Realtime publishers

"Leading the Conversation"

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

Managing Financial Compliance

sponsored by

by Kevin Beaver

Copyright Statement

Managing Financial Compliance

Since its beginning, the financial sector has had deep-rooted government regulation. With the transition to Internet-based solutions and the demand for customer privacy, financial institutions have seen even stricter policies and requirements from both government agencies and industry bodies. Practically any and all financial-related information that is stored, processed, or otherwise handled falls within the scope of these regulations. Financial-based organisations both large and small are affected, and compliance with these regulations is not optional.

Just how do finance directors and managers in the UK approach the challenges of governance whilst maintaining a realistic balance of information risk against the associated costs? Simply put, it is necessary to think about compliance in a new way. It is not a one-time grade or status. Rather, compliance is about changing your perception of information risks and adjusting past ways of looking at policy and procedure management.

As experience has taught us, changes such as these in the business environment increase the likelihood of problems. Things are constantly evolving and shifting, especially in the financial sector. Employees working for financial institutions or dealing with financial transactions often lack the right knowledge and end up misunderstanding the rules. With this, errors and oversights tend to occur putting the very essence of compliance at risk. Minimising trouble and ensuring compliance long term can only be done by proactively managing these changes.

Financial Governance Imperatives for Businesses in the UK

Of all the new laws passed in the UK and globally in recent years affecting information privacy and security, many of them affect financial institutions either directly or indirectly. The Data Protection Act and Regulation of Investigatory Powers Act, among others, create substantial compliance burdens on UK-based financial institutions and those organisations that transmit, process, or store payment card data. This oversight is especially challenging for employers in large part due to the requirements of keeping employees "in the know" and ensuring that policies and procedures are not only followed but enforced. For example, 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 well-thought-out compliance documentation, organisations still have to ensure that the right policies and procedures are properly managed on a consistent basis. This has proved to be the sticking point for many organisations.

Given all the laws and regulations affecting the financial sector in the UK, none has had a more direct impact on managing information risk than the Financial Services Authority (FSA) and Payment Card Industry (PCI) regulations. The FSA regulations—like most others—requires financial institutions to do what is right and adequately protect sensitive information. The FSA Principles have components that directly apply here:

- A firm must conduct its business with due skill, care and diligence.
- A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
- A firm must arrange adequate protection for clients' assets when it is responsible for them.

Another relevant regulation is the FSA Senior Management Arrangements, Systems & Controls Rules 3.2.6 that states:

> *(1) A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.*

This regulation is another that financial institutions can only be in compliance with by having an adequate information risk management system in place that includes the right policies and procedures.

The PCI Data Security Standard (DSS) is another regulation affecting any organisation that transmits, processes, or stores payment card data in the UK. PCI DSS is an industry-specific regulation overseeing credit cardholder data. Although it has a very specific focus and relatively few requirements, the regulation still necessitates that organisations adhere to the widely accepted practices of developing a policy and properly disseminating its requirements to employees. PCI DSS Requirement 12 states 'Maintain a policy that addresses information security'. Relevant subcomponents include:

> *12.1 Establish, publish, maintain, and disseminate a security policy…*
>
> *12.2 Develop daily operational security procedures that are consistent with requirements in this specification…*
>
> *12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors.*
>
> *12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.*
>
> *12.5 Assign to an individual or team…information security management responsibilities:*
>
> *12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.*

The consequences of failing to comply with the FSA and PCI directives are like many other regulations affecting information privacy and security. With FSA, individuals can be banned from the industry, businesses can lose permission to practice, and there are fines and potentially prison sentences. With PCI, there are fines and the loss of credit card privileges—the latter of which hardly any business can afford to be without. With these regulations, the message is loud and clear that management in UK-based financial institutions has undeniable fiduciary responsibilities.

The Realities of the FSA and PCI Regulations

As with any set of information security regulations, standards frameworks, or best practices, financial institutions do have to look at the FSA and PCI regulations realistically. Management never has and never will just throw money and other resources to become 100% compliant with 100% of every regulation without reasonable justification. Those holding the purse strings must consider:

- Tangible costs of initial compliance;
- Internal resources required for ongoing oversight;
- If and how the requirements of all applicable regulations across the board can be managed at once at the same level using the same policies and similar procedures;
- Whether or not compliance requirements mesh with the goals and intentions of the business.

With this said, if financial institutions are going to do business with the rest of the world in today's electronic marketplace, they will undoubtedly have to work within the parameters of the government and industry regulations being thrown at them.

It is also important to note the dangerous assumptions often made with regard to information assurance and compliance. By and large, most regulations say the same things and have the same requirements—the wording is just a little different. However, just because a financial institution is compliant with one regulation does not mean it is compliant with all the others. By the same token, information security and assurance do not directly correlate with compliance. In other words, compliance does not always mean that sensitive financial information is safe and sound and vice versa.

The Value of Policies and Procedures for Financial Managers

It is one thing to have policies and procedures documented, but being able to demonstrate compliance is something quite different. Those responsible for policy and procedure oversight in financial institutions and departments must be able to provide evidence of compliance on demand. This means being able to demonstrate that users are aware of current requirements and processes, and specifically, what they have agreed to. However, without the right systems in place, this is no simple task.

When it comes to compliance, the following are the real benefits of sound policies and procedures:

- They clearly specify what can or cannot be done.
- They assist with overall corporate governance and minimising business risks.
- They set expectations of everyone involved, which helps ensure that everyone's thinking is aligned and sets up all parties for success.
- They spell out exactly what to do and what not to do, which in turn minimises the chances of errors and oversights in daily work.
- They can serve as a fall-back layer of insurance in the event that a violation does occur.
- They demonstrate to regulators, business partners and even customers that the business is serious about compliance.
- They help all business units across the organisation by cutting down on duplicated efforts and ongoing administration, which in turn lowers overall costs.

The bottom line is that compliance-related directives and rules not documented are merely dreams and unfulfilled ideas.

Security Policy Considerations for the Financial Managers

More often than we like to think, managers in financial institutions and departments do not understand the information risks and compliance concerns the business is up against. There are also managers who assume that employees are always going to do the right thing. How is anyone supposed to support compliance within the organisation if management does not have its priorities straight and the right mindset for compliance?

In my work as an information security consultant, I see many financial firms failing to adequately implement their policies and procedures; likewise with employee training and awareness. It is often on paper but rarely done well. In addition, I often see a general lack of communication between IT, compliance and internal audit, and thus a lot of wasted effort that only serves to create compliance gaps.

A key point often forgotten by management is that policies and procedures are living documents that must be proactively managed. Many people also fail to realise the fact that policies and procedures are needed to outline 'This is how we do it here'. This documentation is intended to shape and change behaviour as it relates to handling sensitive financial information and doing business in such a dynamic market. Unfortunately, it is often not used in the way it should be, and therefore, creates rather than helps to eliminate business risks.

It is important to remember the following when putting together compliance-related documentation in any financial institution or department:

- The complexities of financial information systems and related business processes often make policies more difficult to enforce.
- The issue of higher employee turnover in certain financial sectors can make it difficult to get the word out and keep the word out on what is expected.
- An annual review of all documentation is critical to ensure that it is still appropriate and applicable.
- Tie compliance into employee reviews to give people an incentive to abide by them wherever possible.
- Not all policies are alike. Some are mandatory and absolutely critical. Others may not be critical for the protection of sensitive financial information. Therefore, it is important to use discretion with enforcement.
- Focus on rewarding good behaviour rather than punishing bad behaviour.
- Establish an audit trail that proves delivery of the policies and procedures to everyone involved, monitors their comprehension, and tracks their acceptance and agreement of each policy.

An integrated information governance and assurance programme—supported by management—must be in place to ensure reasonable compliance. A key component of a solid programme is using centralised and automated technologies to simplify the process wherever possible and reasonable.

Getting the Word Out to Users

A key concern in the financial arena is determining the best way to ensure employees are aware of all the compliance-related policies and procedures. This is due, in large part, to the myriad controls and regulations in the financial world that complicate things more than in the average business. In order to ensure that employees understand what is expected of them, you must make sure the lines of communication are always active and people are free to ask questions and submit concerns. This will help to support employees not only to sign-off on policies but also understand what the policies actually mean and how their responsibilities fit in with their daily job functions.

By and large, getting the word out to everyone consistently and effectively is not as easy as it may seem. One thing is certain, the old method of documenting everything in a manual that's placed on a shelf and never referenced again doesn't work. To ensure consistency, communication should be coordinated by a centralised source such as HR, Audit, or Compliance teams and facilitated by IT. The responsible group can then disseminate the information. This can and should be done using automated technologies whenever possible. In fact, a centralised solution that provides insight into policy viewing, comprehension, and enforcement is the only realistic way to make this work without incurring significant administration overhead. The secret is to get the word out and keep compliance concepts and responsibilities on the top of people's minds.

Essential Requirements for Effective Information Assurance in Financial Management

With all the complexities associated with the information systems and business processes in most financial institutions and departments, management has to be extra vigilant to ensure compliance with all the regulations. This may mean investing more resources to make it happen—something that the financial institutions are not unfamiliar with.

In order to maintain the checks and balances required for information assurance and compliance in the financial sector, organisations must have streamlined processes and utilise automated controls wherever possible. This will ensure sustainable and repeatable processes are in place. Be careful, though. Financial institutions with even the most advanced manual processes and technologies may be unable to meet the latest governance requirements if they're not properly implemented and administered. In the end, strong audit trails are needed that prove delivery of the policies and procedures to everyone involved, monitor their comprehension and track their acceptance and agreement of the applicable rules.

Leadership in the areas of information governance and compliance has to come via a top-down approach. Senior management must support the proper policies and procedures and take ultimate responsibility. However, line managers have to implement and enforce them. When they do not have the tools or the gumption to enforce the rules, bad things inevitably happen. Many people—even those in management—shudder when they hear about all the responsibilities required. However, if an organisation is to ensure information protection and compliance, responsibility is required for everyone in the organisation—regardless of role or position within the institution.

Compliance with the myriad of financial regulations starts in the boardroom and ends with users. Minimising costs, maximising effectiveness and proving ongoing compliance in a reasonable fashion can be accomplished. It is just a matter of choosing the best way to get the job done and exploring the right tools as well as management ensuring that business priorities are where they need to be.