
The Convergence of I.T. Regulatory Compliance

Compiled by Opeyemi Ore – 10th June 2008

SSCP, CISSP, ITILv3

TABLE OF CONTENTS

1	INTRODUCTION.....	3
1.1	WHAT IS COMPLIANCE?	3
1.2	WHAT CAN WE TAKE FROM THIS?	3
1.3	WHY RUN THE RISK?.....	4
2	UK AND INTERNATIONAL REGULATIONS	5
2.1	PAYMENT CARD INDUSTRY – DATA SECURITY STANDARD (PCI-DSS)	5
2.2	BASEL II ACCORD (BASEL II).....	6
2.3	SARBANES-OXLEY ACT (SOX)	7
2.4	DATA PROTECTION ACT 1998 (DPA)	7
2.5	FINANCIAL SERVICES AUTHORITY HANDBOOK (FSA HANDBOOK)	8
3	CONCLUSION.....	9

PREFACE

This document introduces the concept of Regulatory Compliance and the need for it within UK organisations today. It aims to clarify the requirements for a comprehensive IT risk strategy in order to:

- Meet the needs of the ever increasing number of regulations
- Cut the cost of regulatory compliance, and
- Remain competitive in an increasingly regulated world

It is targeted towards senior executives within UK organisations, with a little bit more focus on the financial services industry.

1 Introduction

1.1 What is compliance?

Compliance is the action or fact of complying with a law or recommended industry standard. Every business in the UK is governed by regulations of which at very least, its minimum requirements must be met. The most prominent of these regulations include:

- Data Protection Act 1998
- EU Privacy Law
- Payment Card Industry – Data Security Standard (PCI DSS)
- Financial Services Authority (FSA) Handbook
- Computer Misuse Act 1990
- Sarbanes-Oxley Act
- Basel II Accord
- Markets in Financial Instruments Directive (MiFID)

In practice, compliance to these regulations means protecting all company and third party data, by auditing and controlling the activities of users who have access to this data. 'Guarding the gates' of the organisation with firewalls, intrusion detection systems and access control, is no longer enough. The threat from insiders, i.e. employees and contractors, has become a primary security concern. This threat has become so prominent that regulatory bodies throughout the world have implemented compliance legislations (including those listed above) to ensure that organisations recognise the risks and take action to prevent the theft and/or loss of sensitive or private data.

All of the abovementioned regulations have a common element; **any access to confidential or third party data must be audited and controlled.**

From our specialised experience in this field, it is evident that most organisations view compliance as a costly exercise which is not aligned with their business objectives. Many fail to realise that an effective compliance plan will increase productivity and improve the organisation's competitive advantage, in addition to controlling the risks.

The ultimate aim is to balance the costs of being compliant versus the penalties and associated risks, with a focus on turning compliance into a competitive advantage.

1.2 What can we take from this?

Compliance to these regulations is not optional and failure to meet the requirements will lead to penalty charges proportional to the degree of non-compliance as determined by the regulator. While such penalties can be significant, it is often the case that the actual business and reputational losses resulting from incidents of non-compliance are far greater.

In practice, this means protecting your data and knowing what your users are actually doing. The threat from insiders, that is employees and contractors, is increasing. It is not sufficient to deploy only reactive security technologies internally, such as anti-virus and patch management solutions. You need to know who is accessing your data and what they are doing with it; and be able to prove it.

1.3 Why run the risk?

The goal is to balance the costs of being compliant versus the penalties, and turning this to your competitive advantage. Little or ineffective investment in security controls greatly increases your risks, and it is the insider threat that often is the cause of failure to comply. There is also evidence of the fact that a lack of effective controls directly affects your company's performance. Not only are there just both personal and business financial risks, there are personal and company liability issues and the risk of loss of consumer and market confidence. Examples of damage from insider threats are:

- A regulator fine for Merrill Lynch of US\$100m for conflict of interest which may have been averted with email monitoring.
- An employee of America Online stole 92 million email addresses and the associated telephone number, ZIP code, and credit card type, with each account. These were sold to Spammers.

There have been a number of high profile cases where a regulator has been investigating a seemingly straightforward incident and has uncovered a deeper issue, which has resulted in bad publicity and a large fine. For example, Nationwide received a £980,000 fine for what seemed to be an issue of a lost laptop, but was actually issued for "failing to have effective systems and controls to manage its information security risks".

Information technology risks are growing in importance as core business processes, procedures and decisions are automated and come to rely on the availability and accuracy of IT systems. If you cannot guarantee the accuracy of your systems then you cannot trust the information or decisions they generate.

It should be noted: that the threat to information technology systems has significantly increased as a result of the deliberate actions of internal employee and not external parties. Risk strategies have historically concentrated on external facing aspects of the enterprise. Whilst these are still important they are largely understood and covered by existing solutions.

We will cover five prominent regulations in turn and their implications for information security.

The following regulations will be covered in this document:

- Payment Card Industry – Data Security Standard
- Basel II Accord
- Sarbanes-Oxley Act
- Data Protection Act 1998
- Financial Services Authority Handbook

2 UK and International Regulations

2.1 Payment Card Industry – Data Security Standard (PCI-DSS)

Formed to ensure safe handling of payment card data, the PCI Data Security Standard was originally the result of aligning the security programmes for VISA and MasterCard. The latest release has been developed further by VISA, MasterCard, AMEX, JCB and Discover Financial Services.

The need for such a standard has been highlighted through security incidents such as TJX (TK Maxx), and Newcastle City Council, which involved exposure of cardholder data. All merchants and service providers dealing with cardholder data are now required to demonstrate compliance to the PCI Data Security Standard.

The PCI Data Security Standard provides a framework for developing a robust account data security process - including preventing, detecting, and reacting to security incidents. It includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The current version of the standard (1.1) specifies 12 requirements for compliance, organized into 6 logically related groups, which are called "control objectives." The control objectives and their requirements are:

- **Build and Maintain a Secure Network**
 - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
 - Requirement 7: Restrict access to cardholder data by business need-to-know
 - Requirement 8: Assign a unique ID to each person with computer access
 - Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
 - Requirement 10: Track and monitor all access to network resources and cardholder data
 - Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
 - Requirement 12: Maintain a policy that addresses information security

These deal with two main areas:

- **Technical Foundation:** The standard details technical requirements for the secure storage, processing and transmitting of cardholder data.
- **Testing Methodologies:** The standard provides for common auditing and scanning procedures. Assurance that security strategies are in place and working correctly is an important part of any security programme. To that end compliance to PCI-DSS is audited. The form of the audit depends on the volume of transactions your business processes.

Failing to comply can carry some fairly hefty fines. The card vendors can also choose to suspend settlement of card transactions, which would disable your company's ability to process card information until verified as compliant. As an example of how much it can cost, TJX estimate to have spent or put aside \$250m for a series of compromises. TJX settled with Visa for \$41m to avoid further penalties relating to non compliance with PCI-DSS at the time of the data loss.

2.2 Basel II Accord (Basel II)

Basel II Accord was initially published in 2004. It created an international standard which banking regulators can use when regulating how much capital banks need to put aside to guard against the types of financial and operational risks.

The framework is the result of work from the G10 countries and to promote the adoption of stronger risk management practices by the finance industry. This should result in a more timely warning of potential issues affecting an institution's financial position.

There are 3 key features to Basel II, known as "pillars". These are:

- Minimal capital requirements. This compares capital held against total risk. For example, looking at contingency funds.
- Supervisor review of an institution's internal assessment process, risk management process and the capital an institution should hold in reserve – that is internal controls and risk management
- Enhanced disclosure to strengthen the market discipline for an institution as a complement to supervisory efforts – that is transparent financial and risk reporting.

One of the key compliance areas for Basel II is proof of accuracy of financial reporting. This relies on your ability to prove the accuracy of your systems, the data they hold and access to that data. In order to prove this, you will need to record changes to your environment and data, including how and when they occurred. An example of what can happen if you do not monitor and audit your internal users is Capita Financial Administrators Limited's FSA fine. Due to a lack of auditing and monitoring they failed to pick up on insider fraud.

In the UK the FSA regulates compliance to Basel II. It has the authority to issue uncapped fines and revoke licenses, it has granted, for failure to comply.

2.3 Sarbanes-Oxley Act (SOX)

With senior management liability up to \$5m and 20 years in jail, depending on the infringement, this is probably the regulation that has received the most publicity in the last few years.

SOX was conceived following a number of high-profile incidents across some of the world's biggest accounting firms including Enron-Arthur Anderson, as a way of restoring the stock-holder's confidence in these markets. It aims to increase the independence and accuracy of auditing and corporate governance, so in-turn protecting investors and the stock market.

The act is made up of 11 Titles (sections) the main ones cover:

1. Public Company Accounting Oversight Board (PCAOB)
2. Auditor Independence
3. Corporate Responsibility
4. Enhanced Financial Disclosures
5. Analyst Conflicts of Interest
6. Commission Resources and Authority
7. Studies and Reports
8. Corporate and Criminal Fraud Accountability
9. White Collar Crime Penalty Enhancement
10. Corporate Tax Returns
11. Corporate Fraud Accountability

As with PCI-DSS this act has a broad remit. You need to implement a corporate governance framework, have strong **internal controls** and be able to prove all the measures you have in place are working. An important part of internal controls proof is monitoring and auditing these controls so you are able to prove who did what and when.

As with Basel II in order to provide accurate financial reporting you need to ensure you have accurate data.

2.4 Data Protection Act 1998 (DPA)

This act is designed to protect individual's data from misuse and unauthorised dissemination. It provides individuals with the right to know what data is stored and, be able to correct inaccurate data.

Now in line with EU data protection, the key principles of the DPA are:

- Data may only be used for the specific purposes for which it was collected.
- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (for example, the prevention or detection of crime). It is an offence for Other Parties to obtain this personal data without authorisation.

- Individuals have a right of access to the information held about them, subject to certain exceptions (for example, information held for the prevention or detection of crime), and can change such information, if incorrect, or where necessary.
- Personal information may be kept for no longer than is necessary.
- Personal information may not be transmitted outside the EEA unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.
- Subject to some exceptions for organisations that only do very simple processing, and for domestic use, all entities that process personal information must register with the Information Commissioner.
- Entities holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organisational measures (such as staff training).

In order to meet DPA requirements you must have suitable internal controls in place and be able to audit and monitor data access and prevent any potential abuse. You need to know who is accessing your data and when.

Failure to comply with the DPA can result in unlimited fines and prevention from processing personal data. These fines can be levied at directors and managers of organisations that fail to comply. Fines can be issued by the Information Commissioner's Office (ICO) or, in the case of financial institutions, the FSA. An example of this is Capita Financial Administrators Limited fine for failures of anti-fraud systems and controls. In this case internal employees were instrumental in the fraud. **This highlights the necessity for adequate auditing and monitoring of staff, and a proactive approach, not just relying on policies and procedures.**

2.5 Financial Services Authority Handbook (FSA Handbook)

The FSA regulates the UK financial services industry and its handbook is the authoritative guide to its regulations. Their main aims are:

- Promoting efficient orderly and fair markets
- Helping retail consumers achieve a fair deal
- Improving business capability and effectiveness

The main areas of regulation are risk management and due care, skill and diligence. A couple of examples where companies have fallen foul of these are:

- Nationwide fined £980k for failing to have effective systems and controls to manage its information security risks
- Norwich Union Life £1.26m fined for not having effective systems and controls to protect information and manage risk

To meet FSA regulations there is a clear need to develop a risk management framework, including operational risk, and strong internal controls. You will also need to prove these are in place and effective. It should be noted the FSA holds senior managers responsible for risk management and internal controls.

3 Conclusion

The number and complexity of regulations is growing. In order to reduce costs and still be compliant a unified strategy is needed. You will need to assess what you have now. This will include auditing the controls you already have in place and monitoring them for their effectiveness.

Once you know where you are, you need to evaluate your requirements based on governing legislation and business strategy. A gap analysis will be necessary to establish the shortcomings of your present strategy. Repeating processes, practices and evaluations for every legislation is neither efficient nor cost effective, therefore having a unified approach for these regulations is essential. You need to ensure you have an effective, efficient, and comprehensive framework to manage IT risk and compliance. This will ensure your approach is systematic and repeatable.

Key areas to look at are:

- **Protection of Data** – relies on both confidentiality and integrity of data.
 - For data to be trusted you need to be able to guarantee its authenticity.
 - For data to be of value to your business you need to protect its confidentiality.
 - You need to be able to prove data protection is working, which can be achieved with audit logs and proactive monitoring.
- **Robust Internal Auditing and Controls** – generally part of operational risk management. Controls that are more effective lower risks. Examples of internal controls are, granting and tracking user access. Change management is also a very important internal control. If you cannot validate the status of a system can you trust the data it holds? As with protecting data, proof is needed to ensure your controls are working as expected.
- **Proactive and Reactive Risk Management** – Both of these are necessary and reduce risk to your organisation. Examples of proactive risk management are:
 - Restricting user or system access to perform non-essential functions
 - Segregating a high risk activity into two separate roles or monitoring user activity for known suspicious events.
- **Documenting Policies and Procedures** – It is very easy to say everyone knows the drill but if it is not written down it is not enforceable. People will take shortcuts or add their own steps. This can expose your data or business to unnecessary risks.

You need to address entire business and enterprise, not only the areas which you think are affected: many areas will interact in ways that are not anticipated, until there is an issue. No risk should be a surprise because that is how it becomes a liability.

By attacking the issue of compliance in a controlled and repeatable manner, continually monitoring and auditing the measures you put in place, you will be well prepared for the next wave of legislation whilst also saving money and remaining competitive.

As can be seen, one thing in common with all regulatory compliance standards is the need to actively and regularly monitor all activities relating to the usage of an organisation's data. It is also essential to be able to pro-actively test the network and its components to meet the requirement for regular monitoring and testing of the network for vulnerabilities, both internal and external. Both of these require the use of external or independent verification, however there should also be continual internal auditing and monitoring to ensure operational controls are working correctly. There is little point in waiting for an external audit to check for any potential issues, the damage could already be done.

Overall, mitigating the objective of all regulatory compliance is about gaining better control over sensitive data, protecting this data by changing the mind-set of every employee, educating them about the importance of compliance and building information security into the 'DNA' of your organisation.