Realtime
publishers
"Leading the Conversation"

The Essentials Series: The Business Imperatives of Compliance in the UK

Managing Compliance in Business Today

by Kevin Beaver

Copyright Statement

Managing Compliance in Business Today

In today's world, there is hardly anything that is not regulated in business. The governance and oversight of sensitive information stored, processed, or otherwise handled in a business setting is no exception. It used to be that best practices and best effort were thought to be enough. They really were not, but they were still the accepted norm. We now have compliance to deal with. Regulation after regulation from both government entities and industry bodies affect literally every organisation both large and small. And compliance with these regulations is not optional.

But how do business managers in the UK approach the challenges of compliance whilst maintaining a realistic balance of information risk against the associated costs? Simply put, we have to think about compliance in a new way. It is not a one-time grade or status. Rather, compliance is about changing the way we think about information risks and adjusting our past ways of looking at policy dissemination and enforcement. This, in turn, involves not only changing certain business processes—the procedures and steps required to implement policies—but also looking at ways to automate and enforce them. And it takes more than just the creation of policies and procedures. Cooperation is needed at all levels of the organisation. Senior management is responsible for strategy, line managers have to help with enforcement, and users are the ones who actually have to comply.

Business transformation such as this requires change and, as experience has taught us, change increases the likelihood of problems. With this change, the very essence of compliance is put at risk because employees often lack the right knowledge and end up misunderstanding new and evolving policies and procedures. We need a way to minimise errors and prevent oversights that are often avoidable. Proactively managing these changes is the only way to make it work long term. This means changing the way people work and establishing effective processes and control mechanisms such as automated electronic systems to help with monitoring and enforcement.

What Compliance Means in Today's UK Business Environment

In recent years, there have literally been hundreds of new laws passed in the UK affecting information privacy and security. Many of these require the creation and implementation of new policies and procedures. From the Data Protection Act to the Freedom of Information Act to the Regulation of Investigatory Powers Act, U.K. businesses are bombarded with numerous compliance requirements. If employees don't know what is required of them and integrate these behaviours into their daily work, there is room for trouble. In fact, these laws send the clear message that people need to be 'in the know.' For example, the Regulation of Investigatory Powers Act states:

> *(2) Conduct is authorised by paragraph (1) of this regulation only if - (c) the system controller has made all reasonable efforts to inform every person who may use the telecommunication system in question that communications...may be intercepted."*

In the same sense, the supplementary guidance to Part 3 of the Employment Practices Data Protection Code issued by The Information Commissioner's Office states:

> *The capabilities of electronic systems should be used to remind workers of their responsibilities. These can be set so that workers cannot proceed to access the internet or e-mail services without acknowledging the acceptance of certain conditions.*

Even with the multitude of compliance requirements, there is hope. The good news is that there is often overlap between the different laws and the requirements. Frequently, many of these can be integrated into a relatively small set of internal policies—some of which are likely to exist already. It is just a matter of putting them into action. The bad news is that organisations still have to ensure that the right policies and procedures are properly managed on a consistent basis.

Organisations want people to agree to follow policies but should not pressure them for acceptance. There needs to be a process by which people may not accept a policy for valid reasons. Or they may just need assistance in understanding the requirements. This is how business leaders take compliance from beyond the tick in the box and actually start to use compliance requirements to their advantage. That is, to use the policy management process to understand what people are really doing and then proactively adjust policies to meet practical operational demands and thus improve working practices.

Management Concerns

It is one thing to have a set of policies and supporting procedures, but evidencing compliance and being able to show regulatory bodies and auditors that they are actually working is a whole different issue. In fact, this is often a big area of concern for those responsible for policy and procedure oversight. You need to be able to prove compliance with policies and procedures on demand. This means being able to demonstrate that users are aware of current requirements and processes and specifically what they've agreed to. However, doing so is not an easy task if you do not have the right systems in place.

There is also the problem of avoidable errors. These are errors that occur even when written policies and procedures are in place and seemingly everyone is on board. Often caused by simple oversight and honest mistakes, many of these violations are preventable, if policies and procedures were more consistently and effectively communicated. Furthermore, many managers in IT and HR will readily admit that they do not have the right tools to properly manage compliance and information risks. Managing all the policies and procedures required for adequate information governance manually is very difficult and time consuming. It is practically impossible to do it well because there is no realistic way to keep up with all the checks and balances required. These may include such audit requirements as a list of those people to whom each policy has been communicated, those people who have accepted or declined a policy, random or systematic testing to prove comprehension, and overall compliance reports for management. In fact, with even the most streamlined manual processes, businesses are still unable to meet the latest governance requirements. Factoring in the administrative costs that have been shown to be around £10 per policy, per version, per user, it is becoming clear that businesses in the UK have to go about this differently.

Another concern is that many people view this business transformation edict and evidencing compliance as Big Brother coming in. Well, it is to an extent, but it is also where we just happen to be in the timeline of doing business in an electronic world. The fact is we're choosing to work within these parameters and working towards doing what is right in a business environment. A relatively simple concept compared with the Big Brother concerns we have in our personal lives.

Finally, dangerous assumptions are often made with regards to information assurance and compliance. Security and assurance do not necessarily equal compliance. Likewise, compliance does not always mean that everything is safe and sound. This is why management must take a more structured approach to managing risk to ensure that all areas involving sensitive business assets are in check.

The Value of Policies and Procedures

Forward-thinking business managers understand the value of getting everyone approaching things in the same way. This is exactly what effective policies and procedures do. They set the expectations of everyone involved. Good policy and procedure documentation outlines 'This is how we do things here'. Expectations that are properly set are the foundation of a well-run organisation—especially an organisation that manages compliance effectively and reduces information risks through sound business practices. However, when employees do not know about policies or truly understand what they are supposed to do, all parties are set up for failure. Furthermore, information risks are introduced and compliance gaps widen.

From creation to destruction, sensitive electronic information must be protected. It is not only the right thing to do, it is a requirement that the regulators have their eyes on. Savvy managers know this and understand what it takes to make it happen in business today. This starts with well-written policies and procedures that are implemented effectively and enforced consistently. Those in business who do a good job managing compliance-related documentation and related processes not only help their own departments but also help every business unit across the organisation. This type of business transformation aided through policy management automation not only lowers costs but also contributes to minimising business risks.

One of the primary benefits of policies and procedures is to improve overall corporate governance. That is to help ensure that specific controls are in place so that people and processes are kept in check. This can be demonstrated to regulators and auditors and makes the case that management takes compliance seriously. They also communicate secure practices and spell out how information risks are managed and how compliance is handled within the organisation. Specifically, they alert everyone what to look out for as well as what to do and not do—essentially spelling out the responsibilities of everyone involved.

Another positive aspect of good documentation that is well-communicated is to strengthen the business' case in employee-related lawsuits. For example, when an employee is fired for violating a company policy and claims it was unjustified. If management can prove that the employee knew about the policy, understood the policy, and agreed to adhere to the policy, then the business has a stronger legal case.

Policies and procedures can also help with compliance and risk management in that they outline the best ways to perform specific internal business processes that have evolved over many years. This minimises errors and oversights and in turn helps raise productivity. Overall, well-managed policies and procedures also benefit the business by minimising upkeep and eliminating duplicated efforts.

Problems Associated with the Lack of Proper Enforcement

There is a universal law of business that states people will violate policies and sidestep procedures simply because they can. It does not matter what type of industry the business is in or the quality of its people. Employees can also be lazy, disagree with, or otherwise not buy into the rules. They may even observe management not enforcing policies or even violating the rules themselves. They just lack the incentive. Can you blame them?

There are also the all-too-common employees whose desire to violate policies outweighs their perception of the risks involved. These employees are no doubt doing more risk calculations than their own management—obviously a big part of the problem! Compounding the issue are naïve business managers. There are certain people who assume that just because employees should comply with business policies and their associated procedures that they actually will. Unfortunately, people are not that simplistic.

All too often, management doesn't even understand the information risks and compliance concerns the business is up against. They either do not have the in-house expertise to properly assess information risks and compliance gaps or they have not bothered to outsource the right expert for the job. In other situations, the policies and procedures that are being pushed on employees are not relevant to the specific user or the context in which the business unit operates on a daily basis.

People not only misunderstand what is expected of them but they also do not know what to look out for. Because of a general lack of communication or the failure of management to properly classify information and how it needs to be protected, many employees are often out of the loop.

Often, the wrong person is managing the process. I have seen many situations where a company's network administrator was the person creating and attempting to enforce policies and implement procedures. I have even seen people in IT being assigned the compliance officer position. The truth is that it cannot be done this way. Even with upper management 'owning' the compliance process, I often see very little enforcement of policies in most organisations I've worked in. People get busy and complacent. It is also human nature for people to not want to hurt the feelings of their colleagues or even put their jobs in jeopardy. Ultimately, a weaker culture is created and the cycle of non-compliance begins.

I’ve also seen very little follow-up when policy and procedure gaps are identified. Interestingly, many organisations are willing to pay an independent consultant or auditor good money to find out where compliance gaps exist, yet I see over and over again those very businesses not doing anything about the issues once they’re identified.

Leadership has to come from the top with management backing policies and procedures and taking ultimate responsibility for compliance. However, it is line managers who bear most of the burden to ensure staff adhere to documented processes. When middle management lacks the tools and/or the gumption to enforce the rules, bad things inevitably happen. Employee priorities get misaligned, they misunderstand the business reasoning behind the policies and procedures, and the lack of respect and trust between employees and management grows. Many people shudder when they hear the word ‘responsibility.’ However, if an organisation is to ensure information protection and compliance, responsibility is required of everyone in the organisation—regardless of role or position.

Getting the Word Out to Users

In the majority of organisations I’ve assessed in my work, most have some form of documented policies and procedures. In many cases, however, I see that employees often have no clue that these exist, much less what they actually mean. Often, basic policies and procedures are included in employee handbooks or referenced on Intranet sites, but that is not enough. Compounding the problem, it is rare that anyone in management (IT, HR, or elsewhere) takes true ownership of the policies and procedures in order to keep them properly maintained. The documentation is all too often there to woo the auditors on their annual visit, but there is no real audit trail showing just how the documentation is being managed and whether it is even working.

So how do you get the word out to your users about what is expected? It is clear that the old method of documenting policies and procedures in a manual to be placed on a shelf and never referenced again does not work. In order to enhance overall compliance and risk management, a formal method has to be put in place to not only make documentation accessible but also kept at the top of everyone’s mind. Ignorance is not an option. Proactive notification of policies enabled by automated policy and procedure systems are proving effective in ensuring people are aware of current policies and procedures. Get the word out in simple language in terms of the employee.

To ensure consistency, communication should be coordinated by a centralised source such as HR, Audit, or Compliance teams and facilitated by IT. It makes sense for authorised line of business managers to retain authoring of procedures that are then approved and automatically disseminated. This can be done using technology to advantage. A centralised solution that provides insight into policy viewing, comprehension and enforcement is the only realistic way to make this work. In the end, you must have the right tools for the job. Every business uses computers and networks in some fashion. Why not use them to advantage for something as important to business success as this?

Once the word is out, you can then use various reminders such as computer screensavers, banner pages on intranet sites, even posters throughout the workplace. The key is to keep these concepts and responsibilities on the top of people's minds. Use outside trainers and incentive programmes including employee reviews where possible to help boost effectiveness. Rewarding good behaviour for jobs well done in the areas of policy awareness and compliance is much more effective than punishing bad behaviour. Regardless of how you go about keeping information fresh, just make sure it is an ongoing process. Information risk management and compliance are as much a mindset and culture as anything else.

Essential Requirements for Effective Information Assurance

Regardless of industry or line of work, information assurance needs to play a key role in the business. Compliance and the containment of information risks is all about visibility and control. The following list highlights the most effective long-term solutions that any given business can put in place to start making a difference:

- Management taking ownership of compliance and having ultimate oversight of all related policies and procedures.
- Management supporting a risk management approach to information assurance and compliance throughout the organisation.
- Management facilitating the creation of policies and procedures that are reasonable, accurate, and fair given the context in which they're being implemented and enforced.
- Management getting everyone on board by properly communicating what is expected.
- Management funding and supporting the ongoing administration of a proactive approach utilising centralised and automated software for policy management.
- Management sponsoring the periodic review of policies and procedures to ensure they're aligned with business goals and the latest compliance requirements.
- Management supporting the checking and re-checking of compliance. Compliant now doesn't mean compliant always. Likewise with the understanding of policies and procedures. Educate users now and then continually test them to ensure their level of understanding is where it needs to be.

Compliance-related policies and procedures must be created and integrated into the business in the right way. This means choosing and using the right technologies to automate the process wherever possible. Otherwise, such documentation is merely busy work providing advice that no one benefits from—overall a wasted effort for everyone involved. Compliance starts in the boardroom, is monitored by line managers, and ends with users. Minimising costs, maximising effectiveness, and proving compliance in a sustainable and repeatable way can be accomplished. It is just a matter of choosing the right tools for the job as well as management ensuring that business priorities are where they need to be.