Jersey Financial Services Commission

BANKING BUSINESS

THEMED EXAMINATION PROGRAMME 2011: INFORMATION SECURITY SUMMARY FINDINGS

Issued: March 2012

GLOSSARY OF TERMS

The following table sets out a glossary of terms used in this report.

Content filtering	Content filtering is the technique whereby content is blocked or allowed based on analysis of its content, rather than its source of other criteria. It is most widely used on the internet to filter email and web access.
Encryption	Encryption is the conversion of data into a form that cannot be easily understood by unauthorised people.
End User computing/ End User Developed Applications	End User Developed Applications are applications created by non IT staff in the course of their work, most typically spreadsheets and databases.
Instant messaging	Online chat systems such as Facebook, Twitter and Windows Messenger.
Intrusion detection/prevention systems	Network monitoring software intended to identify known methods of attack.
ISO27001	An Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
Least privilege access	Giving staff only those access rights which are essential to do their work.
Removable media	Storage media which is designed to be removed from the computer without powering the computer off e.g. CDs, DVDs, memory cards.

CONTENTS

1 Executive summary

1.1 Introduction

1.1.1 This report provides an overview of the findings from a themed on-site examination exercise conducted by the Banking Division of the Jersey Financial Services Commission (the "**Commission**") on the topic of Information Security ("**IS**") during 2011.

1.1.2 The findings in this report are drawn from five on-site examinations of banks conducted by Commission staff as well as responses to a self-assessment questionnaire that was sent to each of the banking groups represented in Jersey.

1.1.3 This exercise was carried out in co-ordination with the Guernsey Financial Services Commission which also undertook a thematic examination on the topic of information security during 2011.

1.2 Findings

1.2.1 Overall, the Commission found that banks in Jersey were well advanced in implementing their IS policies and procedures.

1.2.2 In the main, the Commission found that the IS policies adopted were benchmarked against international standards and, as such, were comprehensive in scope. Where banks tended to vary was in the extent to which the IS policy had been implemented in practice. Those banks that had appointed a dedicated local information security officer tended to be better advanced.

1.2.3 Areas in which banks tended to be well advanced as a whole included:

- Adoption of an IS policy;
- Adoption of clean desk policies;
- Adoption of removable media policies;
- Implementing physical access controls;
- Implementing appropriate network controls;
- Adopting malicious code protection;
- Adopting appropriate procedures for the use of test data; and
- Adopting incident management procedures.

1.2.4 Those areas potentially requiring further focus were as follows:

- Regular discussion of IS issues by the board or equivalent;
- Requiring that IS officers possess relevant qualifications;
- Implementing controls around End User Developed Applications ("**EUDAs**");
- Monitoring outsourced staff vetting;
- Vetting staff on an on-going basis;
- Implementing e-mail controls; and
- Incorporating additional controls around the use of customer data for marketing purposes.

1.3 Conclusion

1.3.1 The Commission would encourage all banks to consider the findings in this report in the context of their own business.

1.3.2 The Commission has issued individual reports with relevant recommendations to those banks that received an on-site examination.

1.3.3 Those banks that did not receive an on-site examination have submitted a self-assessment questionnaire to the Commission which, in some cases, will form the basis for further discussion of this topic.

2 Introduction

2.1 Objectives and limitations

2.1.1 The Commission regularly undertakes on-site examinations on specific themes to assess the extent to which regulated entities are operating in accordance with their obligations under the respective Laws, Orders, Codes of Practice and Guidance Notes. These examinations focus on identifying instances where depositors, customers or the registered entity itself may be at risk or where standards and practices required by the regulatory regime are not being observed.

2.1.2 The Commission's on-site examination programme is designed to:

2.1.2.1 assess the risks faced by the entity and review the controls, procedures, policies and processes in place to mitigate those risks;

2.1.2.2 obtain a greater understanding of the entity's activities, thereby enabling the Commission to focus attention on higher risk areas; and

2.1.2.3 take into account existing relevant information, review the resolution of any previous examination issues and to obtain assurance on any deficiencies highlighted through off-site supervision.

2.1.3 This review did not cover all aspects of IS and the findings set out in this report should be treated as examples of good practice rather than formal regulatory guidance.

2.1.4 IS is considered a pertinent topic owing to the increasing risk that customer data might be lost or stolen and then used to commit fraud or other crimes. There have been a number of high profile examples of data loss in recent years involving not only financial services but also the public sector. Banks in Jersey are not immune to such risks which, in most serious cases, have the potential to damage not only their own reputation but also that of Jersey as an international finance centre.

2.2 Methodology

2.2.1 This examination programme was undertaken by way of a self-assessment questionnaire and a series of on-site examinations.

2.2.2 A self-assessment questionnaire was prepared with the assistance of an external IS consultant, Carl Ceillam. This was based around the ISO27001 standard and comprised of 60 questions covering the following topic areas:

- Information security policy;
- Organisation and governance of information security;
- Information inventory;
- Human resources;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition and development;
- Incident management; and
- Compliance and audit.

2.2.3 The self-assessment questionnaire was completed by eighteen banking groups. A further five banks received a three day on-site examination from the Commission covering the same subject areas.

2.3 Regulatory Requirements

2.3.1 Jersey registered deposit-takers are required to adhere to the Codes of Practice for Deposit-taking Business (the "**Banking Codes**") which are issued by the Commission under Article 19A of the Banking Business (Jersey) Law 1991. The Banking Codes set out the requirements for, *inter alia*, the risk management framework that must be maintained by Jersey deposit-takers and contain the following provisions considered relevant to IS:

3 A registered person must organise and control its affairs effectively for the proper performance of its business activities and be able to demonstrate the existence of adequate risk management systems

A registered person's systems must ensure that:

3.2.1.10 Adequate procedures are in place for controlling changes to systems and records to ensure that only valid changes are made to such systems and records; and

3.2.1.11 Adequate logical access controls are in place to protect the confidentiality and integrity of electronic assets.

3.7.1 A registered person must ensure that its directors, senior managers and all other employees are fit and proper for their roles. The term "employees" includes not only staff directly employed by the registered person but also indirect employees such as temporary or contracted employees and other contracted service providers.

A registered person must:

3.7.2.4 Adequately vet and monitor the probity of its directors, senior managers and other employees.

3 Findings

3.1 Organisation of Information Security

Governance

3.1.1 IS is a broad ranging topic which needs to be properly co-ordinated across the business. A potential pitfall is to regard IS as a purely Information Technology ("**IT**") issue when in fact internal audit, compliance, facilities management and Human Resources ("**HR**") all have important roles to play.

3.1.2 The Commission found that approaches to the governance of IS varied depending on the size and nature of the Jersey operation. Some of the banks had adopted IS as a standing agenda item for board meetings. However, a more typical approach was to discuss IS through a relevant risk sub-committee of the Board.

3.1.3 Some banks exhibited a largely reactive approach to IS whereby the topic would only be addressed on an ad-hoc basis in response to IS breach incidents or through the cascade of relevant technology or policy changes instigated by the bank's parent group.

3.1.4 Overall, it was found that a little under 60% of the banks sampled considered IS as a regular standing agenda item with the remainder considering the issue on a more ad hoc basis.

Good Practice:

- The bank has a regular standing agenda item at which IS is proactively considered, drawing in all relevant parts of the business.

Poor practice:

- IS is considered on a purely reactive basis, if at all.
- IS is regarded as an "IT issue".

Policies and procedures

3.1.5 Without exception, the banks sampled had adopted an IS policy developed by their parent group. These polices were typically benchmarked against international standards (most often ISO27001) and were therefore similar in scope.

3.1.6 Where banks tended to vary was in the level of adoption of the group policy. In some of the cases examined, it was accepted that certain aspects of the IS policy had yet to be fully implemented across the group and consequently the local operation had been granted a waiver or exception from the relevant part of the group policy.

3.1.7 Some common areas that had yet to be fully adopted included:

3.1.7.1 The adoption of a full inventory of information assets;

3.1.7.2 Full implementation of EUDA policies; and

3.1.7.3 Implementing e-mail security controls.

3.1.8 Whilst banks tended to be good at ensuring that their own staff were aware of the IS policy, some had failed to adequately communicate the policy to relevant third party contractors.

Good Practice:

- A group policy, benchmarked against international standards is adopted.
- Relevant parts of the IS policy are adapted into tailored "dos and don'ts" factsheets for staff and contractors.

Poor practice:

- The bank has failed to adopt a comprehensive IS policy.
- The bank is relying upon extensive waivers from the group IS policy.

Information Security Officer ("ISO")

3.1.9 Most of the banks sampled had appointed an individual with responsibility for IS. In the case of larger banks, an ISO (or equivalent) had been appointed locally; smaller operations often fell within the responsibility of a regional ISO.

3.1.10 Unsurprisingly, those firms that had appointed an ISO tended to perform better in the on-site examinations and self-assessment questionnaire. The most successful approaches were where a dedicated ISO, or equivalent, had been appointed with responsibility to liaise with all relevant parts of the business on IS. In some cases the ISO was an incidental role undertaken by a senior person in the IT department. In such cases there is a risk that non-IT aspects of IS might be overlooked (e.g. human resources, facilities management and compliance monitoring).

3.1.11 A common theme emerging from the IS self-assessment questionnaires was that the ISO is not typically obliged to hold an IS qualification. In a number of cases the appointed ISO held relevant qualifications, such as Certified Information Security Manager ("**CISM**") and Certified Information Systems Security Professional ("**CISSP**"). However, it was rare that this was a mandatory requirement for the role.

Good Practice:

- The bank appoints a dedicated ISO with relevant experience, training, and qualifications.
- The ISO has responsibility for liaising with all relevant parts of the business on IS matters.

Poor practice:

- There is no dedicated ISO, or equivalent.
- IS is considered solely the responsibility of the IT department.

3.2 Outsourcing

3.2.1 Risk assessment and standard contract clauses

3.2.2 Without exception, the banks surveyed relied upon some form of outsourcing, whether within their own group or to external suppliers. The Commission focussed on those outsourcing arrangements that involved the handling of customer data in order to establish:

3.2.2.1 what level of initial vetting that was undertaken upon the outsourcee;

3.2.2.2 whether on-going monitoring was performed; and

3.2.2.3 whether standard contract terms governing confidentiality, service levels and the right to audit were used.

3.2.3 The majority of banks performed well in this area, with almost 80% having adopted a formal third party procurement process involving a standardised risk assessment of the third party vendor. The best examples of this were where the bank had adopted a risk based approach and therefore focussed its efforts on those contracts representing the greatest impact in the event of a breach.

3.2.4 This formalised approach resulted in a contract containing standardised terms around confidentiality and the right to audit, as well as establishing clear performance expectations against which the bank would monitor.

3.2.5 Those banks performing less well in this area had not insisted on standard contract terms. A number of the banks sampled had self-identified this as an area for improvement and were already in the process of reviewing their legacy outsourcing contracts.

Good Practice:

- The bank has adopted an initial, risk based, assessment process for its third party contractors.
- The bank insists upon standard clauses governing customer confidentiality, service levels and the right to audit.
- Contractors are made aware of relevant parts of the bank's IS policy.
- The bank monitors adherence to the contract on an on-going basis.
- Outsourcing due diligence procedures include the requirement for service providers to complete self-assessment questionnaires covering IS controls.

Poor practice:

- No formal risk assessment is undertaken.
- The bank has not insisted on standardised contract clauses.

3.3 Asset Management

Inventory of information assets

3.3.1 In order to safeguard information assets, it is first necessary for the business to identify what it wishes to protect and to record its location.

3.3.2 Most of the banks sampled had adopted an IS policy which required that information assets be classified, assigned an owner and recorded on a central inventory. However, in practice, a significant number had not progressed beyond establishing a register of physical assets (e.g. laptops, USB sticks) and were yet to extend this to information held in applications, databases and paper files.

Good Practice:

- The bank interprets "information assets" in its wider sense, to include data as well as computer hardware.
- An inventory is maintained recording what is held, where it is located, who controls the data and how it is protected.

Poor practice:

- Limiting the inventory to computer hardware.

3.4 Human Resources

Initial and on-going vetting

3.4.1 Vetting the probity of staff is a key component of safeguarding information assets.

3.4.2 Banks tended to perform well in this area. Without exception, the banks sampled conducted pre-employment vetting of their staff. For permanent staff this work tended to be undertaken by the bank itself, either through the local Human Resources function or through a centralised group vetting function. The vetting of temporary staff was more often undertaken by recruitment agencies operating to an agreed standard under a service level agreement with the bank.

3.4.3 The scope of vetting tended to include, inter alia:

3.4.3.1 Police checks;

3.4.3.2 Past employer references;

3.4.3.3 Credit checks; and

3.4.3.4 Qualification checks.

3.4.4 In some cases, a more rigorous set of checks was applied to certain roles (typically those involving the giving of investment advice to customers).

3.4.5 Some potential areas for improvement were that:

3.4.5.1 A number of the banks examined were found not to be conducting checks against the list of individuals that the Commission has restricted from working in the finance industry. Registered persons are urged to incorporate a check against the Commission's register of restricted individuals as part of their vetting process.

3.4.5.2 The register is available on the Commission's website at http://www.jerseyfsc.org/the_commission/general_information/public_statements/RegisterOfRestrictedIndividuals.asp.

3.4.5.3 In some cases, it was noted that, where vetting has been outsourced to a group vetting function or to a local recruitment agency, the bank has not sought to exercise its rights to audit the performance of the function. The Commission would expect banks to verify that staff vetting is being completed to an acceptable standard through sample checking.

3.4.5.4 Finally, few of the banks had adopted any formal process for the on-going vetting of staff. In some cases, the bank had adopted a policy to undertake updated or additional vetting where an individual was appointed to a new role within the organisation (particularly roles involving the giving of advice to customers). A number of banks conducted informal on-going vetting against convictions reported in the local paper and the petty debt court lists; however, this process tended to be informal.

Good Practice:

- Staff are subject to both initial and on-going vetting. Vetting is also updated when there is a change of the employee's role.
- Temporary staff are subject to the same level of vetting.
- All key credentials are validated independently of the information provided by the individual.

Poor practice:

- Outsourcing of vetting without appropriate monitoring.
- Failing to check against the Commission's register of restricted persons.

Contract terms

3.4.6 The Commission explored whether staff contract terms contained relevant clauses in relation to IS and the non-disclosure of customer data. These topics were tended to be addressed either within the staff contract or within the staff handbook.

Good Practice:

- Standard contract clauses and/or cover this area in the staff handbook with an annual attestation.

Poor practice:

- In at least one case, a bank had a number of staff working under legacy contracts which did not contain relevant information security and customer confidentiality clauses. Banks should review legacy contracts and, where relevant, seek to bring them up to a common standard.

Training

3.4.7 Proper staff training is an important safeguard against data loss. Training also helps ensure that policies are understood and practiced. This was an area in which clear distinctions could be drawn between the banks. At one end of the spectrum, a number of banks considered it sufficient to place their data security policy and procedures on the intranet and to expect that their staff read and understand them. Occupying the middle ground were banks that required that their employees attest to having read and understood the policy at induction and on annual basis thereafter.

3.4.8 Best practice was exhibited by those banks that prepared training materials, often delivered via computer based training, which helped bring the IS policy to life. In some cases, staff were required to achieve a pass rate, with their performance being advised to line management.

Good Practice:

- Regular IS training, tailored to the role being undertaken.
- Induction training with periodic attestation as a minimum.
- Innovative approaches designed to bring the subject to life for staff.

Poor practice:

- Assuming that staff have read and understood the IS policy.
- Policies that are highly technical and difficult to read.

3.5 Physical Security

Physical access controls

3.5.1 In the majority of cases examined, the banks had adopted a swipe card or fob based electronic access control system whereby employee access was restricted to defined zones within the bank's premises. Some areas will be subject to highly restricted access, most typically the IT server room and any treasury dealing rooms.

3.5.2 In some cases, the Commission made the observation that generic access cards had been created to give access to external contractors. This was considered to be a potential risk, particularly where the bank does not insist on external contractors being accompanied at all times within the building.

3.5.3 A further observation was that some banks should limit the access to highly restricted areas still further, particularly in cases where permanent access to premises had been granted to external contractors.

3.5.4 Manual digilocks had been retained by a small minority of banks (13%) however, these tended to be in less sensitive areas and codes were typically changed with appropriate frequency.

3.5.5 There was some divergence between the banks in terms of the audit logs maintained for access records and CCTV footage. Best practice was for regular exception reporting to be produced (failed access attempts, access out of hours etc.) and considered by local management. Poor practice in this area tended to be a lack of exception reporting and the overwriting of audit logs.

Good Practice:

- Role based access controls, assigned under a dual sign off process.
- Dual factor access controls in the most sensitive areas.
- "Least privilege" based approach to assigning access rights.
- Regular exception reporting and the retention of audit logs.

Poor practice:

- Use of digilocks in sensitive areas.
- Use of generic contractor access cards.
- Allowing unaccompanied contractor access, particularly to sensitive areas.

Clear desk policy

3.5.6 All of the banks had adopted a clear desk policy. This aspect of IS appears to be commonly understood and tends to be regularly enforced through on the spot inspections. One point that was noted during the on-site examinations was that the clear desk policy tends to be one of the few aspects of IS that is monitored by the Compliance department. Banks must ensure that there is a comprehensive monitoring plan in place for all aspects of IS and that undue focus is not placed on non-technical aspects simply because they are comparatively straightforward to test.

3.6 Communications and operations

Removable media policy

3.6.1 The majority of banks sampled had restricted the use of removable media such as USB storage devises and CDs by locking down all relevant ports and drives and only permitting such access to staff with a genuine business need.

3.6.2 Where such access is permitted, an important additional safeguard is to require that any data placed upon removable media is encrypted. In a number of cases, banks were making use of specialist software to control and monitor the use of removable media.

Good Practice:

- Only permitting the use of removable media where there is a genuine business need.
- Ensuring that any removable media is encrypted.
- Monitoring any unauthorised attempts to download data to a removable storage device.
- Logging of files transferred to and from removable devices.

Poor practice:

- Lack of controls over removable media.
- Allowing some staff permanent access to removable media when only temporary access is required.

Destruction policy

3.6.3 The destruction of customer information encompasses not only paper based records but also computer hardware in order to ensure that all traces of customer data have been rendered irrecoverable. Banks had typically adopted a group IS policy which included detailed procedures for the destruction of paper based records and computer hardware. This process was often outsourced, making the findings at 3.2 of this report relevant.

3.6.4 Examples of best practice in this area were for the destruction of computer hardware to either be performed in house or to a certified standard by a third party supplier.

Good Practice:

- Use of locked confidential waste bins.
- Effective monitoring of the performance of outsourced providers.
- Timely and effective destruction of obsolete computer hardware.

Poor practice:

- Relying on outsourced providers without proper monitoring.

E-mail controls

3.6.5 In most cases banks have implemented website content filtering software that prevents their staff from accessing webmail accounts (e.g. Hotmail, Gmail, Yahoo).

3.6.6 Just over 60% of the banks sampled had implemented further controls around the use of e-mails including:

3.6.6.1 E-mail encryption;

3.6.6.2 File size limitation;

3.6.6.3 Content scanning and blocking software;

3.6.6.4 Limits on the number of recipients; and

3.6.6.5 Disabling the autocomplete e-mail address function.

3.6.7 The Commission noted that there were very few examples where the bank had simply removed external e-mail access from those staff that did not have a business need for it. One bank explained that restricting such access would be an impediment to staff having full access to its internet based training solutions however, the Commission formed the impression that external e-mail access may not be approached on a "least privilege" basis in the same way as other applications.

Good Practice:

- Blocking webmail and instant messaging facilities.
- Limiting external e-mail access to those staff with a genuine business need.
- Imposing limits on attachments and the number of addressees.
- Use of e-mail encryption.
- Use of content scanning/blocking tools.

Poor practice:

- Unrestricted access.
- Reliance on staff policies without monitoring and secondary controls.

Malicious code protection

3.6.8 The banks sampled all made use of anti-virus software and over 90% of the banks sampled confirmed that they were making use of intrusion detection/prevention systems, application firewalls or other protection mechanisms.

3.6.9 The Commission formed the view that this was an area of strong adherence to best practice, likely reflecting standard IT infrastructure requirements imposed by the banks' parent groups.

Good Practice:

- Multi-layered defences against malware i.e. anti-virus software, network intrusion/prevention systems, browser restrictions.
- End users and critical servers use different antivirus products.
- Antivirus signatures monitored to ensure all devices are up to date.

Poor practice:

- Reliance solely on desktop anti-virus for protection.
- Failing to check that all devices have up to date anti-virus software.

Internet banking

3.6.10 A number of the banks examined offered an internet banking facility to their customers. Clearly such a service introduces additional risks and the Commission sought to understand what additional safeguards had been adopted by the bank in developing and monitoring such facilities.

3.6.11 In all cases where internet banking facilities had been developed, the bank confirmed that a secure software development lifecycle methodology had been followed when developing the system and that regular penetration testing was being conducted.

3.7 Access control

Joiners/Movers/Leavers process

3.7.1 An important IS protective measure is to ensure that staff are granted an appropriate level of access to the bank's systems, based on the role that they perform. In order to control and monitor this effectively, it is important that a bank adopts a rigorous process for assigning access rights upon recruitment and when an employee changes role or leaves the organisation.

3.7.2 All of the banks sampled claimed to have adopted a formal joiners/movers and leavers process but the Commission identified some differences in approach when undertaking its on-site examinations. Those banks with the best controls in this area had adopted role based access control, whereby each role within the bank is assigned a predetermined set of access rights to the bank's systems based on a "least privilege" approach. The Commission found that this approach, whilst challenging to initially implement, offered the best safeguard against employees being assigned inappropriate access rights.

3.7.3 All of the banks that received an on-site examination required that line managers confirm that their staff had appropriate access rights on a periodic (at least quarterly) basis. However, the Commission made the observation, in at least one case, that the reports provided to managers were so complex that it was unlikely that any meaningful check was being achieved in practice. A role based approach was found to make such checking more straightforward.

Good Practice:

- Granting access rights based on standardised, role based profiles.
- Providing managers with clear and intelligible staff profiles to check against.
- Use of timely independent checks to ensure that access rights have been properly assigned or removed.
- Regular reconciliation of access rights to HR records.

Poor practice:

- Assigning access rights on an ad-hoc basis.
- Lack of effective independent checking of access rights.
- Failure to fully disable user profiles when an employee leaves the bank.

3.8 Information systems

End User Computing/End User Developed Applications ("EUDAs")

3.8.1 EUDAs are applications that are developed by the bank's staff in the course of their work, most typically involving databases or spreadsheets. The potential risks associated with EUDAs are that they may contain sensitive or restricted data or support a critical business function without having commensurate access and audit controls.

3.8.2 Best practice is for the bank to identify the EUDAs being used by its staff, and to ensure that these are subject to appropriate controls based upon the level of risk that they represent. Such controls might include:

3.8.2.1 File or folder level access controls;

3.8.2.2 Sheet and cell level protection;

3.8.2.3 File naming conventions;

3.8.2.4 Version control; and

3.8.2.5 Data integrity checks.

3.8.3 Implementing a EUDA policy is challenging in practice, given the sheer volume of legacy applications that will have been developed by staff across the business over a long period of time. Responses to the self-assessment questionnaire indicated that this is an area in which banks still have some way to develop, with only 35% of the banks sampled having fully implemented their EUDA policy.

3.8.4 Of the banks sampled through on-site examinations, it was noted that those that had progressed furthest in this area had adopted a two pronged approach: firstly, the EUDA policy had been rolled out using a staff awareness programme in order to give practical examples and guidance. This approach was then supplemented by the use of technology. In one case, the bank had considerably eased the scope of the task of identifying its EUDAs by simply moving any spreadsheet that had not been accessed for a given length of time to a secure part of the network and then waiting to see whether anybody asked where it had gone. The Commission also noted that some banks were using specialist software to identify any spreadsheets meeting defined parameters (file size, complexity) and then reconciling these against their register of EUDAs.

Good Practice:

- Identifying EUDAs and assigning risk based controls.
- Ensuring that staff are aware of and understand the EUDA policy.
- Using technology to identify potential EUDAs.
- Replacement of business-critical EUDAs with formally developed applications.

Poor practice:

- Failing to establish whether the EUDA policy is understood and is being followed in practice.

Use of test data

3.8.5 The use of test data can expose the bank to risk because it releases customer data to a test environment where it may be subject to less stringent user access controls. There is also a risk that test data could corrupt the bank's records if it is not properly segregated. Of the banks sampled, 95% had implemented controls around the use of test data. Typical controls implemented were for all test data to be made anonymous prior to use or, where live data was allowed to be used, for its release to be approved by the relevant business owner and for it to remain segregated through to disposal.

Use of customer data for marketing

3.8.6 The Commission asked banks whether they had established additional controls where customer data was used for marketing purposes. Some 35% of the banks had not adopted such controls, which represents a potential risk where, for example, an extract from the customer database is manually manipulated before being used to generate a mailshot. Examples of good practice in this area were for independent data validation reviews to be undertaken prior to any mailshot being produced.

3.9 Incident management

3.9.1 An overwhelming majority (over 90%) of the banks sampled claimed to have adopted a formal IS incident management procedure. These procedures tended to form part of a broader policy adopted by the parent group and would typically involve a local response team that reports into a group IS incident management function.

3.9.2 It was noted that several of the banks sampled had yet to test their IS incident response plan and it is therefore recommended that this is undertaken, possibly in conjunction with any on-going business continuity testing.

Good Practice:

- The bank adopts and regularly tests a formal incident response plan, setting out clear roles and responsibilities and reporting lines.

Poor practice:

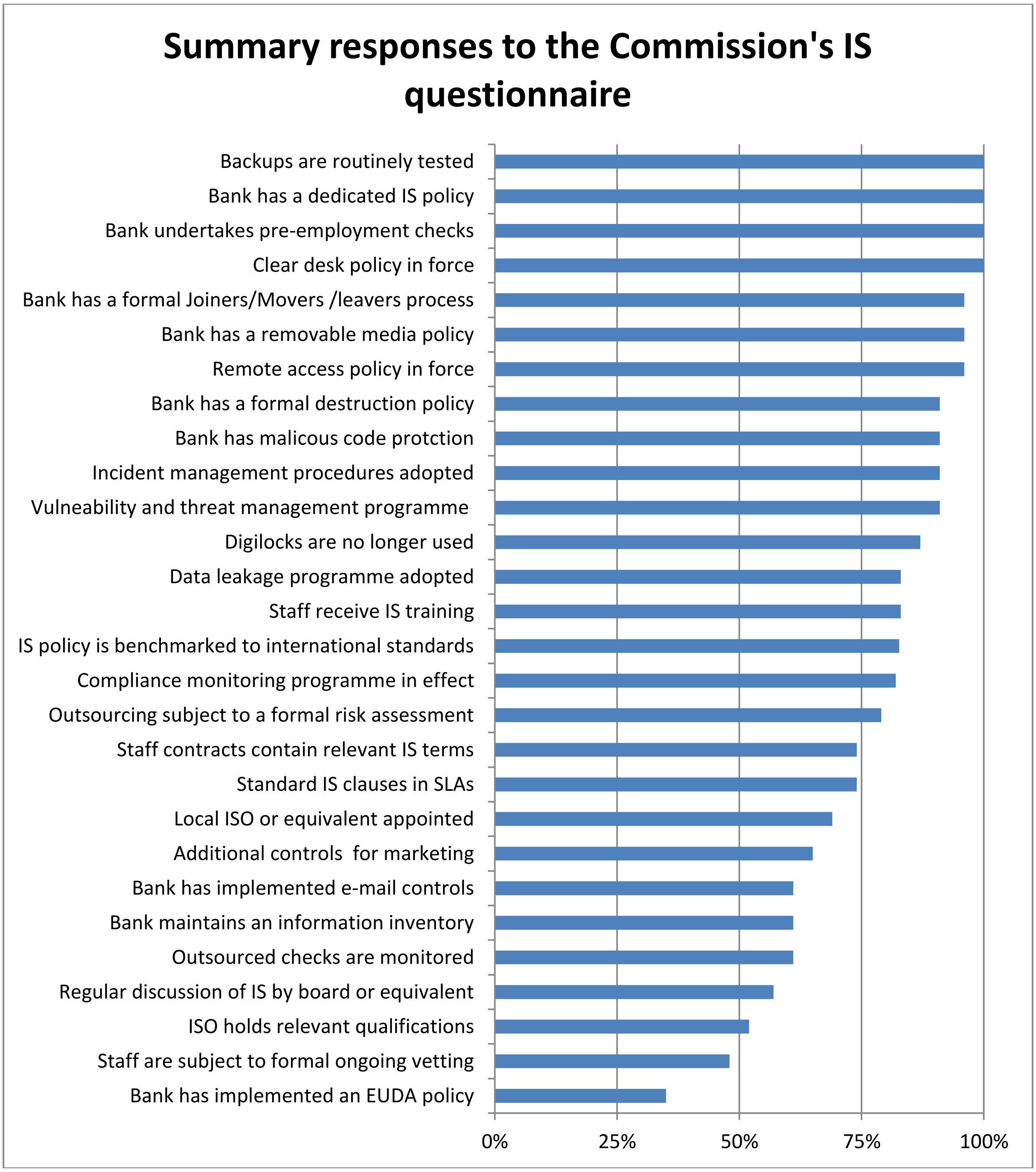
- Failing to adopt or to test a response plan.

3.10 Compliance and audit

3.10.1 The Commission regularly meets with internal audit teams visiting the Island and is aware that IS and IT control reviews are now a regular feature of most group internal audit programs.

3.10.2 Where the bank is not subject to regular internal audit reviews on this topic, it is especially important that an effective compliance monitoring programme is adopted and, if necessary, augmented through the use of external auditors or consultants. The Commission found that compliance monitoring of IS was in some cases quite limited, with a focus on non-technical areas such as the clear desk policy. This is understandable; however, it is important that technical aspects of IS are subject to appropriate monitoring, drawing on specialist functions from within the group where necessary.

4 Statistical Overview



ACKNOWLEDGEMENTS AND FURTHER READING

The Commission wishes to thank those banks that participated in this exercise for their co-operation and assistance.

The Commission also acknowledges the assistance of Carl Ceillam CISSP, EnCE in designing the audit tools and questionnaire used in this themed examination programme and for providing training to those members of the Commission that undertook the on-site examinations.

Persons wishing to gain a further insight into this topic may wish to consult the following websites and publications:

- Information Security Forum www.securityforum.org
- International Standards Organisation (ISO27001) www.iso.org
- The Financial Services Authority, "Data Security in Financial Services" (April, 2008) http://www.fsa.gov.uk/pubs/other/data_security.pdf

The Commission would welcome comments on any of the contents of this report and would also be happy to address any concerns or questions that the reader may have in this respect. Any such communications should be addressed to the relevant Supervision Manager or, where this does not apply, to:

Darren Boschat
Deputy Director, Banking

Tel: +44 (1534) 822060
E-mail: d.boschat@jerseyfsc.org