Guernsey Financial
Services Commission

Data Security

A Thematic Report on Practices within the Banking Sector of the Bailiwick of Guernsey

February 2012

Table of Contents

Disclaimer:

This report is not intended as formal regulatory guidance, nor should it be taken to cover all relevant aspects of the subjects addressed. Rather its purpose is to identify and communicate examples of good practice as well as areas where improvements could be made.

Produced by:

Carl Ceillam CISSP, EnCE

Foreword by:

Philip Marr, Director of Banking

1. Foreword by Philip Marr, Director of Banking

Good practice in data security should be regarded as a pre-requisite of effective and successful banking businesses. This is principally because good data security is an integral part of customers' confidence in a banking business and confidence is at the heart of banking.

It is well known that Guernsey has for many years been a significant centre for wealth management and private banking. Indeed following the publication of the Hunt Report on the Guernsey Banking Sector the Bailiwick has sought to develop as a centre of excellence in private banking. In that context Guernsey banks need to demonstrate "best of class" practice in data security.

With that background in private banking it is appropriate to record that the failure in 2009 of data security disciplines and practices in a large well known private bank in Switzerland (the world's preeminent centre for private banking) was a significant driver behind the Commission deciding to undertake a thematic review of data security practices across the banking sector in Guernsey. Clearly a major theft or loss of customer data in any bank, but especially in a private bank, has the potential to inflict serious reputational damage on the bank and from which it may take a significant period of time to recover. It is this potential reputational risk which lies at the root of our encouragement of greater awareness of good practice in the field of "data security" or "information security" (which terms we regard as equivalent and interchangeable).

You will see from the Report that the ISO 27001 standard has adopted several areas of good practice including an inventory of information assets. The concept of "information assets" may not be immediately familiar to many licensees or bankers generally but when transposed into the notion of a customer database, a segmented customer database or a product database, then it should become more readily recognisable. The Report identifies a wide spread of practice with regards to the maintenance of an inventory of a firm's databases and we are not, at this stage, giving a hard and fast recommendation on this practice: we are, for the moment just alerting recipients to the fact that adopting good practices in this area may be of benefit to your bank since we know that many of the databases have intrinsic value and that their loss could be a serious disruption to business activity so that an inventory could assist in any business recovery process or security breach investigation.

Licensees and other readers may like to know that in addition to conducting on-site reviews of a selection of banks the Commission also considered it appropriate to conduct the same assessment on itself as an institution within the finance sector. The findings of that review have been presented to the Commission's Audit and Risk Committee which has taken note of the Review's observations.

I would encourage licensees to benchmark their own data security practices against the ISO standard and the examples of good practice described in this Thematic Report.

2. Executive Summary

Maintaining the confidentiality of customer banking details is vital to the success of both the individual bank and to the Guernsey banking industry. For this reason the Commission performed a review of Guernsey bank's approaches to managing data security risk. The review consisted of a self-assessment questionnaire, sent to all banks, followed up with a number of on-site visits. In the review we found many examples of good practice with relatively few areas for improvement. However, data security is a rapidly moving area and demands a process of continuous improvement. Therefore, even those banks with highly effective security controls will be able to build on the findings of this review.

The key areas for attention can be summarised as follows:

- Banks must take full responsibility for their own risk assessments of data security controls. The most effective and proactive approach uses multiple levels of complementary control activities. Local management should perform their own policy-enforcement activities, preferably on a continuous basis, for example a clear-desk policy. Risk or compliance functions should provide oversight and supervision through regular monitoring and reporting; an example in this area would be verifying that staff have completed regular security awareness training. Periodic independent audits should be conducted with the results used to refine and enhance local procedures.
- All licensees had deployed a wide range of data leakage prevention controls, but these were largely technical counter measures and access controls. Good data governance should begin with a data classification policy which defines the sensitivity levels to be assigned to different types of data, and the corresponding protective controls that are expected. Similarly an inventory of "information assets" is an essential record of what data is processed or stored, where it is held, by whom and how it is controlled. Without such a record it is difficult to imagine how a major security breach could be handled effectively.
- Several banks had begun to use automation to good effect to ease the burden of user management (i.e. maintaining and auditing user accounts and access permissions etc.) We see this as a positive trend that should be encouraged, particularly in larger institutions. Examples include workflow applications to manage the creation and deletion of user accounts, and reporting tools for user rights recertifications. Properly implemented software solutions in this area will reduce control issues and make processes more efficient.
- Although most banks professed to use the ISO 27001 information security framework, the review findings indicate that compliance with the standard is patchy and selective, leaving key information security controls overlooked. Following a widely adopted standard for data security is essential for effective information security risk management, and we would encourage all banks to formally adopt a security framework where none exists.
- Finally, although most banks made good use of specialist vetting agencies to validate prospective employee credentials, almost all could enhance procedures further by including checks of social networking sites and general internet searches.

3. Introduction

Terminology: throughout this document the terms ‘data security’ and ‘information security’ are considered equivalent.

The confidentiality of customer bank account details is seen as fundamental to the activity of banking. The loss of customers’ account details or their acquisition by unauthorised third parties, whether inadvertent or deliberate, will unquestionably undermine the normal relationship between banker and customer. A major or recurrent loss of customer data would go a long way to threaten the reputation of any jurisdiction with a significant banking sector. Whilst those reputational risks are self-evident they are doubly threatening in a jurisdiction like Guernsey which is widely regarded as a centre of excellence in private banking. Clearly there should be adequate disciplines and procedures in place to mitigate those risks. This review focuses primarily on the security of customer data, and so covers a wide range of data security issues.

4. Methodology

As in previous thematic reviews a two-stage approach was followed:

- An industry-wide survey of Guernsey licensed banks, using a self-assessment questionnaire, was issued.
- On-site visits to a representative sample of banks, to examine controls in more detail, and to perform a limited amount of testing was undertaken.

Both the survey questionnaire and on-site audit programme were based on ISO/IEC 27001. This is an internationally recognised standard for implementing information security. ISO 27001 was chosen because it covers virtually all aspects of data security, making it an obvious choice for a general review of the subject.

A small amount of customisation was carried out of the ISO 27001 control objectives, mainly to remove control objectives that were of less relevance to customer data security. We also removed business continuity from the review, since this had been covered in a previous thematic. This resulted in a review covering ten of the eleven ISO 27001 categories:

- Security policy
- Organisation of information security
- Information asset management
- HR security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Compliance and audit

All Guernsey licensed banks were then sent a copy of the questionnaire, which contained over 60 questions. To support the on-site visits, each bank was asked to provide supporting documentation for inspection prior to each visit.

The Commission was very grateful for the considerable amount of time and effort the banks visited went to in preparing documentation, which was of high quality and of great assistance. We also appreciated their openness in discussing their approach to managing data security. Each bank visited was given individual feedback on areas of good practice, and where the Commission felt improvements could be made.

5. Findings

5.1. Overview

Findings are presented separately for the self-assessment questionnaire responses and the on-site visits. Both sets are provided in the order of the ISO 27001 control categories.

5.2. Findings from the Questionnaire

Policies and Standards

Each bank had an approved data security policy. In most cases employees were required to formally confirm that they had read and understood the policy both on joining, and annually thereafter. Often monitoring of policy declarations was performed by the compliance department, along with other annual declarations. However, several organisations admitted that they did not share the policy with third parties, and instead relied on non-disclosure agreements ('NDA') and confidentiality clauses in contracts.

Whilst contractual terms may provide some recourse in the event of a breach, they are not an effective means of conveying the data security expectations of an organisation to an individual. For example, an NDA may make a contractor aware of their obligation to keep bank information confidential, but it would not normally stipulate how that is to be achieved, or what to do if a breach is suspected. Conversely employment policies generally provide guidance on each aspect of the individual's expected behaviour, and what controls are to be maintained. Therefore contractors and other third-parties should be required to adhere to the same set of policies and standards as employees who have access to the same information.

There appeared to be a widespread adoption of international standards for practicing data security. Fifty percent cited the popular ISO/IEC 27001 as their chosen framework, although so far no local banks have gone as far as achieving formal certification with the ISO standard. Other relevant standards followed included the Information Security Forum's Standard of Good Practice [1]and the Payment Card Industry's Data Security Standard[2].

Following a standard for data security helps ensure a consistent and complete approach to managing information security risk. Having a baseline for security also makes it possible to measure and benchmark the effectiveness of controls. When improvements are needed and management need to take action, decisions can be made on widely accepted principles.

Organisation of Information Security

The allocation of security roles in local banks was largely dependent on each organisation's size. However, it was reassuring to see that each bank had at least one individual locally with day to day responsibility for data security. Some were trained and dedicated to the role; others were not. In either case, local security representatives closely linked to central security teams located elsewhere in the group. The critical success factor is that everyone is clear on who is responsible for what, both in terms of day to day security, and in the event of a problem.

Most respondents maintained that security is a regular topic of discussion at board meetings or through various risk-focused sub-committees. Several said data security was a standing agenda item. A small number said that security was only discussed when issues arose, rather than being proactive in planning for data security threats. Some only discussed the subject annually.

With security threats ever changing, only a proactive approach to managing risk is likely to be effective. Hearing about issues after the event is not good governance, and an annual review of the topic does not constitute a comprehensive risk management process.

Information Asset Management

The term 'information assets' refers to any data that is of value; common categories include customer, corporate, and employee data. Typically in private banking the details and make-up of the customer base will be perceived as an asset and in the event of the discontinuation of the bank it may be a saleable asset. These assets usually reside in applications, databases, and paper records. Significantly most banks failed to understand what the term 'information asset' meant, with many assuming it to relate to computer equipment. This section of the ISO 27001 standard includes the following categories:

- Inventory of information assets
- Ownership of assets
- Acceptable use of assets
- Classification guidelines
- Information labelling and handling

Only one third had any form of information asset inventory. Only six had a specific information asset inventory, with many others relying on service catalogues and application registers. Without such a record of what data is held, where it is held, who controls it, how sensitive it is, and how it is protected, security breaches can be difficult to respond to. Furthermore, unless you have a clear view of what data you are trying to protect, there is no way of knowing whether you have appropriate protection in place.

Sixty percent claimed to have a data classification scheme, but only 17% had specific labelling. Several took the view that everything is confidential and applied the same level of controls across the board. This may be possible for low complexity companies, but is not an efficient way of applying security controls. A small number classified data by client, according to the client risk assessment; this is a step in the right direction.

The above gaps bring into question the true levels of awareness and compliance with the ISO 27001 standard as well as pointing to shortcomings in data leakage programmes that many banks claimed to have. It is also at odds with The Commission's Code of Practice for Banks which provides direction on several operational risk requirements, including "*Adequate system security and data protection procedures should be established*."

Human Resources Security

HR security covers the lifecycle of an employee from joining to leaving. It includes screening, granting and revoking system access, awareness training and contractual obligations for security.

All questionnaire respondents used multiple verification checks when taking on new staff and contractors. Methods included credit and police checks, and verification of references, qualifications and employment history. One performed annual credit checks on its staff, another did random re-screenings. To some follow-up verifications may seem overly intrusive but even good employees can turn bad, so 'Know Your Employee' procedures should be appropriate but thorough.

There was significant variance in banks' approaches to employee security awareness training. Some just relied on initial induction training, or self-service online materials. A number felt that AML and anti-fraud training covered information security adequately, a view that we do not share. Conversely, others approached security awareness as an on-going programme, using a mix of delivery media, pushed out regularly. Examples included tutor-led and CBT training, security bulletins, poster campaigns and even desktop calendars. This multi-pronged and continuous approach is likely to achieve the best results.

Physical and Environmental Security

Most organisations control physical access by swipe card. Further controls included CCTV and weekly reviews of computer room access. Surprisingly, some manual combination locks were still in use and some of these only had their codes changed annually, others were changed on staff departure. Changes after staff leave and at regular intervals are essential. For this reason in all but the smallest organisation, any standalone lock mechanism is unlikely to be a viable solution.

All had a clear desk policy. Several went further and practiced enforcement through regular checks of work areas, sometimes daily.

Most had a secure disposal policy, which stipulated approved disposal methods. Many required destruction to be supervised. Methods included shredding or smashing disks, incineration, and degaussing (de-magnetisation of hard disks and tapes). In some cases destruction was certified. This last step is important as it provides an audit trail of what has been sent for disposal.

Many banks were reducing the risks associated with sending backup tapes offsite by running backups directly to a secondary, secure, location. Where tapes were still transported by third parties, tapes were encrypted.

Communications and Operations Management

As expected all respondents had anti-virus software in place. However, a small number used a different anti-virus product on user workstations to the one deployed on servers. This is a more effective approach, as it provides more than one line of defence if one product should fail to detect a virus.

Nearly all had locked down USB/CDROM access. Where still used, access was limited to senior staff, or limited by business justification. One bank allowed access but logged details of all files transferred to and from USB devices. Although this approach provides no protection against a breach, it does make valuable evidence available to an investigation. Therefore an improved approach would be to limit access according to business requirement and log all file transfers.

A wide range of protective mechanisms were in place over electronic communications in and out of the organisation. Many simply did not accept client instructions electronically; this is most effective but perhaps rather restrictive. Others had secure websites with two-factor authentication (eg pin and password), or had deployed industry-standard secure email tools like PGP[3] and TLS[4]. Many were also using encrypted network links to protect internal communications with other locations. At the broader level of network communication in general, most had an integrated firewall and intrusion detection system. Nearly all purported to have network access controls in place between internal networks.

All respondents test backups, but some only through routine restores or annual Business Continuity or Disaster Recovery tests. This gives some level of comfort but fails to take into account the fact that not all systems need to be restored routinely, and an annual test that highlights a problem with a backup or tape drive may be up to twelve months too late if there is a genuine need to restore. All backups should be tested on a rolling basis. Checking a different tape set each month is usually practicable.

Several used content filtering and email scanning services. All but one blocked external webmail and instant messaging services. The bank in question had the unusual view that they believed such controls did not help combat data leakage. Both communication tools are virtually impossible to monitor and control; they provide additional channels for the spread of malware, and are a convenient tool for employees to remove data.

Of those allowing laptops, only one did not use disk encryption; in this exceptional case the machines in question were under strict physical control and not removed from the premises.

Those banks with internet banking services all commissioned penetration tests at least annually. A few had read-only services, for example online statements, which had not been fully tested. The banks in question regarded these sites as low risk, so did not feel that they required in-depth security testing. Experts would challenge the logic of this argument since any site containing customer data is an attractive target to an attacker. Even if a successful intruder cannot perform fraudulent transactions or access back-end systems they can steal customer identity information and financial records for further illegal activities. The fact that such sites are less stringently tested makes them even more attractive. All web sites should be risk assessed, and security tested to a level that is appropriate for that risk. No site should go totally untested for security weaknesses.

Access Control

Most banks performed quarterly reviews of users and their access rights. Smaller entities were less frequent, but still required line managers to recertify users.

Most performed regular reviews of firewall rules, and enforced strict controls over changes to the firewall. Some also performed monthly vulnerability scans and periodic penetration tests. Several banks relied solely on change management controls to ensure effectiveness of the firewall. A more effective approach to network security would be to include a mixture of all of these elements, rather than rely on an individual control.

Most claimed to restrict access to sensitive customer data on a 'need to know' basis. One segregated on- and off-shore customer data (so that offshore data could only be viewed locally). However, several large institutions admitted that access was not restricted by individual customer. With a large, national or international customer database this situation opens up possibilities for data leakage.

Information Systems Acquisition, Development and Maintenance

Part of our review focused specifically on End User Computing ('EUC'). This term is used to describe applications developed by business users, often using spreadsheets or databases. Spreadsheets are particularly difficult to control because once they are created they are not subject to the same access controls and auditing that formally developed applications offer. They are also much easier to copy and email, increasing the risk of data theft and accidental data leakage.

Despite these concerns there appeared to be good controls in place over extracts of customer information to spreadsheets. Leading organisations required explicit authorisation for all extracts, and had established an End User Computing policy for user-developed spreadsheets. A small number relied only on access permissions. Almost half had specific EUC policies and guidelines in place. However, when asked what controls were in place over EUC applications, only one organisation performed audits of EUC. This omission undermines the best practice already followed, so as with any control we would recommend that proper attention is given to monitoring and enforcement.

Four banks stated that they used live data in the test system, on the basis that controls were equivalent and therefore adequate. Others outlawed this practice in their policies, and had segregated systems with different access profiles. Most used anonymisation and scrambling techniques or fictitious data. Removing real customer data is essential as although a duplicate test system may appear secure when it is created, testers normally require elevated privileges, and tend to generate reports and other information in a less controlled manner than operational staff. Furthermore, test systems normally grant administrative privileges to developers, contractors and software vendors, often remotely, increasing the risk of unauthorised access even further.

Information Security Incident Management

A significant number of banks had a framework for quickly establishing an incident response team. This was usually a distributed team made up of central security specialists and local responders. Smaller organisations referred all issues to the locally nominated security officer; this may be acceptable provided the individual has adequate understanding of information security matters, and has already identified and engaged with external security specialists before an incident occurs. The skills used to deal with a security incident are very different to those needed for day to day management of information security. Security incident management shares many principles with business continuity management. Regardless of size, any organisation should have a formally documented incident response plan with the following elements:

- Roles and responsibilities for handling a suspected incident
- Reporting and escalation procedures
- Emergency contacts and external advisors
- The plan should be reviewed and tested periodically.

Compliance/Audit

Banks performed a large range of security-related reviews. This is to be expected and is consistent with the Commission's Code of Practice for Banks, which states the following requirement: "*Banks should have in place comprehensive risk management processes to identify, measure, monitor and control material risks*." However, the results in this section raise some concerns that processes are not as comprehensive as they should be.

Most have annual independent audits, in addition to other local reviews. However, three of the banks surveyed were reliant on visiting Internal Audit teams with a three-year cycle between visits. With such a low frequency of assurance, we would challenge management to meaningfully assess the effectiveness of internal controls. This approach also suggests that the organisations involved have diluted their responsibility for assessment to a control function outside the island.

Similar concerns arose over some managed entities that relied on reviews of their service providers to provide assurance over their own systems. We would question whether the managed entity has sufficient knowledge of the review scope or findings, and indeed whether any such review specifically covers the entity's own systems and control environment. For this approach to work, the managed bank needs to engage with their service provider and internal auditor (and possibly the parent bank's internal audit function) to agree the scope of the review and have full access to any relevant findings.

Others organisations took assurance from statutory external audits. This is a helpful addition to other forms of assessment, but care should be taken when relying on external auditors as the scope is specific to the financial audit. Again we would encourage banks to engage with the external auditors to discuss and understand the scope of the IT review.

We did note far more effective and proactive approaches; one bank operated a "three lines of defence" model, with main reviews being commissioned by each business unit, second level oversight by the Risk function, and finally periodic, independent reviews by Internal Audit. As well as being more thorough, this approach demonstrates the entity is taking full responsibility for control assessments, which the Commission welcomes.

Most performed some form of review of business partners. These usually followed a clearly defined assessment process, often utilising self-assessment questionnaires. Many followed up with on-site visits and independent reviews by Internal Audit. Some relied on performance reports provided by the service providers, which is informative but lacks independence. Finally, a few were reliant solely on NDAs and contractual obligations in SLAs to maintain data security, which although important, does not provide any control assessment.

We were surprised to find only one bank was subject to third party reporting ('TPR'), in this case a SAS70 report. TPR's are an independent external audit of controls, usually covering a period rather than a point in time. Reports such as the AICPA's SAS70 [5](now ISAE 3402), and ICAEW's AAF 01/06[6] are heavily focused on information security controls. Reports are intended to be provided to business partners, stakeholders and other auditors, so they can significantly raise the assurance bar.

5.3. Findings from Site Visits

Policies and Standards

Examples of good practice	Areas where improvements could be made
End-user computing policy	
Several banks had established an End User Computing ('EUC') policy to control user-developed applications such as spreadsheets and personal databases. Another bank's policy was to not support end user applications.	

Both approaches help discourage 'home-grown' applications, and the many control issues that can arise from such applications.	
Vendor management policy	
At least one bank had a formal vendor management policy in place. This policy stated the requirements for vendor assessment and included an element of IT risk reviews.	
Formal adoption of ISO/IEC 27001	
One bank had formally adopted the ISO/IEC 27001 information security framework. This internationally recognised standard allows security teams to work together to deliver information security consistently and effectively throughout the organisation.	

Organisation of Information Security

Examples of good practice	**Areas where improvements could be made**
Local security officer with business focus	
One bank had its own local dedicated Information Security Officer. This individual worked with the business to identify and address security issues. This is generally a more effective approach than having a purely technical security officer, or an IT administrator with a security role. This is because most security issues tend to arise from the business or users. Therefore engaging with the business helps to educate users, and gives the security officer a deeper understanding of the business objectives.	
Supplier due diligence	
One bank had centralised and standardised its approach to outsourcing by establishing a 'supplier selection committee'. From a data security perspective this is beneficial as it helps ensure that supplier due diligence is fit for purpose and includes consideration of data security controls.	

Information Asset Management

Examples of good practice	**Areas where improvements could be made**
Data classification policy	Data classification controls
Several banks had established an information classification policy and used protective markings (e.g. private, restricted, public). This is a fundamental principle of data security that many organisations have so far failed to implement.	Although a classification policy and protective marking scheme was in place there were no system controls to enforce policies.

	Inventory of information assets
	Surprisingly few of the banks visited were able to produce an inventory of information assets.

HR Security

Examples of good practice	**Areas where improvements could be made**
Security awareness training programme	Limited security awareness training is offered
Most of the banks visited had established a continuous education programme that included information security training. The key elements of success included: regular mandatory training, use of multiple delivery methods (classroom, online, DVD etc.), monitoring and measurement, and linkage to security related policies and procedures.	One bank had a well-developed security awareness program, which included posters and enforcement checks. However, formal training was limited to new joiners and then within annual compliance training. Offering employees a wider range of training, both in terms of frequency and format would aid both comprehension and retention.
Automation of user-provisioning	Annual declarations do not specifically cover information security obligations
Two banks used a workflow system to manage the provisioning and de-provisioning of users i.e. assignment of access rights. This is an excellent example of where technology can make security more effective. In this case by helping to process joiners and leavers in a timely manner, with approval and authorisation checks and audit trails.	As we found elsewhere, staff at one bank were required to sign a year-end confirmation covering compliance with various policies and principles. However, the confirmation did not refer explicitly to the staff handbook or any other security-specific policies.
Policy compliance linked to remuneration	User recertifications and independent review
At a large international bank a mandatory training programme and certain aspects of compliance with data security policies (e.g. clear desk and office) were linked to employee appraisals, and therefore remuneration. A robust measurement and enforcement procedure was in place to detect and follow up policy violations. The effect of this tough approach was that local line managers took far more responsibility for their individual areas, and as a result violations were very rare.	Despite having a periodic recertification process, we still found a leaver account at one bank which was no longer required. No security policy declaration was held for this individual. This highlights the importance and value of independent reviews.
Outsourced employee screening process	Social networks not used in employee screening
Many of the banks visited used a specialist vetting agency to validate a wide range of employee background information. Established facts are reconciled to the employee’s own submission and any deviations are reported in an easy to read return. Checks included credit history, criminal convictions, employment and education records. Use of a third-party for this function brings objectivity and independence that would be difficult to achieve in-house.	Employee pre-screening checks did not include reviews of social networking sites. Social media can provide valuable insights into the suitability or otherwise of future employees. Noting that many banks used external agencies for vetting, this form of screening is probably most effectively performed by local staff as they are more likely to have network connections to the individual under review.

World-Check used in screening process	Vetting procedures ignore qualifications
Several banks used World-Check as part of their employee screening process. This is a simple way to enhance the vetting process and pick up issues early on in the recruitment process.	One bank did not validate the academic achievements of prospective employees, placing more emphasis on experience. Even if qualifications are irrelevant to a position, educational records are normally easy to validate; any discrepancies can provide insight into an individual's personal integrity.
	No third party security compliance declarations
	Several issues were found with security and confidentiality compliance declarations. One bank only required its own employees to sign the declaration, even though contractors were also granted access to confidential data. Another required service providers to have their employees sign a compliance statement, but no checks were done on the supplier to ensure these declarations were made, or if they were kept up to date.

Physical and Environmental Security

Examples of good practice	**Areas where improvements could be made**
Effective data disposal procedures	Insecure confidential waste containers
Most banks had an effective approach to data disposal, both for printed and electronic media. Some lowered third-party risk considerably by supervising destruction of computer hardware on site by a destruction specialist; they then reconciled their own records against the certificated returns from the destruction company. Paper waste was best controlled by either daily shredding on site by bank staff or daily removal by facilities teams to a secure area pending bulk destruction.	Several banks held confidential waste in specially designated bins, pending removal and destruction by an external company. During two on-site visits we found confidential shredding bins that were not locked. In any case the containers and locks were of poor design and easy to compromise. If confidential waste is to be stockpiled in containers in an open office then it must be properly secured, or removed from the main office each day. Any movement of confidential waste should be supervised by bank staff.
Clear office policy	
Rather than a 'clear-desk' policy, one bank we visited had extended the principle to a 'clear-office' policy. This is a logical approach to office security, and encourages employees to think beyond the confines of their own workspace.	

Communications and Operations Management

Examples of good practice	**Areas where improvements could be made**
Internal vulnerability scanning	IT service provider access unmonitored
In addition to other technical assessments one bank scanned its internal servers every month for	One bank outsourced its IT functions to a local service provider. However, there was no

security vulnerabilities. This is a simple way of highlighting common vulnerabilities and picking up security misconfigurations early before they lead to problems.	monitoring of the privileged activities performed by the provider. The bank claimed that the service provider's contractual obligations covered data security. This may be the case, but legal requirements are only a deterrent, and do not remove responsibility from the bank. In any case terms in company contracts are normally rather detached from the individuals who actually perform the work. Governance would be improved by having oversight of the actions performed. At a basic level we would expect the bank/firm to receive a periodic report of system accesses and the purpose of the access.
	Firewall does not restrict outbound traffic
	One network administrator explained that the bank's firewalls did not restrict outbound traffic. As with other access controls, firewall rules should be set to deny by default and explicitly allow only those services that are necessary. Failure to restrict access in this way makes it much easier for an attacker or malware to covertly transfer information out of the organisation; it is also more difficult to monitor and identify abnormal network activity if everything is allowed through.

Access Control

Examples of good practice	**Areas where improvements could be made**
Application restricts client data downloads	Title
Reacting to data leakage concerns, one bank put application access controls in place to prevent client relationship managers from downloading client data. Although this is a technical control, it also sends a message to employees that the organisation is serious about protecting client data which is an asset/resource owned by the bank.	One bank only performed annual reviews of user rights, with the justification that there were few employees and turnover was low. Nevertheless an annual review is too infrequent to detect exceptions in a timely manner. Instead a more pragmatic approach would have been to perform high-level interim reviews quarterly (e.g. dormant accounts and leavers) and less frequent reviews of access rights and privileges. However, most organisations should have sufficient changes to require full quarterly reviews.
Electronic diary system for compliance checks	USB device blocking software missing
One bank used an electronic reminder system as a simple but highly effective means of prompting and documenting a wide range of compliance activities, of which data security reviews formed a significant part. The system helped ensure that checks were done on time and correctly, and provided an audit trail to demonstrate that checks had been performed, and captured the results of	Despite rolling out USB device blocking software across the organisation, we found that a computer in the bank's boardroom did not have USB device blocking enabled. We would normally expect automated processes to be in place to detect and report policy violations like this before they are discovered by anyone else.

each review. Overdue checks were automatically escalated to the individual's line manager.	
Bespoke recertification reporting system	Single-factor authentication for remote access
One bank had developed its own application for user recertifications. Normally recertifications involve circulating large volumes of reports showing user rights and access levels. The reports are often difficult to understand, particularly by non-technical business users. In this case the bank had created an application that presented reviewers with user information in a meaningful and easy to review format.	We were surprised to find one bank that was still using a remote access system with single-factor authentication i.e. just a username and password. Single factor authentication is strongly discouraged for any form of remote access and should be replaced with strong two-factor authentication e.g. password and PIN or token.

Information Systems Acquisition, Development and Maintenance

Examples of good practice	**Areas where improvements could be made**
Live data is anonymised before use in test system	
One bank scrambled and anonymised live data for use in a test system using a specially developed tool. Live user profiles were also removed and replaced with test accounts. This approach significantly reduces the risk of data leakage from development systems.	

Information Security Incident Management

Examples of good practice	**Areas where improvements could be made**
Incident response procedures in place	No formal incident response plan
Most banks had established security incident management procedures, and defined roles and responsibilities. This helps team members work together effectively whether they are locally or centrally based.	One bank did not have a formally documented Incident Response Plan ('IRP'). Ideally an IRP should be established that clearly defines procedures for incident escalation, handling of potential evidence and liaison with third parties. The latter should include security specialists, law enforcement, the media and affected customers. Roles and responsibilities for incident handlers should be defined and plans should be reviewed and tested periodically.

Compliance/Audit

There were no findings in this category from the on-site visits.

6. Conclusions and Summary of Findings

In this review we found many examples of good practice with relatively few areas for improvement. However, data security is a rapidly moving area and demands a process of continuous improvement. Therefore, even those banks with the highly effective security controls will be able to build on the findings of this review. The Commission's main findings are as follows:

- Most employees were formally required to agree their on-going compliance with data security policies, but several did not share their policies with third-party handlers of customer data.
- Internationally recognised standards for data security were widely followed, with half adopting the principles of ISO/IEC 27001[7].
- All had implemented a wide range of data leakage prevention controls. However, surprisingly few had an inventory of information assets (i.e. what data is held, its sensitivity, who owns it etc.), and only a small number had begun to implement data classification and protective markings.
- Most had comprehensive employee vetting procedures, usually engaging an external specialist agency to screen prospective employees. Several used World-check to enhance this process. However, only a few performed follow-up checks, and none claimed to review social networking sites for employee suitability.
- Security awareness training approaches varied greatly but the most effective used a wide variety of training methods, delivered at regular intervals.
- All had clear desk and some clear office policies, with several performing regular spot checks to ensure compliance with policy.
- All had either removed, restricted or monitored USB/CD ROM access.
- Those banks with transactional internet banking services commissioned regular penetration tests. However, some had read-only services and these had not been tested for security vulnerabilities.
- Most banks performed quarterly reviews of user rights. To make the review easier for non-technical line managers, one bank had developed its own application to present the rights assignments in a meaningful form to the reviewer for recertification.
- There appeared to be good controls in place over end-user applications, with many having specific policies governing their use. One organisation had prevented relationship managers from downloading customer data completely.
- Approaches to using live data in test systems varied. One bank scrambled and sanitised customer data before using it for testing, others felt live data could be used provided user rights were equivalent to the live system, even though test systems are usually more open to developers and third parties. The Commission would discourage access to live data.
- All banks were subject to a wide range of compliance checks and audits. However, few seemed proactive in this area, commissioning their own control reviews and risk assessments. Instead they tended to rely on the work of others, usually external or internal audit, whether or not it provided relevant risk coverage. One notable exception supplemented these externally driven reviews with additional reviews driven by the Risk department and individual business units.
- A few banks had begun to implement workflow applications for user provisioning. This way they were able to leverage technology to make the joiner/leaver process more secure.
- Procedures for disposal of printed and electronic media were generally good. Many combined on-site supervision with a certificated audit trail for hardware disposal. Others removed confidential waste from open office areas on a daily basis.
- One bank performed monthly vulnerability scans on its internal servers.
- One had an impressive diary system for driving and documenting periodic compliance checks. The results from some of these checks, notably clear desk policy, were included in employee performance appraisals. This was a tough but highly effective policy enforcement tool.

7. Glossary of terms

Account	A unique user login identifier.
Application firewall	An application firewall is a form of firewall which controls input, output, and/or access from, to, or by an application or service. Examples include web applications and databases. Application firewalls can block flaws in the logic of the underlying application.
Content filtering	A system to block or allow user internet activity based on the type of website and predefined keywords. Content filtering is also performed on email activity to prevent data leakage and spam.
Data leakage	A security breach where data has been lost, stolen or otherwise exposed externally.
Encryption	Technology used to scramble and descramble data so that it cannot be read or modified by unauthorised parties.
End user computing / end user applications	Applications created by end-users without the involvement of IT or software development teams. Common examples are spreadsheet models, and databases created for manipulation and reporting of data drawn from central systems.
Formal process	The process that is defined in an approved and documented procedure. When executed formal processes normally are normally recorded using standard forms or systems that can easily be audited to evidence completion and approval. Email-based processes do not normally constitute formal processes.
Formal review	A review that is planned and follows an agreed methodology. Evidence of the review, and any actions arising are documented and retained for future inspection.
Information assets	Any definable piece of information that is classed as 'valuable' to the organisation.
Instant messaging	Online chat systems such as Windows Messenger, Facebook chat, Lotus Sametime, Twitter etc.
Intrusion detection / prevention systems (IDS/IPS)	Software applications which monitor network activity looking for known patterns of attack. Preventative systems can automatically terminate the offending session.
Malware	A general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or programme code.
NDA	Non-disclosure agreement.

Port security	A function of a network switch or router that only allows traffic to pass to and from a predefined network address.
Protective markings	A classification system used to identify documents and communications at different security levels. Common examples are RESTRICTED, CONFIDENTAL and SECRET.
Provisioning/de-provisioning	Creating and removing accounts for users and leavers.
Recertification	The periodic review of user rights.
Rulebase / ruleset	A firewall ruleset is a table of instructions that the firewall uses for determining what types of network traffic are allowed or rejected by the firewall.
Two-factor authentication	An authentication process that uses more than one of the following: something you know (e.g. Password, PIN), something you are (facial features/IRIS/fingerprint), or something you have (smartcard, SecureID token, dongle)
Vulnerability and Threat Management Program (VTMP)	VTMP is an implementation roadmap for identifying and addressing technical vulnerabilities. It includes inventory, configuration standards, patching, scanning and penetration testing, and risk analysis and remediation.
Webmail	Internet-based email systems such as hotmail, Windows Live, Yahoomail, Gmail and Cable and Wireless

8. Acknowledgements

The Commission would like to thank all of the banks that completed the initial questionnaire. Particular thanks should also go to the banks that agreed to have site visits. The time and effort they spent in supplying the requested documentation and discussing their approach to data security was much appreciated and yielded some excellent evidence of good practice.

9. Useful reference sources

[1] Information Security Forum www.securityforum.org

[2] Payment card industry data security standard (PCI DSS) www.pcisecuritystandards.org

[3] Pretty Good Privacy www.symantec.com/business/theme.jsp?themeid=pgp

[4] Transport Layer Security searchsecurity.techtarget.com/tip/Using-TLS-encryption

[5] American Institute of CPAs (SAS70 / ISAE 3402) www.aicpa.org

[6] Institute of Chartered Accountants in England and Wales (AAF 01/06) www.icaew.com

[7] International Standards Organisation (ISO 27001) www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103