MITRATECH

MAKING THE BUSINESS CASE FOR A POLICY MANAGEMENT SOFTWARE SYSTEM

Show your senior management and board how a policy management system can reduce risk, drive efficiencies and make your entire company more compliant.

OVERVIEW:
Making the Business Case

If you're reading this paper, chances are that you've recognized the need for a robust, end-to-end policy management software system for your company. That's not surprising.

It seems that every day brings news relating to corporate compliance Regulators are continuously issuing new or updated regulations and specific guidelines for compliance. At the same time, companies are facing the risks of noncompliance: increasingly punitive fees, damage to their reputations and disruption to their business. In this environment, businesses face a threefold challenge:

- Posting policies and hoping employees read, understand and follow them is insufficient to meet today's stringent regulatory demands as well as mitigate legal,operational and other risk.
- Taking a step further by attempting to manually track employees' review of and compliance with policies is time-consuming and expensive — especially for growing companies and businesses with multiple locations.
- As laws and regulations rapidly evolve, policies across the entire company must keep up, creating a never ending cycle of policy review, revision and distribution to employees.

THE BOTTOM LINE: A passive approach to policy management is a thing of the past.

Meeting today's stringent demands for regulatory and internal policy compliance while operating efficiently requires technology that offers the ability to easily and accurately manage, monitor and report on the company's policies and employees' adherence to policies. Using a technology-enabled approach to policy communication, sign-off, testing, tracking and reporting helps to reduce risk, drive process efficiencies and ensure compliance across the enterprise.

But how do you convince your company's senior management and board of directors that it's time to invest in a policy management solution?

This paper includes information, tips and examples to help you build and present a business case that demonstrates how implementing a policy management software system will help your company manage policies more efficiently and prove that your company has an effective compliance program.

TODAY'S Regulatory Environment

Your company's board and senior management likely have a sense of today's regulatory landscape. But to help them truly understand the value of a policy management system, it can help to start with a discussion of the regulatory environment. Here are a few points to prepare you for the discussion:

Regulatory Demands:

Businesses worldwide are facing an increasing number of regulations, changes to regulations and enforcement of regulations including the EU General Data Protection Regulation (GDPR), Foreign Corrupt Practices Act (FCPA), PCI DSS, and the Sarbanes-Oxley Act. Here's an example: According to a 2017 Boston Consulting Group report, regulators levied fines of $321 billion on banks globally since the 2007-2008 financial crisis (through the end of 2016). The same report estimates that banks must track an average of 200 individual regulatory changes per day on a global scale.

And that's just the banking world. Businesses of all kinds are developing extensive internal governance policies to help comply with regulations for their specific industries.

Internal Policies Across the Company

The need for companies to develop and manage policies extends beyond the regulatory compliance world to areas across the company, including legal, human resources, operations and IT departments.

Here are a few considerations:

Risk mitigation — Employees are a company's greatest asset, yet they can also represent the highest risk to the company's future. For example: Dell's 2017 End-User Security Survey found that 72 percent of employees are willing to share sensitive, confidential, or regulated company information. Simply publishing policies and relying on employees to read and adhere to them opens the door to risks including litigation, employee incidents, data breaches — the list goes on.

Certifications and accreditations — Most certifications and accreditations, such as ISO, SOC 2 and PCI DSS are based upon processes and procedures. They require a company to answer questions such as: Do you have processes to ensure your employees are working in a safe environment? Do you have processes in place to stop people from accessing data they shouldn't? A company must not only have policies and procedures in place, but also must be able to track and prove that they have them in place to be able to gain and maintain certifications and accreditations, which often are required for companies that seek to provide assurance to prospective clients that they are a reputable and secure vendor.

Board assurance — Based on risks and regulatory demands, a board of directors will often require that the company they oversee be able to demonstrate that it has both a clear strategy and a means to operate ethically and meet governance obligations to customers, shareholders and staff. This requires a company to be able to provide the board with visibility into:

- Employee acknowledgement, understanding and adherence to key policies

TODAY'S Regulatory Environment

- Status of third-party policies and procedures
- Status and trend data of policy communication initiatives

The Cost of Noncompliance

In addition to reviewing the regulatory landscape, it is critical to help your senior management and board understand the far-reaching cost of noncompliance. A survey conducted by the Ponemon Institute and released in 2011 concluded that the cost of noncompliance is almost three times higher than the cost of being compliant. Likely, the cost of noncompliance today is even higher. Regulator fines are at all-time highs and are pushing fines and penalties up constantly. If that weren't enough, the cost of compliance extends beyond fines.

The Cost of Noncompliance Includes Three Areas:

Fines and penalties — Companies often face fines when a federal or industry-regulated compliance breach occurs, and the fines can be steep. Just a few recent examples:

- Singapore-based Keppel Offshore & Marine and its wholly owned U.S. subsidiary will pay a combined $422 million criminal penalty to resolve charges in the United States, Brazil, and Singapore arising from a decade-long bribery scheme.
- The Financial Industry Regulatory Authority has fined Raymond James Financial Services $2 million for failing to maintain reasonably designed supervisory systems and procedures for reviewing email communications, serving as a warning to compliance officers to review FINRA's guidance concerning the review and supervision of electronic communications.
- Medical manufacturer Alere has agreed to pay more than $13 million to settle charges that it committed accounting fraud through its subsidiaries to meet revenue targets and made improper payments to foreign officials to increase sales in certain countries.

Reputational damage — Public reaction can negatively impact reputation and stock price when a company faces regulatory prosecution or when a breach of policies makes news headlines. Consider recent social media uproar over the removal of passengers from airplanes as well as multiple criminal probes into the Uber ride hailing service. Noncompliance issues like these can have a negative effect on the company's stock, and can result in revenue losses if people refuse to use their service.

"Public reaction can negatively impact reputation and stock price when a company faces regulatory prosecution or when a breach of internal policies makes news headlines."

TODAY'S Regulatory Environment

Business and productivity disruption — When a policy breach occurs, often managers must turn their attention away from their normal roles, employees must travel to conduct investigations, and internal (and often outside counsel) must be involved. In addition, certain locations or divisions of a company can be physically shut down by a regulator — forcing them to stop work or trading until a violation has been corrected. The financial impact of such a disruption to business and loss of productivity can be devastating to a company.

How Does Your Company Measure Up?

Many companies think they are compliant because they have policies and procedures in place. But these days, having policies alone is not enough. Arm yourself with the following information to help the board and senior management understand what an effective compliance program looks like and how your company measures up.

Characteristics of an Effective Compliance Program

Chapter eight of the Federal Sentencing Guidelines for Organizations (FSGO) outlines the standards for an effective corporate compliance and ethics program. The standards have become an important barometer used by federal prosecutors and regulators in determining whether a company should be charged with a crime at the conclusion of an investigation, and if so, the severity of the enforcement action.

According to the guidelines, organizations seeking to protect the corporate brand by reducing the likelihood of incidents and minimizing the consequences if incidents occur should build a compliance program with key components that include:

- Establish policies, procedures and controls.
- Exercise effective compliance and ethics oversight.
- Exercise due diligence to avoid delegation of authority to unethical individuals.
- Communicate and educate employees on compliance and ethics programs.
- Monitor and audit compliance and ethics program for effectiveness.
- Ensure consistent enforcement and discipline of violations.
- Respond appropriately to incidents and take steps to prevent future incidents.

THE CULTURE of Compliance

The hallmarks of an effective compliance program emphasize the need for organizations to demonstrate a "tone from the top" and create a "culture of compliance" — or, in simple terms, put time, money and action toward the company's approach to compliance. According to Hui Chen, the first Compliance Counsel Expert at the United States Department of Justice (DOJ), a culture of compliance comes down to a question of behavior. "Is management leading by example? Are they putting their time, money and action where their mouth is?" Chen said. "When you pause and think about it it all comes down to the choices that are made, how time is spent and how resources are allocated. These answers are what ultimately convince you of a manager's or company's commitment."

The goal of a culture of compliance goes beyond publishing policies to actively and consistently promoting compliance and embedding it throughout the organization. The result is policy compliance that runs throughout every process and across every function of the business — demonstrating to employees and regulators alike that a company is truly committed to compliance.

Demonstrating a culture of compliance can be particularly important when businesses face possible fines. Regulators use structured penalty guidelines to calculate a Culpability Score that dictates the range of penalty to levy against a company, and the Culpability Score (and thereby the fine) can be reduced if the business is able to effectively demonstrate that it has FSGO guidelines in place. Proving you have an effective compliance program can generate reductions of up to 60 percent in potential fines. This was demonstrated in the anti-trust case against Kayaba, who received significant reductions on their penalties by implementing "a comprehensive and innovative compliance policy."

The Complete Spectrum

In addition to understanding the components of a strong compliance program, it is important to analyze your own company to understand how it measures up and what gaps need to be addressed. The following compliance spectrum shows typical stages of compliance for businesses based on the FSGO guidelines. A company's risk is greatest when it is "Unstructured" and least when it is "Best-in-Class."

Demonstrating where your company falls on the compliance spectrum, and creating a gap analysis to identify weaknesses, can be powerful tools in helping your company understand the need for a robust policy.

TIP: Conducting a gap analysis can be time-consuming: Hiring a firm that offers compliance program analysis services can speed up the process and provide a more objective assessment of your company's compliance program.

HOW TECHNOLOGY SUPPORTS An Effective Compliance Program

In addition to presenting a clear case for robust policy management, it's also critical to discuss the need for technology that supports a proactive approach to policy management. In the past, companies have used an intranet or other content portals to share policies with employees. However, that approach relied on employees to proactively read and understand policies, and provided little to no reporting capabilities for auditing the compliance program.

Today, posting policies and hoping employees read, understand and follow them is insufficient to mitigate risk and meet today's stringent regulatory demands. Companies need a holistic, automated approach to policy management that includes communication, sign-off, testing, tracking and reporting to:

- Reduce risk
- Drive process efficiencies
- Ensure regulatory compliance across the enterprise
- Provide an audit trail

Accommodating stringent demands for regulatory and company-wide policy compliance while operating efficiently requires technology that provides the ability to:

- Maintain versions of all policies in a single database
- Set up levels of review and approval for each policy before releasing the policy
- Automatically present the right policy documents to the right employees in the right language, depending on their department, role and location in the organization
- Secure agreement from employees with in required timeframes
- Test employees to ensure they've understood (not just read) policies
- Generate detailed audit trails and reports on employee acceptance and understanding — which are critical for demonstrating effective compliance when regulators perform an audit

"A holistic, automated approach to policy management that includes communication, sign-off, testing, tracking, and reporting helps to reduce risk, drive process efficiencies, ensure regulatory compliance across the enterprise and provide an audit trail."

THE COMPLIANCE Spectrum

Unstructured

- No “tone from the to
- No formal function
- Every unit addressing issues independently
- No risk assessment
- Difficult to respond to compliance or other failures
- Too many or not enough escalation routes
- No code of conduct
- Reactive

Established

- Strong “tone from the top”
- Established compliance governance procedures and function
- Efforts aligned with corporate and segment strategies
- Consistent risk mitigation approach
- Measured and monitored
- Clear escalation channels
- Technology enabled
- Comply with revised Federal Sentencing guidelines

Emerging Ad-Hoc

- Moving from reactive and episodic to proactive
- Inconsistent “tone from the top” messaging
- Increased coordination with other functions
- Ad-hoc risk assessments
- Ad hoc training and communication
- Limited use of technology
- Few standardized policies and procedures
- Informal escalation
- Code of conduct exists

Best-in-Class

- Proactive
- Embedded into culture, strategy, and operations
- Escalation metrics is a vehicle for communications with a variety of stakeholders
- Seen as differentiator with associates, regulators, customers and shareholders
- All employees know they are accountable; incentives tied to compliance

OVERVIEW
Yesterday's Approach vs. Today

Employee Review

YESTERDAY: INTRANET / DOCUMENT SHARING	POLICY MANAGEMENT SYSTEM
• Employees must take initiative to read documents	• Employees notified of new documents and can access personal library of documents at any time
• Employees struggle to locate required documents	• Sophisticated search capability included
• Employees must wade through documents to find those relevant to their role	• Each employee has access only to documents applicable to their role
• Multiple copies of documents often can be found	• Employees can access only most recent version of a document
• Employees visiting an intranet to read documents as proven to be irregular	• Rules dictate timeframe in which documents must be read; reports indicate who has and has not done so

Testing

YESTERDAY: INTRANET / DOCUMENT SHARING	POLICY MANAGEMENT SYSTEM
• Does not include regular testing to ensure competency	• Testing feature included; automatically marked and reported
• Tests cannot be easily written within an intranet	• Various types of assessments can be created, incorporating multiple choice, multiple input and written input questions
• Individuals, departments or branch offices cannot be easily identified as requiring additonal training	• Document distribution rules and testing identify and additional training requirements escalate

Updates, Distribution, and Reporting

YESTERDAY: INTRANET / DOCUMENT SHARING	POLICY MANAGEMENT SYSTEM
• Limited distribution capabilities	• Distribution groups are automatically populated
• Collaborative reviews of documents difficult to initiate and manage	• Collaborative review functionality fully incorporated
• No automatic method for sending documents to new employees	• Required documents automatically sent to new employees
• No enforcement of rules to ensure documents have been read	• Rules for reading documents are recorded, with complete audit trail of events
• Reporting on who has read each document is not included	• Reporting includes complete view of all actions and inactions
• Departments struggle when all using the same intranet	• Department heads can manage their own policy library

System Administration

YESTERDAY: INTRANET / DOCUMENT SHARING	POLICY MANAGEMENT SYSTEM
• Training to use an intranet can be time-consuming	• System is intuitive and user-friendly and includes online help
• Set-up times can be lengthy and expensive	• Implementation is quick and easy

THE ROI OF A ROBUST Policy Management System

It is important to demonstrate to your board and senior management that the return on investment (ROI) of a policy management system is measurable and substantial. The ROI for a policy management system will vary based on a company's methods of management and distribution of policies. Some organizations still use traditional paper-based methods; others are more advanced, but still fall short of the automation, collaboration, distribution and reporting capabilities a software solution can bring.

A policy management solution offers ROI in three primary areas:

1. Management, Review and Approval of Policies
2. Manager Time-Savings and Compliance Reporting
3. Retrieval of Policies

Example 1: Review and Approval of Policies

Between staff time, management time and approval time from your leadership team, your company can easily spend hours per week reviewing, updating and gaining approval for various policies and standard operating procedures. The more policies your company has, the more complex this system becomes and the more difficult it becomes to maintain manually. Eventually, outdated policy management methods lead to a waste of resources and becomes a significant cost center.

A policy management software solution provides policy owners an automated review procedure with scheduled reminders, approval workflows and improved collaboration. With proactive reminders, notifications and streamlined review and approval processes, the policy management system significantly reduce the amounts of senior level time and effort spent on mundane manual tasks by providing full automation.

Example 2: Manager Time-Savings and Compliance Reporting

Once distributed, it is essential for organizations to ensure they gain sign-off from employees on various policies and procedures to protect themselves in the case of a breach. When reports are not automated and employee compliance is not automatically tracked, staying on top of which employee has signed-off on which policy can be a total nightmare. The more employees a company has, the more managers it has undergoing this process, and the more expensive this process becomes.

Policy management software automates emails that escalate notifications to noncompliant employees and reports to management on a regular basis. These emails and reports quickly alert managers about which employees have not attested to which policies. In other words, managers get the right information at the right time, right at their fingertips - so no one's time is wasted. As the old adage goes, time is money. So don't waste either.

THE ROI OF A ROBUST Policy Management System

Example 3: Retrieval of Policies

Retrieval of policies is often the largest headache for both employees and the organization in question. For the employee, having multiple areas to look for policies (intranet, paper, email, etc.) is a time-consuming burden. Additionally, paper based retrieval does not guarantee that the recipient of a policy even reads the latest version, which creates a compliance issue for the organization.

A robust policy management system can provide targeted distribution of policies so that employees only see relevant and current versions. Combine that with a dedicated employee inbox for actionable policies and a full text search engine with metadata, and employees are able to retrieve and read policies in a fraction of the time.

When using traditional methods, the average time spent searching for a single policy is about five minutes. With policy management software in place, you can reduce the time it takes to find a specific policy to **just 60 seconds.**

Total Savings

Added up, the total of savings for automation of policy management employee attestations/ compliance reporting and retrieval of policies in these scenarios could be as much as:

- 500 employees = $28,915
- 5000 employees = $55,125
- 50,000 employees = $551,250

In addition, other "soft," but important, returns on investment include:

Increased Compliance

Auditable reporting on employees receiving, reading, accepting and understanding key policies and standard operating procedures.

Increased Productivity

Employees now use their time better and more efficiently; senior managers are free to perform skilled tasks as opposed to administration.

Improved Output

Employees now receive up-to-date training and procedures, ensuring their work and output are at the highest level.

Risk Management

The company avoids costly litigation and prevents errors and negative outcomes.

For a more detailed view into what kinds of savings a policy management solution could offer your company, connect with us.

OBJECTIONS
You May Encounter

Senior management and the board may question aspects of your case for a policy management system. Here are a few objections they may raise, and suggested counter-arguments for each:

"We aren't heavily regulated so we don't need to prove an effective compliance program."

Counter-Arguments:

It's best practice to demonstrate to our clients that we have a strong policy management system and an effective compliance program in place, making us a solid vendor of choice.

It's good quality risk mitigation — The risk of noncompliance (for example, an employee breaching a data protection policy or a sexual harassment policy) is too high to ignore.

"We already spend enough money on compliance."

Counter-Arguments:

The ROI is there — Review the ROI scenarios and consider the implications of the cost-savings long-term.

The cost of noncompliance is too high— Consider all of the potential costs of noncompliance: fines, reputational damage and business disruption.

Regulators are watching — When determining if a company has an effective compliance program, regulators will analyze the size of the compliance department, the budget of the compliance department compared with other departments and whether or not the department has ever rejected a compliance spend on technology or other investments to help demonstrate that they are effectively compliant.

"Litigation and risk are just part of doing business."

Counter-Arguments:

Regulators are emphasizing a culture of compliance — They will evaluate whether or not you are leading and demonstrating to your employees that your organization is ethical and compliant.

Risks and costs are rising — Every day, we hear of new regulations, more detailed compliance guidelines, larger fines being levied for noncompliance and businesses facing damage to their reputation when a policy breach makes headlines.

WHERE DO YOU GO From Here?

Where Do You Go From Here?

Implementing an automated, robust policy management software system is a critical component of a defensible compliance program. Using the ideas from this paper, you can build and present your own case for the implementation of such a system for your company.

Be sure to include:

- Discussion of today's regulatory environment and characteristics of an effective compliance program
- A review of the cost of noncompliance
- A gap analysis and assessment of how your company measures up against regulatory guidelines
- Discussion of the importance of modern technology to support the compliance program
- A demonstration of ROI

Conclude your presentation with a challenge to senior management and the board: Let them know that the organization needs senior-level buy-in to implement a policy management software system, and stress that the technology is critical to the company's ability to conduct policy management efficiently and prove that the company has an effective compliance program now and for years to come.

ABOUT POLICYHUB

Mitratech's PolicyHub consistently delivers a complete, cost effective and measurable policy management solution. From creating, updating, approving and communicating policies to automated knowledge assessments, audit and reporting, PolicyHub gives an organization the program it needs to demonstrate corporate responsibility and a defensible compliance program, reducing the risk of breaches and heavy fines while making the policy compliance function more efficient.

www.mitratech.com/policyhub/

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal professionals who seek out and maximize opportunities to raise productivity, control expense and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, operational best practices spreads throughout the enterprise, standardizing processes and accelerating time-to-value. By unlocking every opportunity to drive progress and improve outcomes, we're helping legal teams rise to the challenge of serving the evolving needs of the modern, dynamic enterprise.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com