policies, and employees are simply instructed to follow them.

However, while policies are in fact communicated down from management throughout the organization, no one is in a better position to assess the accuracy and completeness of those policies than the employees following them. A culture that does not readily accept employee comments will likely produce a substandard set of policies, far from perfect and potentially not even used. Worse, a culture that doesn't enable employees to easily ask questions when they don't understand a policy or can't find reference to their specific situation may result in those employees making the wrong decisions.

Effective policy management requires a feedback mechanism to enable employees to post questions and suggestions to improve policies. Policy management technology can be used to integrate these questions directly into the electronic versions of the policies; absent this technology, email can be used when a clear procedure for posting and directing questions is understood. For the most non-technical organizations, simple printed question and suggestion forms can be distributed to employees, with central collection points for general comments and with specific managers listed for more urgent questions.

**Sarbanes-Oxley Update:** Feedback mechanisms are used for two distinct purposes: first, to identify gaps in controls and procedures or improvements that can be made to processes, and second, to report any known or suspected issues. The first purpose provides for the continuous improvement of a company's processes and internal control structure, and ensures that controls and procedures are not just dictated from the top down but can originate from the bottom up. The second purpose is part of general corporate governance and is also a legal requirement: providing a means for employees to report anonymously issues that they become aware of. Supporting both is necessary to maintain proper corporate governance.

## 10. Force periodic review and update of all policies by their respective managers

Unfortunately, with the speed of change in today's business world, policies can have a very short "shelf life" before becoming outdated.

A key element of effective policy management is an ongoing commitment to periodically review and update all policies before they become outdated. Once the policies become outdated, the *Negative Policy Cycle* described in the introduction will occur and require more effort to break.

All policies should be reviewed on a recurring basis, regardless of the policy, and the review dates should be decided when the policy is first created. Based on their content certain policies might be reviewed every 6 months, for example, with others being reviewed annually. The review dates should be chosen so that not all policies are reviewed at the same time, to spread out the time commitment.

Adequate controls are necessary to identify and report managers that are not complying with this responsibility. For managers, ensuring relevant and updated policies should be a factor in their annual evaluation.

**Sarbanes-Oxley Update:** After all of the effort and money put into Sarbanes compliance, a company needs to ensure that the “fire drill” does not occur every year and must implement a strict process of continuous periodic review of all information. Of course a company is going to periodically test its internal controls, but that might represent a small fraction of the total documentation that is created. What about all of the flowcharts, memos, policies and other information? If you do not put in place, or rely on technology to monitor, a process forcing the expiration of pages without periodic review and signoff, then eventually all of your documentation will need to be redone.

## Conclusion

Most companies have never invested the time to adequately document and communicate their policies and procedures. The common belief has been that the cost required to follow the above 10 steps did not justify the benefit. Operating efficiencies were the only tangible benefit to compare the cost to; the intangible benefits of reduced risk are difficult to value and typically were not included in this evaluation.

The current crisis is changing the cost/ benefit equation. For public companies in particular, the equation has shifted substantially – the intangible benefits may not be any easier to calculate, but the magnitude of stock price collapses (temporary or permanent), lawsuits, and criminal investigations is showing that the ability to avoid these risks clearly has some value. In some cases, the benefit in this equation is not just a benefit, but also a requirement – from investors, stock exchanges, boards of directors, audit committees, auditors, and government agencies. Companies that ignore these risks will face substantial business and personal penalties if it is later shown that the opportunity to protect their company was ignored.

Protecting your company does not require significant expenditures or monumental efforts; proper discipline following these 10 steps combined with the benefits of the right technology can create an effective policy management system

that will significantly reduce the risk that your company becomes the next scandal.

**Sarbanes-Oxley Update:** As every public company is aware, proper policy and procedure documentation is no longer an option but a requirement. The new regulations have “teeth” as well, in the form of external audit opinions, and given the impact that Enron had in the downfall of Arthur Andersen external auditors are not expected to be very flexible in their evaluations of their client’s internal controls.

Because of the tight deadlines imposed by Sarbanes-Oxley, many companies have not spent sufficient time planning for the long-term, and have instead focused only on their current year compliance efforts. As a result, the documentation processes that they are currently following, and the audit testing tools that they have selected, may not follow the Policy Management Process which would likely compromise their long-term maintenance, update, and communication of this information.

## About the Author

Rocco Tarasi is a Certified Public Accountant, a National Director with Resources Global Professionals, and is the author of the Policy Management Process and Effective Policy Management Best Practice. His early career as an auditor in the “Big 5” was spent reviewing and improving policies for companies ranging from startup to Fortune 1000. He was CEO and founder of Snap River Technologies, a software company that developed the policyIQ® policy management system. In July 2003 Snap River was acquired by Resources Global Professionals and he joined to manage all policyIQ sales. He can be contacted at rocco.tarasi@resources-us.com.