The five critical stages of policy management
Take control and achieve compliance
Introduction

Organisations continue to face regularity pressures and scrutiny, putting a significant responsibility on the work of compliance teams throughout the world. Penalties for non-compliance continue to be issued, published and reported on. Such instances cannot only damage the reputation of a business, but in some extreme cases lead to the business ceasing trading. The ever increasing volume of regulatory and security demands on a global scale, relentlessly continues to drive up costs and risks for a compliance team. The question needs to be asked if the business will recognise this trend and release adequate levels of budget to address this and fully support the compliance function.

Since 2008, a sea of change in Director accountability has made individual Board Members responsible for the actions of their employees, and across the enterprise the responsibilities of Compliance and Risk Officers has vastly increased. One of the many responsibilities of a compliance team is to monitor new regulations and communicate them to the business; however common methods to do so are often very intensive to manage and have a number of shortfalls.

Whilst policy management is usually in place; senior management often have little visibility of policy understanding, acceptance or compliance. Historical methods currently adopted to manage and communicate policies, such as the corporate handbook, email, shared databases, or an intranet will become more and more difficult and intensive to manage as the workload of the compliance function continues to grow. Solutions to this problem are limited and usually involve bringing in additional head count or developing an internal intranet; however budgets are limited or being capped, putting additional strain on the overall compliance function and its ability to manage the communication and reporting of policies.

In relation to policies, the function of compliance is to:

- Get the right policies to the right people at the right time;
- Ensure employees read, understand and sign-up to key policies;
- Identify employees who have not adhered to a policy;
- Regularly review, assess and update policies;
- Provide senior management with detailed reports and a clear audit.

Adopting a software solution specifically designed to handle these processes can fundamentally reduce the risks of non-compliance by demonstrating rigorous management processes to regulatory bodies, as well as driving down administrative costs and allowing the Compliance team to focus on core activities.

Drawing on our experiences in this area, in this paper we explore the five critical stages of policy management, comparing traditional and unsustainable approached with rigorous methods demanded by today’s environment:

1. Establishing policy requirements;
2. Drafting policy;
3. Policy communication;
4. Testing understanding and affirming acceptance;
5. Auditing policies.
Why Create Policies?

It is a fair question to ask: why should organisations have to divert precious resources away from key business areas and allocate them to the irritating overhead of creating and administering policies?

There are three fundamental reasons why organisations need corporate policies; to achieve compliance with relevant legislation and regulations, to drive positive culture, and to help achieve an organisation’s goals.

We occupy a society where there is an ever-increasing range of requirements affecting the way in which an organisation is obliged to conduct itself. In particular, requirements are set down by the legislature, judicial and regulatory bodies. Compliance is an increasingly important part of everyday business life as more and more aspects of an organisation’s conduct become “compliance issues”.

Well drafted and effectively deployed policies can have an extremely positive impact on culture. The biggest and most successful organisations are often characterised by a very clear and well established culture – usually set by the business owners and refined over time. All employees are clear as to what is expected of them and the way in which they should conduct themselves.

As organisations grow and take on new staff, policies have a key role to play in maintaining this culture.

In a similar way to culture influencing policy, a company’s goals will also pervade the whole organisation. Policies will have a role in shaping the appropriate behaviour for attaining those goals.

While the consequences of not being able to demonstrate the required level of compliance is sometimes purely financial, it would be unwise to underestimate the hidden costs of lost management time and negative publicity that can flow from a compliance failure. Similarly, whilst penalties for compliance failures have traditionally been a problem for the organisation, there are an increasing range of situations where there is a tendency to look behind the corporate veil towards those with a stewardship of the organisation.

Well-drafted and communicated policies should also be viewed as a protector – both for the employer and the employee. A policy should leave both parties in no doubt as to what their obligations and expected behaviour are, which should dramatically reduce the likelihood of a compliance breach.

Current methodologies for policy creation and deployment

Having established why organisations need to invest time and effort in corporate policies, let us investigate the current common methodologies, together with the pros and cons for each – for policy drafting and deployment.

Creating policies

As we have already identified, organisations can use a wide range of policies to govern and shape employee behaviour. As such, it is quite normal for a number of individuals with specific expertise within the company to play a part in creating policy, and there is no reason why an experienced professional should not be capable of drafting certain policies in house. Fully researching the area and the legislative/regulatory requirements, however, can be a lengthy process.

Pro forma policies also exist, sometimes very inexpensively (such as on the internet). Yet the frequent downside with the acquisition of a policy in this way is that the document is sold subject to stringent terms and conditions making it clear that the policy is up-to-date only on the date of purchase and so the buyer is left with a requirement to keep the policy updated. Another disadvantage with these policies is that they can often be difficult to tailor to your own organisation’s needs.

A third option is to engage a third party professional such as a lawyer or consultant to assist with policy drafting (or at least review what has been produced in house). This can be argued to give additional peace of mind and may be a more efficient use of management time. This method also affords the organisation the option to shift the onus for keeping the policy up-to-date to a third party. However, such expert advice usually comes at a price.

www.grcsolutions.com.au
Deploying and auditing policy

Just as there are a number of alternatives when drafting policy, organisations have devised a wide range of techniques for deploying policies to employees. However, just as a poorly-written policy is ultimately going to fail, so too will a policy that is not effectively deployed – no matter how well-written it is. And, unfortunately, most organisations’ policy deployment methodologies are far from perfect.

In some organisations, policies are simply posted on a notice board. This method, however, does not create any sense that an organisation is trying to actively reach employees and influence positive behaviour – especially as most notice boards are infrequently read by staff. Some organisations have adopted the technology-based equivalent of posting a document on a notice board by posting on an intranet, although these are often paid as much attention by employees as physical notice boards.

A more traditional approach to policy deployment is to issue a new joiner with a staff handbook containing a clause in the employee’s contract obliging them to read the information. The reality is however, that few people take the trouble to read a policy handbook carefully and they are rarely updated to reflect new policies. The staff handbook also makes it difficult to periodically re-present employees with policies, allowing information to be forgotten over time.

Within some organisations, certain policies will be viewed as absolutely critical. For those policies, paper copies are often circulated as there is a perception of guaranteed deployment. However, there is no way of knowing the degree to which policies are actually communicated, as those issuing the policy are unlikely to ever know whether or not the policies have been read and understood.

The logical extension of this process is to require the policy to be signed and then returned to the issuing manager. This approach has the beginnings of effective policy management, but the management time associated with this methodology can be extremely high. A common complaint is that organisations find that policies returned by employees have handwritten annotations and amendments added to them, undermining their value.

Rather than circulate paper copies, some organisations distribute policy by email. The speed and ease of distribution, together with some ability to audit the delivery of policy are obvious advantages with this methodology. However, the big shortcoming of email is that it is far too easy for employees to ignore or just delete incoming messages, even resulting in some high profile tribunal decisions going against the employer.

The final step is for an additional button to be included at the early stages of logging on to an application. Through this, the user agrees to abide by the relevant policy in using the application. In many cases, however, the user will automatically click the required button in order to get to the application, and once again there is no real idea as to whether or not the policy has been read and understood.

All of these means of deployment have various advantages and disadvantages. The common advantage to most of the methodologies described above is that they require little management effort – the exception being the time consuming process of deploying hard copies for signature and return. On the basis that you get out what you put in, it is therefore not surprising that most of the deployment mechanisms adopted by organisations do not amount to an effective means of communication. This will not be good enough for an organisation for whom it is essential that key policies are understood and agreed with.

The single failing that links them all is the absence of any way of assessing the level of understanding of the policy among the workforce. Even if individuals have been made to agree that they will abide by the policy, there is no way of knowing if they really appreciate what they must do in order to comply. For an organisation seeking to drive a positive culture or avoid compliance breaches, this is a critical issue.

We have looked at the issues around policy creation and deployment, and why in many instances they fail to meet today’s compliance and regulatory requirements. Below we now set out the five basic stages of policy management that we suggest should form the backbone of a successful policy management programme.

1. Establishing policy requirements: Researching relevant law, regulatory requirements, guidelines and best practice. Identifying the business’s requirements.
2. Drafting policy: Creating legally-sound statements in plain English.
3. Policy deployment: Distributing policies rapidly and reliably around the organisation.
4. Testing understanding & affirming acceptance: Ensuring employees understand policy and agree to abide by it.
5. Auditing policy penetration: Auditing policy and providing management reports on compliance status.
Stage One - Establishing policy requirements

Any policy document issued by an organisation should be compatible with – and a reflection of – all applicable laws, regulatory requirements and best practice. Information navigation is the key to success here. The Internet, trade publications and third party professionals can all assist in setting the parameters for what should and should not be in the policy. Regulatory bodies may also issue some kind of standard advice. It is important to establish a balance between any external requirements with the needs and culture of the organisation itself.

The final decision as to what goes into a policy is a matter of commercial judgement as in reality a policy that sets out to be too comprehensive is more likely to fail as a usable document.

GRC Solutions recommended checklist – Stage One

• Research requirements of policy – laws, regulations, best practice etc.
• Find sources of information and advice to establish compliant policies.
• Consult internet, trade publications, industry bodies, external experts.
• Consider requirements of your organisation.
• Is the culture relaxed or strict?

Stage Two - Drafting policies

Whoever is responsible for drafting a policy will have to take into account the fact that different organisations have different ways of expressing themselves – tone, language etc. The Policy creator should try and achieve consistency of style across a suite of policies. Above all else the creators of policies should strive to use plain English at all times and shy from legalese or needless jargon.

Before a policy is deployed for the first time the organisation should consider whether a consultation process needs to be undergone either directly with those affected by the policy or via a staff consultative body.

GRC Solutions recommended checklist – Stage Two

• Who is responsible for writing policy?
• Who will ensure consistency of language?
• Ensure that policy style and approach is consistent with company culture.
• Check that policy is written in plain English and is understandable by all relevant employees.
• Consider a consultation phase (with either a focus group of employee representative group).
Stage Three - Policy deployment

A process should be designed that includes being able to effectively send the right policy to the right people regardless of their location. Some policies will truly be applicable to all communities within an organisation, but many more will apply to only some. If you have already organised the company into groups using Directory Services, like Microsoft’s Active Directory, the policy deployment system should be capable of integrating with it.

For some policies, a passive approach may be acceptable – such policies are usually those which deliver a benefit on the employee and where it is safe to assume the policy will be sought out. For other ‘mandatory’ policies i.e. those requiring something of the employee in behavioural terms, the deployment will need to be compelling and unavoidable.

GRC Solutions recommended checklist – Stage Three
• For which policies do employees need to be actively informed in a way they can't ignore, or just be made aware that it is available?
• Which employees need to understand and accept the policy, which locations and which languages?
• How will you ensure staff successfully receive and read the policy?
• How much impact will your deployment model have on the organisation (management time, network, existing systems, bandwidth etc.)?
• Decide where to store the policy so it is available once deployed.

Stage Four - Testing understanding and affirming acceptance

For sensitive policies, the organisation needs to be in a position to track the penetration of the policy across the enterprise. Critical to this is the collection of evidence to prove that employees have signed their acceptance to abide by the policy. But, as some recent court cases have shown, an employee’s acceptance of a policy can still be brought into question if the employer is not able to demonstrate that the employee understood exactly what he had signed up to.

Stage four is therefore a twofold process. One of the most accurate ways to assess whether employees have fully understood a policy or not is to ask them questions on it. Obviously, it is not an effective use of time to hand out and mark written tests – but there are electronic alternatives which present questions on-screen and automatically score responses. In the event of failing to demonstrate policy comprehension, you need then to be able to determine appropriate steps – deny system access, alert the line manager and or point to training options.

Only once the organisation has forced the employee to think about the policy should they then make any attempt to record the acceptance of it. Many of the deployment methodologies outlined earlier in this guide make some provision for recording acceptance, but the chosen method must make it clear to employees that they are making a legally-binding agreement, which will be recorded by their employer for future reference.

GRC Solutions recommended checklist – Stage Four
• Is the policy vital to the operation of the company – or critical to compliance? If yes, you need to ensure that staff understand the policy; agree to abide by it, and understand that by accepting a policy they are entering into a legally-binding contract.
• Is the policy well-written enough that there is just one ‘correct’ answer to any questions?
• How will you reliably audit policy acceptance without using precious management time?
• Put steps in place to deal with any demonstrated lack of understanding.
Finally, those charged with deploying policies need to be in a position to readily generate reports on the deployment process. Boards and regulatory bodies with stringent requirements increasingly demand accurate, time-stamped information on policy deployment and acceptance.

On a macro level, management reports to show compliance at a glance are essential to those leading an organisation – to what extent has policy been accepted and understood? If not, by which groups? Which policies are proving hard to understand? What potential risks are highlighted? What trend is visible since the previous policy deployment?

Moving down to the micro level it may be an unfortunate necessity (e.g. disciplinary action) to be able to identify a particular individual to whom a policy has been deployed and ascertain whether and when they agreed to abide by the policy and exactly what was included in that agreement.

**Conclusion and next steps**

Corporate policies are no longer just a ‘nice to have’ culture-shaping tool for large businesses. With the introduction of increasingly strict legislation and the attentions of industry watchdogs focusing in on compliance, policies are now essential for all organisations.

The five stages outlined in this guide have been developed by Hitec to help you develop a best practice approach to policy management – and are borne out of significant experience researching, creating and deploying policy.

Organisations that make a concerted effort to take policy management seriously will over time be able to audit the real value of their efforts. This will be both in terms of a discernible reduction in the risk exposure of the organisations and in the resources that need to be allocated to manage policies.

**Stage Five - Auditing and reporting**

GRC Solutions recommended checklist – Stage Five

- Can you easily build a view of compliance in the organisation?
- Management reports should give directors an instant snapshot view of compliance.
- Audit acceptance and understanding on both a macro (groups) and micro (individual employee) level.
- Positive compliance reports can have advantages when tendering for contracts etc.

**About PolicyHub**

A comprehensive and flexible Solution PolicyHub fundamentally reduces the risks of non-compliance. Giving control back to management, demonstrates rigorous processes to the regulator, and drives down administration costs.

Whether driven by tightening requirements and standards from a mix of financial, government, industry, or technology mandates, regulations, laws, or best practices.

By the need to effectively communicate and manage critical policies such as Anti-bribery or Corporate Manslaughter to avoid liability. Or just by the requirement to reduce costs and increase efficiency. PolicyHub can help.
In relation to the five stages discussed in this paper, PolicyHub gives you the ability to:

**Stage One – Establishing policy requirements**
- Audit employee understanding of the regulatory environment.
- Retain data to feed into subsequent stages of the policy life cycle.

**Stage Two – Drafting policies**
- Cut and paste or import policies from existing documents.
- Collaboratively draft and edit.
- Gain automatic version and tracking control.

**Stage Three – Policy deployment**
- Deliver a clear and consistent presentation of the right policies to the right people across the organisation.
- Set automatic reminders to those employees who haven’t signed up to policy documents.
- Specify different policies for different user groups.
- Provide individual policy libraries with access to up-to-date policies in each.
- Automatically present policies in local languages to staff whatever their location.

**Stage Four – Testing understanding and affirming acceptance**
- Ensure secure confirmation by staff that they agree to terms of the policy.
- Test understanding through randomised, multiple-choice questions (optional).
- Set automatic reaffirmation – periodically re-present policies to refresh / reinforce understanding.
- Respond to low scores or non-agreement e.g. re-present policies and questionnaires, alert policy owner.

**Stage Five – Auditing and reporting**
- Capture and display detailed data on effectiveness of policy deployment.
- Demonstrate acceptance and understanding of policies (by policy, groups, individuals, over configurable timescales etc).
- Provide audit trails e.g. who received/agreed to which version of which policy on what date.
- Highlight ambiguous or poorly worded questions.

To learn more about how PolicyHub and how it can help your organisation please visit [www.grcsolutions.com.au/governance/about-policyhub](http://www.grcsolutions.com.au/governance/about-policyhub)