



Overcoming the barriers to Policy Compliance

A Proactive Approach to Risk Mitigation

Author: Beverley Stonehouse
June 2011

Content

- Foreword..... 3
- Copyright Statement 3
- Introduction..... 4
- The purpose of policies & procedures..... 4
- Policy pitfalls 4
 - Poorly worded policies 4
 - Badly structured policies..... 4
 - Out-of-date policies..... 5
 - Inadequately communicated policies 5
 - Unenforced policies..... 5
 - Lack of management scrutiny 5
- Effective policy compliance 5
 - For The Board 5
 - For Line Managers 6
 - For General Workforce..... 7
- 6 steps to policy excellence 7
 - Create/Review 8
 - Distribute..... 8
 - Achieving Consent 8
 - Understanding..... 8
 - Auditability..... 8
 - Reporting 8
- Conclusion 8
- About Cryptzone 9

Foreword

Regulatory and legislative risks affect the whole organization. Today, policy compliance is an issue that extends beyond HR, IT and legal functions. Policy compliance is of relevance to all directors and managers, who are required to ensure their people understand their responsibilities, act appropriately and can be held accountable for their actions. A failure to measure monitor and manage policy compliance can result in damage to corporate and personal reputations, fines and lost revenues.

This whitepaper offers practical guidance on how automating the policy management lifecycle creates a firm foundation for effective risk mitigation and governance. It examines the benefits of policy compliance for the Board, line managers and the general workforce and puts forward a cost-efficient approach for achieving policy excellence.

Copyright Statement

© 2011 Cryptzone AB. All rights reserved.

Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein are trademarks of their respective owners.

This document is provided "as is" without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult a lawyer. The information provided here is for reference use only and does not constitute the rendering of legal, financial or other professional advice or recommendations by Cryptzone AB or its affiliates.

Introduction

Compliance with laws and industry regulations is a challenge facing all organizations today. Striking the right balance between risk mitigation and the demands of the business is an art, which varies according to the nature of an industry sector, size and culture of the organization and the level of acceptable risk. Organizations that take a systematic and proactive approach to risk mitigation are more prepared to satisfy evolving legal and regulatory requirements, manage the costs of compliance and even realize competitive advantage.

Getting people to do the right thing, in the right way, every time!

Policy compliance is about getting people to do the right thing, in the right way, every time. Ensuring everyone understands what is expected of them and how they are required to carry out their jobs according to corporate policies and procedures is not a new practice. Achieving and maintaining policy compliance becomes more difficult to sustain as organizations grow, become more geographically dispersed and more highly regulated.

The purpose of policies & procedures

Policies and procedures establish guidelines to conduct activities and business processes in accordance with an organization's strategic objectives. While policies and procedures are developed with reference to legal and regulatory requirements, their primary purpose should be to convey accumulated wisdom on how best to get things done in a manner which is both efficient and compliant. Where policies are only put in place to satisfy compliance requirements they can become misaligned with an organization's strategic objectives and restrict performance rather than enhance it.

Creating policies that purely satisfy auditors and regulatory bodies are unlikely to improve business performance or bring about policy compliance, as they rarely change employee behavior appropriately. Policies and procedures need to be written in language that is easily understandable for those required to follow them. They should be effectively distributed in a timely manner, and consistently enforced across the entire organization. After all, what is the point of expending considerable effort and cost to write and approve policies, if they are not ultimately distributed effectively? Don't forget policies also spell out the consequences of non compliance and may be required to strengthen a disciplinary case or law suit. Given all these considerations it is vital that policies and procedures are fit for purpose and well communicated.

Policy pitfalls

There are many reasons why policies fail to bring about appropriate changes in human behavior. Here are some of the most common grounds for policy non-compliance.

Poorly worded policies

Organizations have a tendency to write lengthy policy documents, which contain a lot of legal or technical jargon. While this may satisfy legal departments and look impressive to auditors and regulators, busy employees are instantly turned off by the length and tone of such documents and often delay reading them indefinitely, unless there are incentives or sanctions for not doing so.

Badly structured policies

Many so-called policy documents contain a mixture of policy, procedures, guidelines, reference material and standard forms. The volume and confused assortment of information makes reading these documents a daunting prospect, which many users never complete. The average reader finds them difficult to navigate and therefore fails to grasp the underlying core message.

Out-of-date policies

Factors that affect policies are evolving all the time. Technological advances lead to information security policies and procedures becoming obsolete. Changes in the law or industry regulations require operational policies to be frequently adjusted. Some policies, such as Payment Card Industry DSS compliance, have to be represented and signed up to on an annual basis. Unless systematically updated and redistributed not everyone can be sure they are working within the current policy. Inconsistent policy compliance may open an organization up to a claim of unfair treatment if disciplinary or legal proceedings are instigated.

A government organization sent out emails to 3,500 employees asking people to read one policy on the intranet.

After 5 months only 40 people had read

Inadequately communicated policies

A key step in the policy management lifecycle is to ensure that staff members are aware of relevant policies and procedures. Many organizations do not use a proactive or consistent method for communicating new and revised policies to their employees. It is assumed that people will reference documents located on an intranet or in a policy handbook; nothing could be further from the truth. Even if emailed people tend to overlook or postpone reading policy communications unless actively required to do so.

Unenforced policies

There is a saying that rules are made to be broken'. The same holds true of policies. If people see others ignoring corporate policy and getting away with it, they are tempted to do likewise. Quickly a sub-culture of non-compliance develops and people stop taking policies seriously, putting an organization at risk.

Lack of management scrutiny

Collating policy compliance status is a time-consuming and costly activity if the process is not automated. The lack of accurate management information makes it more difficult to pinpoint potential areas of risk, so resources are likely to be evenly distributed across the entire organization rather than targeted to where they are most needed.

Effective policy compliance

Maintaining large policy manuals in a hard copy format is no longer a sustainable approach to policy management. Inadequate version control and high production costs can be reduced by moving content to an electronic format, such as the corporate intranet. In many cases regulatory requirements call for evidence of policy acceptance, which demands a more pro-active and thorough approach to the policy management lifecycle. There are also business advantages to managing the policy management process more effectively.

For The Board

Strategic Leadership

Strategic leaders require an overall perspective of how their organization is doing in all areas of operation. Confirming that policy goals are being achieved helps leaders to establish what is working and where change may be necessary. Policies establish an organization's culture and seek to influence attitudes toward personal conduct, governance, risk and compliance. Effectively automating the policy management process provides reliable management information to ascertain whether policies are nurturing the intended workplace culture and engender appropriate standards of conduct.

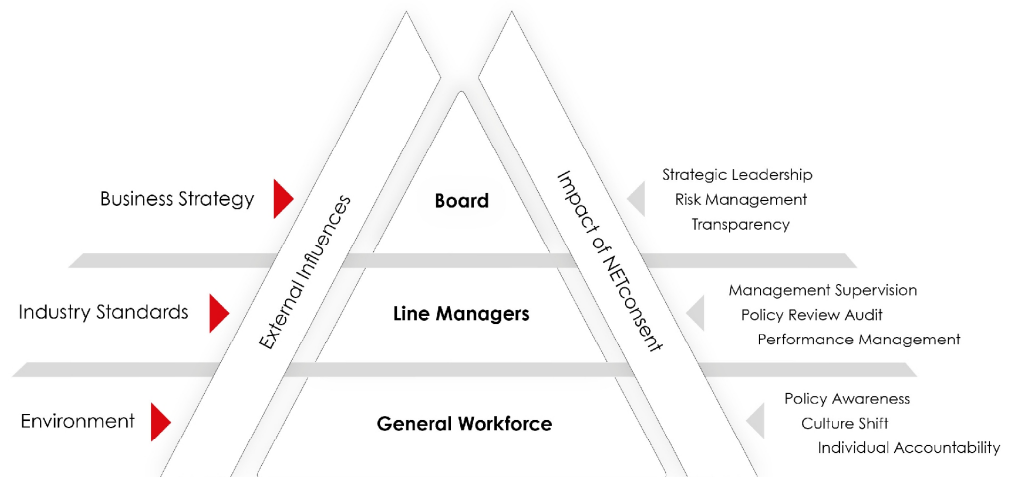


Figure 1. Corporate Governance Pyramid

Transparency

To affect change and improve compliance it helps if key performance indicators relating to policy uptake are clearly visible across all levels of an enterprise. Dashboard visibility of policy compliance by geographical or functional business units helps to consolidate information and highlights exceptions. Being able to quickly drill down for specific details in areas of poor policy compliance dramatically improves management's ability to understand and address underlying issues.

For Line Managers

Management Supervision

It is the responsibility of line managers to ensure workers adhere to policies and procedures. People who are unaware of the correct way to work and who go undetected will persistently underperform and their actions may put an organization at increased risk of governance, security and compliance failures. A systematic and flexible method for testing employees' understanding of the correct way to do things and an ability to collate the results automatically helps managers efficiently pinpoint problems with an individual or ascertain common areas of policy misunderstanding.

Performance Management

An effective policy management system must create an environment where managers have accurate information on which to base their decision-making. Exception reporting provides actionable insight for line managers to respond quickly when business goals are not being met in an effective and efficient manner.

Policy Review Audit

The complexities and expense associated with traditional methods of redistributing revised policies does not encourage the regular review and auditing of policies. Many policies would benefit from more frequent review than they typically receive. The creation of a fool-proof mechanism that delivers relevant policies to people and compels them to read them within a prescribed timescale enables more regular review and certification of policies. Automatic creation of an audit history of policy versions and user acceptance reduces the managerial workload required to gather admissible evidence should a disciplinary case or lawsuit arise.

For General Workforce

Policy Awareness

A lack of awareness and understanding of policies has been at the heart of many recent corporate governance failures and security breaches. Employees confused about their responsibilities are much more likely to make mistakes, which lead to lost productivity, poor revenues, damaged reputation, litigation fees and regulatory penalties. Creating an enterprise approach to policy management should not only provide a central repository for policies and associated documentation, making such documents easier to find, but also offer a consistent and fair process to notify relevant people when new and revised policies are published in a way that elicits a response from the recipient.

Culture Shift

Unless there is a strong culture of compliance, or people are at least aware that a failure to comply with the policy management process will impact on them directly, only cursory attention is paid to the compliance process. It is therefore vital that any system for policy compliance guarantees people read those policy documents, which are relevant to them and respond to them. Regular reinforcement of key messages is required to influence people's behaviour, until it is reflected in work practices and established as a group norm.

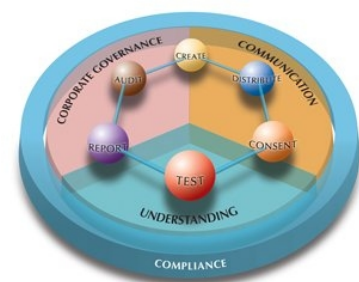
Individual Accountability

One way of ensuring individual accountability and meeting regulatory requirements to prove that people are both aware and understand their responsibilities is to require sign up to policies. This is most effectively achieved if policies are presented when someone needs to know. This might be when they go to access the network or an intranet application. Ideally policies will reflect their type of usage so people are not confused by unnecessary and irrelevant information. Unless an automated approach is adopted this process quickly becomes cumbersome and costly to administer. Properly recording and collating who has received policy information and chasing those who do not reply in a timely manner is an extremely labor-intensive and protracted manual process, which is only cost-efficiently achieved through automation.

6 steps to policy excellence

To assess the level of policy compliance within your organization, ask the following questions:

- Who has seen our current policies?
- Who has read our current policies?
- Do our staff understand them?
- Are policies being followed by staff?
- Are policies effectively managed?
- Are they up to date?
 - and can you prove this to the Auditors?



Organizations that really want staff to read, understand and sign up to policies choose to adopt automated policy management software to raise standards of policy compliance and provide managers with practical tools to improve policy uptake and adherence. Continuous evaluation of customer ideas for improvement has ensured NETconsent from Cryptzone is the most feature-rich policy management software on the market. Cryptzone is the only vendor to provide a fully documented Implementation Methodology to ensure the success of customer projects and to maximise return on investment.

Create/Review

Policies, procedures, guidelines, e-learning modules & forms can be created and edited directly in the NETconsent Policy Editor or quickly imported from Microsoft Word® or linked pdf documents. By cross referencing multiple Associated Documents information can be broken down into manageable chunks for the reader. Text entered into the NETconsent Editor, meta-data fields and associated pdfs is fully searchable, enabling staff to find documents simply and quickly.

Distribute

Policy documentation can be tailored and targeted to pre-determined employee groups so they are only required to read information relevant to them. This is achieved through synchronization of Microsoft's Active Directory, Novell eDirectory, other LDAP directory or groups defined in the NETconsent directory. Through NETconsent's unique system of Policy Enforcement Points on screen notification of outstanding policy related activities can be shown at login, application access or a designated time slot to keep policy compliance high on people's agenda.

Achieving Consent

Within NETconsent, documents can be categorized as advisory, voluntary or enforced. Enforced documents can be set to be mandatory or non-mandatory. Mandatory documents require immediate sign up, while non-mandatory documents may be set to mandatory after a period of time or a number of skips to enforce compliance. In this way organizations are able to determine what people read in which order of priority. Users are prevented from navigating away from the approval process by being presented with the wording within a locked down Policy Management Center. Users may however Snooze the application if the organization makes this option available.

Understanding

To monitor and measure people's comprehension of policies and associated documentation, NETconsent offers immediate or time delayed tests for all, or a subset of users. Questions may be presented randomly or in sequence. The user gets immediate notice of their test score and has the option to print a certificate. All results are available for reporting purposes.

Auditability

A comprehensive audit trail tracks the full revision history of all documents. It also records who has read what and how long it took; who declined a policy and why; and comprehension test scores.

Reporting

Detailed exception reports are available in multiple formats, including pdf, Excel and Word. The Compliance Dashboard can be viewed as a Gadget for Windows 7 Active Desktop, intranet or SharePoint® Web Part to provide maximum policy compliance visibility.

Conclusion

Senior management teams are responsible for developing appropriate measures to reduce risk, maintain and prove corporate governance and compliance. Embedding an automated policy management solution into an organization is really the only viable way to create and sustain a culture of compliance, where people understand their responsibilities and the importance of adhering to corporate standards. In this way people become empowered to do their jobs within an acceptable governance framework rather than constrained by a rigid set of unenforceable rules.

About Cryptzone

The Cryptzone Group is a technology innovator of proactive controls to mitigate IT security risk. We bring together the people, processes and technology to mitigate information security risks identified in the four key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security. Headquartered in Sweden, the company has offices in the UK, USA and Poland, as well as an extensive partner network with more than 150 global partners. For more information about the company and its solutions, visit <http://www.cryptzone.com>.

Cryptzone's share is listed on First North, Sweden, the Nordic alternative market operated by NASDAQ OMX. Certified Adviser is Thenberg & Kinde Fondkommission AB.

For more information about Cryptzone's NETconsent policy management software please contact your local office:

UK:	+44 (0) 370 013 1600
USA:	+1.949.279.6177
Sweden & Rest of World:	+46 (0)31 773 86 00
Email:	netconsent@cryptzone.com
Website:	http://www.netconsent.com