An IT Security Experts View on the

Six Steps to Policy Excellence

Dominic Saunders, CEO at NETconsent, puts forward an IT security experts view on best practice policy management

National government departments and public sector entities are failing to meet their IT governance requirements according to the statement issued by the Auditor-General of South Africa. The national & provincial audit 2010/11 report indicated that 75% of public entities have not implemented all IT governance aspects, and an astonishing 92% had inadequate information security controls. Half of these public entities do not have IT security policies, which are the bed rock to delivering quality services and achieving compliance.

Government and private sector organisations should be taking a more systematic and proactive approach to policy management to satisfy evolving legal and regulatory requirements, manage the costs of compliance and build public confidence. To be a credible player in the global market, demonstrating effective executive management oversight is an imperative, which can no longer be ignored. Here is some best practice advice.

The purpose of policies and procedures

Policies and procedures establish guidelines to behaviour and business processes in accordance with an organisation's strategic objectives. Whilst typically developed in response to legal and regulatory requirements, their primary purpose should be to convey accumulated wisdom on how best to get things done in a risk-free, efficient and compliant way.

Policy Pitfalls

Here are some of the most common grounds for policy non-compliance:

- poorly worded policies
- badly structured policies
- out-of-date policies
- inadequately communicated policies
- un-enforced policies
- lack of management scrutiny

So, what is the secret for effective policy management?

Policy excellence in six steps

<u>Step One: Create/Review</u>

It is important to understand, when creating policies, that those created purely to satisfy auditors and regulatory bodies are unlikely to improve business performance or bring about policy compliance, as they rarely change employee behaviour appropriately. While satisfying legal departments, and looking impressive to auditors and regulators, busy employees will instantly be turned off by lengthy policy documents full of technical and legal jargon.

External factors that affect policies are evolving all the time: for example technology advances may lead to information security policies and procedures becoming obsolete. Additionally, 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 re-presented and signed up to on an annual basis.

Typically, most "policy" documents are lengthy, onerous and largely unreadable – many are written using complex jargon, and most contain extraneous content which would be better classed as procedures, standards, guidelines and forms. Such documents should be associated with the policy. Documents must be written using language that is appropriate for the target audience and should spell out the consequences of non-compliance. Smaller, more manageable documents are easier for an organisation to review and update, whilst also being more palatable for the intended recipients. . Inadequate version control and high production costs can be reduced by automating the entire process using an electronic system.

Step Two: Distribute

A key step in the policy management lifecycle is to ensure that staff are aware of relevant policies and procedures. Organisations need to effectively distribute policies, both new and updated, in a timely and efficient manner. These need to be consistently enforced across an organisation. After all, what is the point of expending considerable effort and cost to write and approve policies, if they are not effectively distributed and read?

Step Three: Achieve Consent

In many cases, regulatory requirements call for evidence of policy acceptance, demanding a more pro-active and thorough approach to the policy management lifecycle.

A process needs to be implemented that monitors users' response to policies. Policy distribution should be prioritised, ensuring that higher risk policies are signed off earlier by users than other lower risk documents. For example, an organisation may want to ensure that a user signs up to their Information Governance policy on the first day that they start employment, whilst having up to two weeks to sign up to the Travel & Expense Policy. Systems need to in place to grant a user two weeks to process a particular document, after which the system should automatically force the user to process it.

Step Four: Understanding

To monitor and measure staff comprehension and effectiveness of policies and associated documentation, organisations should test all, or perhaps a subset of, users. Any areas that show weaknesses can be identified and corrected accordingly. Additional training or guidance may be necessary or, if it's the policy that is causing confusion, it can be reworded or simplified.

Step Five: Auditability

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. The full revision history of all documents needs to be maintained as well as who has read what, when and, if possible, how long it took; who declined a policy and why. This record should be stored for future reference and may be stored in conjunction with test results.

Step Six: Reporting

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 uptake 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.

Bringing it all together

To check the level of policy compliance that exists within your organisation you need to periodically answer the following questions:

- where are you current policies? – Are the accessible to staff?
- who has seen your current policies?
- who has read your current policies?
- do your staff understand them?
- are your policies being followed by everyone?
- are your policies effectively managed?
- are your policies up to date?
  - and can you prove this to the Auditors?

For those organisations that are serious about staff reading, understanding and signing up to policies, they should consider adopting automated policy management software. This raises standards of policy compliance and provides managers with practical tools to improve policy uptake and adherence.

Ultimately, 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. Embedding an automated policy management solution into an organisation 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.

Doing so empowers people to do their jobs within an acceptable governance framework rather than constrained by a rigid set of unenforceable rules. By effectively handling the policy management lifecycle you can create a firm foundation for effective risk mitigation and governance. Automation helps the benefits of policy compliance for senior management, line managers and the general workforce get to grips with policy compliance and puts forward a cost-efficient approach for achieving policy excellence.
==

NETconsent is a technology leader that develops and sells automated policy management software. Since 2004, NETconsent has become the leading policy management system on the market with more than 180,000 licenses sold.
NETconsent is based in Fleet in the United Kingdom with offices and partners around the world. http://www.netconsent.com

Fertech Corporation is a solutions provider and a VAD (Value Added Distributor) that was founded with the main objective to offer a unique portfolio of innovative technology solutions and services that can help our customers to manage the new IT security challenges, improve their inbound marketing strategies, and successfully expand in the Latin American and Spanish speaking market. For more information about the company and its solutions, visit **www.fertechcorp.com.**