



Money Laundering Regulations 2007 and the Relationship to ISO 27001:2005

Introduction

The purpose of this paper is to describe the compliance requirements for firms that are subject to money laundering regulations (which include banks, building societies, estate agents, money transmitters, bureaux de change and investment firms).

It will also address how implementing an ISO 27001:2005 robust information security management system (ISMS), can aid compliance and direct an organisation towards improving the way it controls, checks and monitors customer information.

What are the current requirements for compliance?

The existing money laundering regulations require preventative measures to be put in place. Firms are required to:

- Know their customers, including conducting customer identification, verification and undertaking ongoing monitoring where applicable
- To maintain records of identity
- To train staff on the identity of the requirements
- To report suspicions of money laundering or terrorist financing¹

The New Regulations

The new anti money laundering regulations will take effect in the UK on the 15th December 2007 and together with the Proceeds of Crime Act will affect every business in the UK. The UK is facing more serious and ever changing threats from crime and terrorism, with finance being the lifeblood of both. The HM Treasury's strategy to counteract these threats is disruption and to deter crime and terrorism by restricting access to the UK financial system.²

Significant changes will be introduced requiring firms to:³

- Provide more detailed obligations regarding customer due diligence
- Vary customer due diligence according to the risk of money laundering or terrorist financing i.e. risk assess individual situations for enhanced due diligence in high risk situations.
- Rely on other firms for undertaking customer identification, if required
- Clarify the arrangements for the supervision of firms, including those that will be supervised for the first time

¹ [The Proceeds of Crime Act 2002 and Terrorism Act 2000 impose these obligations on firms and individuals](#)

² [Sourced from the HM Treasury Money Laundering Regs 2007 – An Information Sheet For Firms](#)

³ [Sourced from HM Treasury – summary of the new regulations](#)

Measures an organisation must take to comply and resist attempted frauds

A startling fact is that the market for organised criminal activity is worth more than £11 billion per year. It is becoming more apparent that the larger the size of a particular criminal market the more likely it is to resist attempts at disruption. Around £5.3 billion in profits remain once the costs of engaging in criminal activities have been accounted for. £3.3 billion of the proceeds of crime is sent abroad leaving £2 billion which is then invested into assets in the UK.⁴

Businesses need to have systems and controls in place including an effective anti money laundering policy to guard against abuse by money launderers (the regulations apply to goods or services purchased by customers over the amount of £9,500). Supervisory authorities such as the Office of Fair Trading, (who will monitor estate agents) HM Revenue & Customs (who will monitor Trust and Company Service providers, money service bureaux and high value dealers) will require businesses to register and prove that they are compliant with the legislation. The regulations also specify that relevant staff within the business need to be trained in the law relating to money laundering and terrorist financing and to receive regular updates in their training.⁵

The penalties for non observance are severe including up to two years imprisonment and an unlimited fine.

ISO 27001 and how it assists compliance to the regulations

ISO 27001:2005 (formally BS 7799) is the de facto international standard on establishing, maintaining and improving an ISMS for both public and private sector organisations. If an organisation works towards compliance with ISO 27001, appropriate controls are identified and implemented to manage identified vulnerabilities and lower the risk of threats to an organisation's information assets.

By developing an ISMS the organisation expresses its commitment to establishing an appropriate information security framework. A major benefit of the standard is that it creates a framework to ensure that roles and responsibilities for security, compliance, legal, regulatory and statutory requirements are clearly established. This benefit ensures closer compliance to the money laundering regulations.

As mentioned above, firms must have systems and controls in place to guard against being used by money launderers. In many cases an organisation may have policies and procedures in place however they are sometimes fragmented and may not be clearly communicated throughout the organisation to relevant personnel. By having an ISO 27001 framework in place and managed correctly, it will ensure that all legal obligations, more specifically, relating to fraud are met as far as practically possible.

The risk assessment methodology and exercise is a pivotal part of implementing an ISMS into an organisation. It provides a starting point from which all other decisions relating to introducing new policies, procedures, controls and processes into the business stem from.⁶ The purpose of the exercise is to identify and list all important information assets within the organisation. Information assets for the purpose of ISO 27001 include such things as (but are not limited to) hardware, software, IT systems, information contained on a range of media, the physical infrastructure of the organisation, power supplies, telecommunications, third party contractors and customers. Once these have been identified, realistic threats and associated vulnerabilities must be identified and controls selected to manage the vulnerabilities (i.e. to reduce the risk of a threat exploiting a vulnerability). The benefits of this methodology and how it dovetails in with compliance to the money laundering regulations are highlighted below.

Another key area should an organisation work in compliance with ISO 27001 is management responsibility.⁷ Specifically, this section of the standard states that management shall:

"Communicate to the organisation..... it's responsibilities under the law and the need for continual improvement"⁸

⁴ Figures sourced from recent Home Office report (2007)

⁵ Sourced from Tait Walker (Chartered Accountants) brochure on Money Laundering regulations

⁶ A mandatory requirement from section 4 ISO 27001

⁷ Section 5 ISO 27001

⁸ Section 5.1 d) ISO 27001

By working in accordance with the standard an organisation's executive management demonstrate that they take their legal obligations seriously and can therefore show compliance with the regulations and that their staff are working in accordance with relevant laws. It is the organisation's executives who are ultimately responsible should a breach of a law occur.

ISO 27001 has a direct link with compliance to the law; legal compliance is one of the foundation blocks for developing an ISMS. There is a clear benefit to working in compliance to ISO 27001 as it means that meeting the regulation requirements of The Proceeds of Crime Act (2002) and the Money Laundering Regulations (2007) will be an executive management level priority.

Further detailed (low level specific) areas of the security standard which are relevant for working in compliance to the regulations

(1) The current regulations require firms to know their customers (including conducting customer ID and verification checks).

By having an ISMS in place it becomes best practice for an organisation to address security when dealing with external parties, indeed it is a specific control from Annex A of ISO 27001 contained within security surrounding external parties specifically, "addressing security when dealing with customers"⁹. In practice it means that if there is a legal requirement on the organisation to carry out identification and verification checks on customers, before giving them access to the organisation's assets, then they shall be conducted and the control from the standard implemented and complied. I.e. the customers should be risk assessed in line with the methodology explained above and controls applied in order to reduce the risk of the identified threat exploiting the vulnerability. An example of the methodology is demonstrated below:

Risk Assessment Exercise which would be carried out if an organisation complies with ISO 27001:

Identified Asset	Customer [NAME]
Threat	Customer wishing to purchase goods above £9,500 - Money Laundering
Vulnerability	Organisation currently does not carry out customer verification checks
Impact	Potential breach of regulations and punitive fines/custodial sentence
Control	Organisation will address security when dealing with unknown customer

Established process

A formal process would be established with a procedure for identification and verification of customers. This would be regularly audited by an internal audit function for evidence of continual compliance to ISO 27001. This effective process (and requirement of the regulations) would be introduced into an organisation as a direct result of establishing an ISMS and conducting a risk assessment process.

(2) The current regulations stipulate that records of identity should be maintained.

ISO 27001 specifically deals with this area through both document control and control of records¹⁰ both of which are mandatory requirements for compliance to the standard.

Most importantly the control of records section of ISO 27001 states that:

*"Records shall be established and maintained to provide evidence of conformity to the requirements and effective operation of the ISMS. **They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations.** Records shall remain legible, readily identifiable and retrievable"*

This means that once the management system has been established all records should be maintained in accordance with any regulations the organisation is subject to, this is a direct link to the requirements of the money laundering regulations.

(3) Staff must be trained on the identity of the money laundering requirements.

⁹ A.6.2.2 Annex A ISO 27001

¹⁰ Section 4.3.2 and 4.3.3 ISO 27001

“*Training, awareness and competence*” is a mandatory section contained within ISO 27001.¹¹ The criteria states:

“The organisation shall ensure that all personnel are competent to perform the required tasks by.....providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs”

AND

“All relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives”

By operating in compliance with ISO 27001 the risk assessment will have identified “*non compliance to the money laundering requirements*” as a threat to the organisation. The regulations are automatically brought under scope of the ISMS and therefore a main control will be the “*formal training of designated employees*” who shall be responsible for complying with these laws.

Further more, there are low level controls from Annex A of ISO 27001 which would be selected in order to ensure compliance to the regulations and establish formal processes within the organisation. Human Resources security¹² is a key area of ISO 27001 and a specific section was established for HR when the standard changed from BS 7799 to ISO 27001 in October 2005.

The “*during employment*” section of the HR controls deals with “*Information security awareness, education and training*” and state:

“all employees of the organisationshall receive appropriate awareness training and regular updates in organisational policies and procedures as relevant for their job function”¹³

(4) To report suspicions of money laundering or terrorist financing.

“Information security incident management” is a key area of ISO 27001 and having an established process in place is vital for operating an effective ISMS. Contained within this section is “Reporting information security events and weaknesses”. The objective of having a formal reporting procedure in place for reporting security weaknesses is to provide a robust control which requires:

“all employees, contractors and third party users of information systems and services to note and report any observed or suspected security weaknesses in systems or services”¹⁴

What would happen in practice (should the organisation work in compliance to ISO 27001), is that the member of staff should report a suspicion of attempted fraud or terrorist financing to the relevant departmental head who would liaise with the Information security officer and a designated legal officer. The incident could then be investigated through a formal review. This ensures the organisation maintains stringent measures to prevent frauds occurring.

By having an ISMS in place the established process helps to ensure effective control for legal compliance and all records of the investigation from the initial report of the suspicious incident to the formal investigation. Finally the denial of the transaction would be maintained as evidence for a criminal trial and for the supervisory bodies, enabling the firm to prove that they are complying with the legislation.

The 2007 legislation and why it is important that organisations are aware of their legal obligations

With the introduction of the 2007 regulations it is apparent that more will be expected of firms with regard to showing that they are pro actively implementing measures to counteract attempted frauds and therefore legal compliance should be a priority for them. ISO 27001 contains a dedicated “Compliance” section.¹⁵ To claim compliance to the standard, an organisation is required to meet a number of requirements all of which must be explicitly defined, documented and updated regularly. This includes the identification of all relevant statutory, regulatory and contractual requirements.

¹¹ Section 5.2.2 ISO 27001

¹² Section A.8 ISO 27001

¹³ Section A.8.2.2 Annex A ISO 27001

¹⁴ Section A.13.2 Reporting security weaknesses Annex A ISO 27001

¹⁵ Section A.15 Annex A ISO 27001

This highlights the fact that organisations which have an effective ISMS in place are more likely to comply with the regulations than those that don't. Compliance to ISO 27001 and meeting the requirements of the money laundering regulations go hand in hand.

One new area which specifically ties into ISO 27001 is the fact that firms are now permitted to rely on other firms to undertake customer identifications on their behalf. This situation could however produce a mine field of problems for firms as they will in some cases be completely relying on the competence and due diligence of the external body carrying out the required background checks in an acceptable manner. Should no formal control exist for the external audit of third parties then customers may not receive the required level of necessary verification and this in turn could lead to frauds still occurring and a breach of the regulations.

ISO 27001 contains a section on "Third Party Service Delivery Management"¹⁶ under "Communications and Operations Management". The purpose of the control section is to implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

More specifically it states:

"It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party"

By having an ISMS it ensures third party organisations who are responsible for conducting the background checks of customers are doing so in the agreed manner which was laid down in the initial contract. Furthermore, the organisation operating the management system now reserves the right to formally audit the third party and indeed must be able to provide records that they do so on a regular basis.¹⁷ This control ensures that security breaches don't occur through this channel, moreover the third party contractors should appear on the formal asset register and be formally risk assessed in line with the established process.

Further additional requirements to the old legislation now include terms such as:

*....."require firms to vary customer due diligence according to **the risk of money** laundering or terrorist financing".....*

AND

*....."to take enhanced customer due diligence measures in higher **risk situations** and less due diligence in **lower risk situations**"....*

This clearly demonstrates that a formal risk assessment process for individual situations is now of utmost importance with the introduction of the amended regulations. Therefore implementing a management system should be high on the agenda for registered organisations, subjected to the legislation.

Clearly it is an advantage to operate a formal management system for the reasons described above. Although ISO 27001 covers all aspects of security within an organisation including physical and environmental, application and operating system security it does specifically target legal compliance as a priority for maintaining business continuity. Therefore an organisation operating a formal security management system will put itself in a much stronger position than an organisation which is attempting to comply with relevant legislation on a more ad hoc basis.

¹⁶ Section A.10.2 Annex A ISO 27001

¹⁷ A.10.2.2 Monitoring and review of third party services