INFORMATION TECHNOLOGY AUDIT REPORT
OF FISCAL SERVICES LIMITED (FSL)
REVIEW OF GENERAL COMPUTER CONTROLS

Auditor General of Jamaica
Auditor General's Department
8 Waterloo Road, Kingston 10
Jamaica, W.I.
www.auditorgeneral.gov.jm

August 2011

Table of Contents

EXECUTIVE SUMMARY

Fiscal Services Limited (FSL) is the major technology link in the information flow between the revenue departments, the taxpayers and the Government of Jamaica (GoJ). Among its primary functions is the establishment of a comprehensive monitoring programme of all revenue activities, the development and management of systems to improve tax billing and collection as well as to determine the tax liability and collection status of all taxpayer accounts. Ultimately, the Government relies on the information provided by FSL to improve its revenue forecasting and decision-making.

FSL developed and or supports fifty-one (51) IT systems. Jamaica Customs and Tax Administration Jamaica (TAJ) accounts for the largest number of systems with fourteen (14) and thirteen (13) systems respectively while the other systems include trade facilitation, payroll and financial management systems. It is therefore important that FSL have a very strong control environment especially as it relates to its Information and Communication Technology (ICT) resources to ensure that these systems are not compromised.

Our audit focused on assessing the effectiveness of FSL's general computer controls to determine whether adequate systems, policies and procedures were in place in relation to FSL's core activities, i.e. the provision of ICT services and support to the Government of Jamaica.

Key Findings

CORPORATE GOVERNANCE

1. The company has been without a permanently appointed Managing Director since December 2008. The absence of such a key leadership figure with security of tenure has negatively affected the development and implementation of certain key strategies, policies and procedures that are necessary for a strong control environment. For example, we noted that at least four (4) relevant policy documents including the *Disaster Preparedness and Recovery Plan* were in various draft stages, with two of them being in draft for at least one year.

2. FSL does not have a properly constituted Procurement Committee in accordance with the Government of Jamaica Handbook of Public Sector Procurement. The functions of the Procurement Committee were instead being undertaken by a sub-committee of the Board of Directors which included the acting Managing Director, in breach of GoJ procurement rules. We were able to identify procurements totalling US$ 6,025,816 and JA$100,126,659 that were approved by this committee over the last three years [2008-2010].

3. Despite having a formal policy as well as other guidelines relating to engaging individuals on fixed term employment contracts, FSL was guilty of engaging persons on fixed term employment contracts without the prior written approval of the Ministry of Finance and

the Public Service (MoFPS). We noted the engagement of at least seven individuals at senior levels within FSL on fixed term employment contracts totaling approximately $33.7M per annum without receiving prior approval from the Ministry of Finance and the Public Service. An additional twenty-five (25) other individuals were engaged to posts that were not on FSL's approved establishment resulting in unapproved expenditure of approximately $43M per annum.

4. FSL has failed to consistently comply with its personnel clearance procedures by ensuring that academic credentials submitted by employees or prospective employees are verified with the respective academic/professional institutions. We identified 41 cases where there was no evidence that the employees had the qualifications claimed as no copies of their certificates were on file neither were there any relevant correspondences from the respective academic/professional institutions. This increases the risk that FSL may employ individuals who provide it with fictitious qualifications.

INFORMATION SYSTEM SECURITY

5. Good information system security involves the analysis and management of risks to protect the organisation's information. Risk analysis involves determining the value of each information system to the organisation as well as the degree to which the organisation is exposed to risk. We found that FSL does not have an information systems value assessment mechanism to effectively assess the value of each GoJ information system and the information contained within them. This reduces management's ability to evaluate the business impact of security threats and related risks.

6. There is no formal documented comprehensive Information Security Policy to provide general direction for protecting the confidentiality, integrity and availability of corporate information within FSL. The development of such a policy is currently a work-in-progress. Consequently, greater reliance is placed on the experience of certain key personnel within the organisation leading to a higher information security risk especially within the context of a relatively high staff turnover.

7. Within FSL, there is no designated function or officer(s) to ensure that there is a consistent and co-ordinated approach to information systems security across the organisation. This increases the risk of security vulnerabilities remaining undetected especially since there is no system in place to ensure that all log reports are reviewed periodically to quickly identify unusual activities. Furthermore, FSL lacks the appropriate mechanism to monitor the activities of privileged users and administrators to ensure that they are not abusing or mis-using their access rights. Consequently, irregularities could go undetected, which may lead to the compromise of the organization's systems.

8. FSL does not have an automated network access control system to prevent unauthorized individuals from attaching a device on its network and accessing system resources without management's knowledge. This activity is currently being manually monitored but this is not likely to be very effective given the size of FSL's network and the fact that security officers do not always record or log all electrical equipment at the various points of entry.

PHYSICAL AND ENVIRONMENTAL SECURITY

9. FSL's security policy and procedures outline in detail the circumstances under which visitors are allowed on the company's premises. However, there is no requirement in the policy for visitors to provide proof of identification in order to gain entry to the premises. As a result, FSL is not in a position to properly identify all visitors to the organization. Given the sensitive nature and the critical importance of the data being managed at this facility, all visitors should be required to provide proof of identification in order to gain access.

10. FSL's environmental controls include fire prevention, detection and suppression systems to reduce the occurrence and impact of fire on the company's premises. We, however, observed that there were no fire alarms and kitchen suppression systems in the FSL kitchen/canteen, a usually high-risk area for fires in most organisations. Consequently, the company's entire operations could be jeopardized in the event of a fire occurring in the kitchen/canteen and there is no fire suppression system to reduce its effects.

BUSINESS CONTINUITY MANAGEMENT

11. FSL is currently developing a Disaster Preparedness and Recovery Plan to manage the impact of unplanned service disruption. However, the draft plan does not adequately address the issue of periodic testing procedures to ensure that the plan remains relevant and effective in the event of a disaster. We also found that there is no system in place to ensure that backup media are regularly tested to determine the integrity and completeness of the backup files. This may lead to further complications and delays in the event of an unplanned disruption especially if backup media are corrupted or other circumstances have changed subsequent to the last review of the plan.

Recommendations

1. The FSL Board should, as soon as is practicable take the necessary steps to appoint a full-time Managing Director with a mandate to build an environment that fosters high quality service, integrity, accountability and job satisfaction. The success of any organization especially one in a fast changing sector such as ICT largely depends on effective and stable leadership.

2. FSL should reconstitute its Procurement Committee in keeping with the provisions of the Government of Jamaica Handbook of Public Sector Procurement Procedures [Vol. 1-General Provisions: Section 2.2.5]. The new committee should comprise of no more than 40% of Board members excluding the Chairman and the Managing Director who are not eligible to sit on the Procurement Committee. Potential members of the Procurement Committee should also receive training in GoJ procurement procedures before being selected to serve.

3. The management of Fiscal Services Limited should take immediate steps to ensure that all fixed term employment contracts at the level of *Department Head and above* are approved by the Ministry with responsibility for the Public Service in accordance with Section 20 of

the Public Bodies Management and Accountability (PBMA) Act and FSL's Human Resources Policy Manual. FSL should also engage the Ministry with responsibility for the Public Service to regularize the current situation where individuals are employed to posts that are not on FSL's approved establishment. Additional safeguards should also be implemented to prevent a recurrence of these breaches.

4. The FSL management should ensure that it complies with its personnel clearance procedures in relation to the verification of academic qualifications submitted by employees/prospective employees in order to reduce the risk of employing individuals who provide fictitious qualifications.

5. Information system security best practice requires organisations to determine the value of their information systems as part of their information systems security risk assessment. The value of each information system and the information contained within them directly influences an organisation's decision-making process. We therefore recommend that the management of Fiscal Services Ltd as part of its information systems security risk assessment include an information systems value assessment mechanism in order to increase their ability to effectively assess the business impact of security threats and related risks.

6. The completion of a comprehensive information security policy and the assignment of a designated information security function within FSL with the appropriate staff should be treated as a matter of priority in order to reduce the reliance now being placed on the experience of certain key personnel to drive information system security.

7. Consistent with best practice and international standards, FSL should implement a system of periodic reviews of all network/system logs and ensure that the activities of privileged users and administrators are monitored. The company should also urgently implement the necessary automated network access control system to prevent unauthorized individuals from accessing its IT resources.

8. Given the sensitive nature and the critical importance of the data being managed by Fiscal Services Limited, all visitors should be required to provide proof of identification in order to gain access to the premises. This will serve to strengthen the controls over physical access to the organization's facility.

9. As part of its environmental control mechanism, FSL should ensure that its premises are properly equipped with fire prevention, detection and suppression systems especially at locations that are susceptible to fires such as their canteen and kitchen. The company should, therefore, as a matter of priority take the necessary steps to install an appropriate fire alarm and fire suppression system in its kitchen and canteen in order to reduce the impact of a fire.

10. FSL should conduct periodic tests of backup media and business continuity plans to ensure that its systems can be effectively recovered and shortcomings adequately addressed prior to a disaster occurring. The results of these tests should also be documented for analysis and review.

Conclusion

Fiscal Services Limited has the lead role in the development and implementation of information systems for various Government departments, in particular the revenue departments. The organization is mandated to provide on-going operating service, support and maintenance for these systems and to ensure that controls are in place to maintain the integrity of all data within them. We found that certain controls within the organization were not consistently complied with while others were absent or not adequately reviewed or monitored in accordance with international standards and best practice. Consequently, FSL's capacity to guarantee the security and operational efficiency of the information systems under its control may be impaired if the potential information systems security risks are materialized.

We therefore urge the management of FSL to carefully review the recommendations contained in this report with a view to strengthening their control systems by adopting the measures outlined.

PART ONE Introduction

Audit Scope and Methodology

1.1 The Auditor General, in keeping with Sections 25 and 30 of the Financial Administration and Audit Act commissioned an audit of Fiscal Services Limited (FSL) to determine whether adequate systems, policies and procedures were in place in relation to FSL's core activities, i.e. the provision of information and communication technology (ICT) services and support to the Government of Jamaica. The audit assessed the effectiveness of FSL's control environment and its impact on the level of service delivery.

1.2 Our audit was planned and performed in accordance with the following Information Technology/Information Systems Standards for audit, governance and security:

- Information Technology Audit and Assurance Standards and Guidelines issued by the Information Systems Audit and Control Association (ISACA)[1];
- International Standards of Supreme Audit Institutions (ISSAI) 5310: Information System Security Review Methodology issued by the International Organization of Supreme Audit Institutions (INTOSAI)[2];
- Control Objectives for Information and related Technology (COBIT) issued by the IT Governance Institute[3];
- ISO 27000 family of standards dealing with Information Security Management issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)[4].

These standards enabled us to test and compare FSL's general computer controls against international benchmarks and widely accepted best practices within the ICT sector.

1.3 Information systems controls involve specific activities performed by people (manual) or by systems (automatic) to ensure the confidentiality and integrity of data as well as the continuity of Information and Communication Technology (ICT) systems. These controls can be divided into two broad categories: application controls and general controls. Application controls apply to specific software programs or "Applications". These Applications or Programs are used to facilitate key business processes within an organization, e.g. Payroll and Accounts are typical processes that are dependent on software applications. Application controls are designed to ensure the complete and accurate processing of data from input to output. They ensure that only authorized data is

[1] https://www.isaca.org/Pages/default.aspx
[2] http://www.issai.org/media%28421,1033%29/ISSAI_5310_E.pdf
[3] http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
[4] http://www.iso.org

accepted and that output is reliable. On the other hand general computer controls apply to computing systems as a whole. These comprise the processing environment including management of computer resources, file access, change control, contingency planning and backup.

1.4 Weak general controls could cause application controls to be ineffective because application controls are dependent on general controls. Effective general controls therefore, form the foundation for effective application controls.

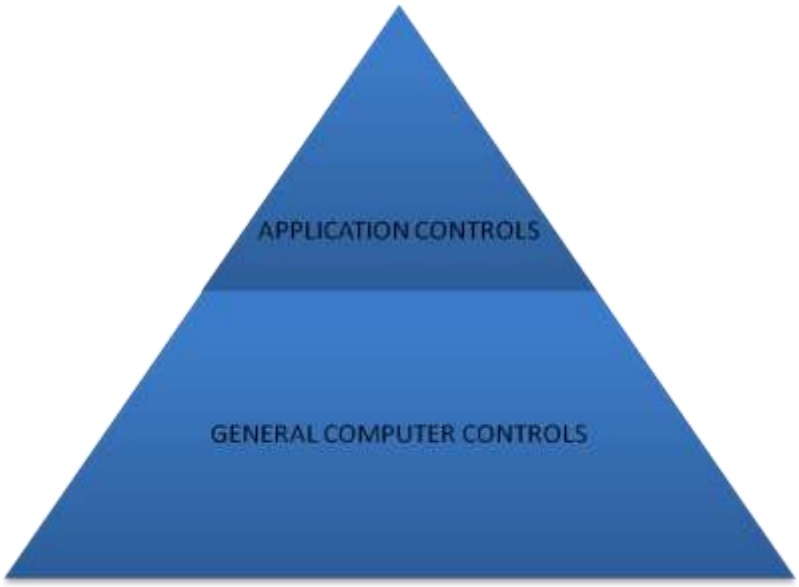

Figure 1: Information Systems Controls

1.5 Our audit focused on assessing the efficiency and effectiveness of FSL's general computer controls to ensure that systems, policies and procedures are in place to preserve the integrity and confidentiality of data as well as the continuity of various Government of Jamaica (GoJ) computer systems. This involved the review and testing of controls in the following areas:

- Physical and Environmental Security;
- Access Controls and System/Network Security;
- Business Continuity and Disaster recovery;
- Change Management and Control;
- Management of Human Resources and Corporate Governance.

1.6 The planning process involved gaining a thorough understanding of the mandate, role and functions of Fiscal Services Limited (FSL) and the nature and extent of Information and Communication Technology (ICT) services it provides to the Government of Jamaica and other entities. This information allowed us to formulate a risk based approach in determining the specific areas to be targeted for review.

1.7 The audit did not include network penetration testing and therefore, our assessment is based on the review of internal and external documents, observations and interviews with senior officers and staff of Fiscal Services Limited.

Background

1.8 Fiscal Services Limited (FSL) was incorporated as a limited liability company under the Companies Act of Jamaica on April 15, 1985 and commenced operations one year later (April 1986). The Revenue Board on behalf of the Government of Jamaica initially held the authorized shares but these were subsequently transferred on March 31, 1991 to the Accountant General, a corporation sole pursuant to the powers vested in him by the Crown Property (Vesting) Act 1960.

1.9 Upon commencement of operations, FSL immediately assumed the lead role in the development and implementation of information systems for various revenue departments, providing on-going operating service, support and training in keeping with the Government's Tax Administration Reform Programme. FSL has effectively become the major technology link in the information flow between the revenue departments, the taxpayers and the Government of Jamaica.

1.10 FSL's stated mission is "*to provide value added ICT solutions to the Government of Jamaica's revenue departments and other clients by employing international best practices through a talented and highly engaged team of professionals, while enhancing earnings and other expectations of stakeholders*"[5]. The objectives of the company at establishment include:

a. To carry on the business of computer service and to establish a comprehensive monitoring programme of all revenue activities;

b. To improve the tax billing and collection system;

c. To determine the tax liability and collection status of all taxpayer accounts;

d. To provide information for the purposes of widening the tax base and improving revenue forecasting;

e. To make available at a price, general time shared computer services to public and private sector institutions;

f. To provide consulting services and advice on all aspects of the planning, design, operation and implementation of computer systems, including management information, control and planning systems[6].

1.11 Consistent with its mission, FSL provides a variety of ICT services to the Government of Jamaica with its primary client base comprising Jamaica Customs and Tax Administration

[5] Source: http://www.fsl.org.jm
[6] Source: Memorandum of Association of Fiscal Services (EDP) Limited

Jamaica **[Appendix 1]**. However, in recent years it has sought to provide ICT services to other governments as well as private sector entities. Currently, the systems that were developed and or supported are grouped in the following categories:

A. **Government of Jamaica (GoJ) Revenue Services Computerization** – These are systems developed and supported for GoJ departments and agencies that facilitate revenue collection **[Appendix 2(a)]**.

B. **Government of Jamaica (GoJ) Trade Facilitation Systems** – These are systems developed to enable smoother, more efficient Government to Customer, Government-to-Government interactions relating to trade. Several of these systems facilitate online application and payment for permits and licenses **[Appendix 2(b)]**.

C. **Other Computerized Systems** – These systems have been developed and or supported for other clients including some GOJ departments and agencies **[Appendix 2(c)]**.

D. **Infrastructure Systems** – These are developments of Network and Computer Hardware infrastructural solutions to meet clients' business needs **[Appendix 2(d)]**.

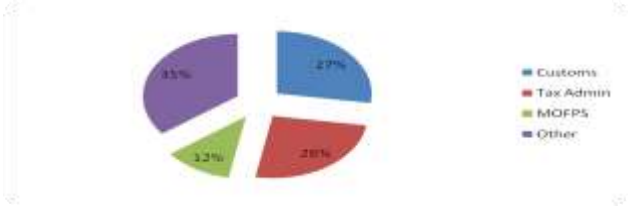

Figure 2: Number of systems developed and or supported by FSL

PART TWO Corporate Governance

FSL Is Without a Permanently Appointed Managing Director

2.1 FSL is a government agency that reports to the Ministry of Finance. A 12 member Board of Directors, appointed by the Finance Minister, is responsible for setting policies and for overall corporate governance. The responsibility for the daily operations of the entity rests with the Managing Director (MD). The MD's role involves the strategic alignment of business goals, the management of risk, resources and performance as well as ensuring that FSL delivers value for money.

2.2 We however, observed that since December 2008, the Board of FSL has not appointed a full-time Managing Director to take charge of the entity's daily operations and strategic direction. Instead, during the ensuing period two members of staff were assigned to act as Managing Director, one of whom has subsequently resigned.

2.3 The Board's delay in permanently appointing a Managing Director is likely to create some level of uncertainty within the leadership of FSL and may negatively affect the development and implementation of necessary strategies, policies and procedures resulting in a weaker control environment.

2.4 The FSL Board should, as soon as is practicable take the necessary steps to appoint a full-time Managing Director with a mandate to build an environment that fosters high quality service, integrity, accountability and job satisfaction. The success of any organization especially one in a fast changing sector such as ICT largely depends on effective and stable leadership.

FSL in Breach of GoJ Procurement Guidelines

2.5 The Government of Jamaica Handbook of Public Sector Procurement Procedures [Volume 1-General Provisions] requires each GoJ procuring entity to establish a Procurement Committee. The Committee shall be constituted in accordance with the following guidelines[7]:

(a) It must consist of not less than five (5) persons and shall include:
   i. A senior financial management personnel; and
   ii. Four (4) other appropriately qualified Public Officers.

(b) Members of the Procurement Committee should have received training in GoJ procurement procedures before being selected to serve.

(c) Board members shall not comprise more than 40% of the entity's Procurement Committee.

[7] Government of Jamaica Handbook of Public Sector Procurement Procedures [Vol. 1-General Provisions: Section 2.2.5]

(d) The Chairman of the Board and the Head of the Procuring Entity shall not sit on the Procurement Committee.

2.6 We however, found that FSL does not have an appropriately constituted Procurement Committee in accordance with the GoJ Procurement Procedures outlined above. The functions of the Procurement Committee were instead being undertaken by a sub-committee of the Board of Directors – the Technical and Research & Development sub-committee. This sub-committee is made up entirely of Board members including the acting Managing Director. We were able to identify procurements totalling US$ 6,025,816.64 and JA$100,126,659.71 that were approved by this committee over the last three years [2008-2010].

2.7 This level of involvement by the Board and the MD in the procurement process may lead to possible conflicts of interest especially in relation to the MD since certain procurements will require his specific approval and authority. FSL should therefore reconstitute its Procurement Committee in keeping with the provisions of the Government of Jamaica Handbook of Public Sector Procurement.

2.8 The management of FSL subsequently informed us that they have recognized the breach and will take the necessary steps to establish a Procurement Committee in accordance with the procurement guidelines.

FSL Issues Multi-million Dollar Employment Contracts without the Ministry of Finance's Prior Approval

2.9 Fiscal Services Limited, as a public body, is subject to the directions of its portfolio ministry as well as to the provisions of the Public Bodies Management and Accountability (PBMA) Act. Section 20 of the PBMA Act requires that in relation to emoluments the board shall act in accordance with such guidelines as are issued from time to time by the Minister responsible for the public service. Additionally, FSL's Human Resources' Policy Manual requires that for fixed term employment contracts at the level of *Department Head and above*, approval must first be obtained from one of the following:

a. Portfolio Ministry;
b. Ministry of Public Services;
c. Attorney General.

2.10 We found that despite having a formal policy and other guidelines relating to fixed term employment contracts, FSL was guilty of engaging persons on fixed term employment contracts without the prior written approval of the Ministry of Finance and the Public Service (MoFPS). We noted the engagement of at least seven individuals at senior levels within FSL on fixed term employment contracts without the prior approval of the Ministry of Finance and the Public Service costing approximately $33.7M per annum.

Table 1: Employment contracts without MoFPS prior approval[8]

Post	Total Annual Emoluments
Director of Finance and Planning	6,116,124.32
IT Consultant	4,849,562.00
Manager, Application Engineering	4,170,000.00
Software Engineering Project Lead	4,287,062.00
Director, Human Resources & Administration	3,903,102.32
Department Head-ISU	5,682,563.00
ICT Project Manager	4,732,500.00
TOTAL	**33,740,913.64**

2.11 Furthermore, we also observed where at least twenty-five (25) other individuals were engaged to posts that were not on FSL's approved establishment resulting in unapproved expenditure of approximately $43M per annum.

Table 2: Employment in Unapproved Posts[8]

Division	No. Of Unapproved Posts	Total Annual Emoluments
E-Government	4	6,481,349.28
HR & Administration	11	12,754,125.52
Software Engineering	6	12,560,395.92
Technical Services	4	11,245,609.28
TOTAL	**25**	**43,041,480.00**

2.12 FSL has failed to comply with its own human resources policy as well as guidelines from the Ministry of Finance and the Public Service, effectively resulting in substantial amounts of unapproved expenditure. The management of Fiscal Services Limited should therefore take immediate steps to have these matters regularized through the Ministry with responsibility for the Public Service and ensure that going forward, the company complies with its human resources policy and the GoJ guidelines.

FSL Fails To Comply With Its Personnel Clearance Procedures

2.13 Typically, personnel clearance procedures in most organizations include individual background checks in relation to criminal convictions, past employer and reference verifications as well as confirmation of certificates of qualifications submitted by current/prospective employees. FSL adopts these procedures as part of its employment screening process and we conducted tests to determine the extent of compliance by the entity.

2.14 We observed 41 cases where copies of qualifications were not present on the employee's personal file to substantiate their credentials. We were therefore unable to verify whether these employees satisfied FSL's qualification criteria. Furthermore, there is no evidence that FSL took the necessary steps to determine whether these individuals actually possessed the requisite qualifications claimed in accordance with its Human Resources Policy. The management should ensure that it complies with its personnel clearance

[8] Compiled and analyzed from data provided by FSL.

procedures in relation to the verification of educational certificates submitted by current/prospective employees in order to reduce the risk of employing individuals who provide fictitious qualifications.

Table 3: No. Of Employees with No Proof of Qualifications[9]

Division	No. Of Employees
Executive Management	04
Technical Services	17
Finance & Planning	01
Software Engineering	19
Total	**41**

[9] Data compiled by the Auditor General's Department.

Part Three Information System Security

System Security Framework

3.1 The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents[10]. The first step to safe computing is adoption of information and administrative management policies and measures, which embrace principles of good security management[11].

Information Security Risk Assessment

3.2 Good security involves the analysis and management of risks to protect the organisation's information. Risk analysis involves determining the value of each information system to the organisation as well as the degree to which the organisation is exposed to risk. On the other hand, risk management involves selecting the controls and security measures that reduce the organisation's exposure to risk to an acceptable level[11].

3.3 In conducting our review of FSL's information system security, we sought to determine whether management has conducted any form of risk assessment or analysis to determine the entity's vulnerability status. Our investigations revealed that the most recent assessment was done in 2009 and involved an analysis of the likelihood and impact of various security threats. The analysis, however, failed to determine the value of each system to the organisation/Government of Jamaica and rank them accordingly.

3.4 We further observed that in the Software Engineering Division's *Disaster Preparedness and Recovery Plan* certain systems were classified as either *critical* or *non-critical.* Systems classified as critical required a restoration time of between 24 & 48 hours. This, however, cannot compensate for the lack of a comprehensive assessment of the value of each system to the organisation/Government as this plan does not take into account all systems managed by FSL neither has it been updated since 2005.

3.5 The value of each information system and the information contained therein impacts on the organisation's business decisions. Therefore, the absence of an information systems value assessment mechanism reduces management's ability to effectively assess the business impact of security threats and related risks.

[10] COBIT 4.1- DS5: Ensure Systems Security
[11] ISSAI 5310: Information System Security Review Methodology

Information Security Administration

3.6 Information security policy is a formal statement that defines top management intentions on information security and provides general direction for protecting the confidentiality, integrity and availability of corporate information[12]. The implementation, monitoring and enforcement of such a policy are usually the responsibility of a designated Information Security Officer, who usually reports to the head of the organisation or to an Information Systems Steering Committee on all information security related matters.

3.7 Presently, FSL's Information Security Policy is a work-in-progress. Aspects of the policy that have already been developed include:

- *Data Classification Standard (Draft)*
- *Workstation Security Policy*
- *IT Acceptable Usage Policy*
- *Email Acceptable Usage Policy (Draft)*
- *Internet Acceptable Usage Policy (Draft)*
- *Remote Access Usage Policy*
- *Password Policy*

However, the absence of a formal documented comprehensive Information Security Policy creates a situation where greater reliance is placed on the experience of certain key personnel within the organisation. This creates a dilemma for FSL especially within the context of a relatively high staff turnover as within the last four years (2007-2010) FSL has experienced an average annual attrition of 21 employees per annum.

3.8 We also found that the responsibility for information security within FSL is dispersed across at least three departments with major responsibility residing with the Network and Facilities Department. Consequently, there is no designated function or officer(s) to ensure that there is a consistent and co-ordinated approach to security across the organisation. This increases the risk of security vulnerabilities remaining undetected. For example, we found that there were reasonably adequate intrusion protection systems in place to guard against external attacks but there was no mechanism to ensure that the logs produced by these systems were thoroughly examined on a periodic basis so as to quickly identify unusual activities. Furthermore, FSL does not have an automated system to prevent unauthorized individuals from attaching a device on its network and accessing system resources without management's knowledge. This activity is currently being manually monitored but this is not likely to be very effective given the size of FSL's network and the fact that security officers do not always record or log all electrical equipment at the various points of entry.

3.9 Our investigations also revealed that there is no system in place to monitor the activities of privileged users and administrators to ensure that they are not abusing or mis-using their access rights. For example, we observed that the password for a Manager within the Technical Services Division, who is also a member of the Administrators Group, was set to

[12] INTOSAI EDP Information Systems Auditing: Glossary of Terms

"never expire" contrary to FSL's password policy. The officer's password was last set on 12/8/2008 and at the time of the audit, we noted that the officer last logged on at 2:00am on 4/25/2011, which was a public holiday. Additionally, the user account of a former employee from the Quality Management division had remained active even though the officer had resigned in December 2010.

3.10 FSL's failure to effectively monitor all network activities could result in irregularities going undetected which could compromise its systems. Additionally, the absence of the above monitoring and review mechanisms may affect FSL's drive towards obtaining ISO and other international information security management certifications.

3.11 The organization should therefore, implement a system of periodic reviews of all network/system logs and ensure that the activities of privileged users and administrators are monitored. FSL should also urgently implement the necessary network access control to prevent unauthorized individuals from accessing its system resources.

3.12 The management of FSL has subsequently advised us that they are in the process of engaging a Consultant to co-ordinate and formalize FSL's IT security as well as prepare the entity for ISO 27001 certification. They also confirmed that the Ministry of Finance has provided budgetary support to acquire an Automated Network Access Control (NAC) system to improve FSL's overall network security.

Physical and Environmental Security

3.13 Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel[13].

3.14 We found that FSL has implemented a range of physical and environmental controls aimed at ensuring that the physical and environmental resources of the organisation are adequately secured. There is a Security Policy and Procedures Manual that outlines the company's security policy and procedures and these are monitored by the Administration Department. All access points are manned by security personnel and access to the building requires appropriate authorization. Access is also restricted to certain sensitive areas such as the Computer Suite and the Main Equipment Room. Controls are also in place to protect electrical and network cables as well as computer hardware and accessories.

3.15 FSL's security policy requires members of staff to produce their ID to security personnel when entering the building and display it at all times when on the company's premises. However, there is no requirement for visitors to provide proof of identification in order to gain entry to the premises. Given the sensitive nature and the critical importance of the data being managed at this facility, all visitors should be required to provide proof of

[13] COBIT 4.1-DS12: Manage the Physical Environment

identification in order to gain access. This will serve to strengthen the controls over physical access to the organization's facility. This is an issue the management of FSL has recognized and is reviewing as part of the upgrading of its security system.

3.16 The environmental controls adopted by FSL includes:

- Fire prevention, detection and suppression systems and training;
- Temperature and humidity controls;
- Uninterruptible Power Supply (UPS) and Alternate Power Supply (Generator) systems.

We, however, observed that there were no fire alarms and kitchen suppression systems in the FSL kitchen/canteen. This is a high-risk area for fires and all steps should be taken to ensure that an appropriate fire suppression system is installed which will turn off the gas supply in the event of a fire.

Part Four Business Continuity Management

Backup, Disaster Preparedness and Recovery

4.1 The need for providing continuous IT services requires developing, maintaining and testing IT/business continuity plans, utilising offsite backup storage and providing periodic continuity plan training[14]. By their nature, contingency plans are needed infrequently and at a time when the organisation is under stress. There is a risk that they will become out-dated or be unavailable when an emergency arises. Therefore, best practice requires that contingency plans be reviewed and tested at regular intervals[15].

4.2 FSL is currently developing a Disaster Preparedness and Recovery Plan to manage the impact of unplanned service disruption. However, the draft plan does not adequately address the issue of periodic testing procedures to ensure that the plan remains relevant and effective in the event of a disaster. We also found that there is no system in place to ensure that backup media are regularly tested to determine the integrity and completeness of the backup files.

4.3 If FSL fails to periodically test its continuity plans and procedures this may lead to complications and delays in the event of an unplanned disruption especially if backup media are corrupted or other circumstances have changed subsequent to the last review of the plan. We therefore recommend that FSL test and document the test results of backup media and continuity plans on a regular basis to ensure that all systems can be effectively recovered and shortcomings adequately addressed prior to a disaster occurring.

Pamela Monroe Ellis, FCCA, FCA, CISA
Auditor General

[14] COBIT 4.1-DS4: Ensure Continuous Service
[15] ISSAI 5310: Information System Security Review Methodology

APPENDIX

APPENDIX 1: ICT Services Provided By FSL[16]

- **A.** Application Hosting and Support Services;
- **B.** Customer Relationship Management (CRM) and Help Desk Services;
- **C.** Hosting Services;
- **D.** Infrastructure Design and Development;
- **E.** Validation Web Services, Licences, Permits and Certificates;
- **F.** Procurement Consultancy;
- **G.** Project Management;
- **H.** Quality Management Services;
- **I.** Software Development and Implementation;
- **J.** Training Room Facilities;
- **K.** Work Space Planning Services.

APPENDIX 2: Systems Developed and Supported By FSL

(a) Government of Jamaica (GoJ) Revenue Services Systems:

- **i.** Automated Motor Vehicle System (AMVS);
- **ii.** Customs Automated Systems (a total of 14 systems);
- **iii.** Integrated Computerized Tax Administration System (ICTAS);
- **iv.** Integrated New Cash Remittance System (INCRS);
- **v.** Jamaica Tax Online Portal;
- **vi.** Land Valuation System (LVS);
- **vii.** Property Tax System (PTS);
- **viii.** Stamp Office Information System (SOIS);
- **ix.** Tax Compliance Certificate (TCC);
- **x.** Taxpayer Registration Number (TRN);
- ***xi.*** Tax Reminder System (TaxRem).

(b) Government of Jamaica (GoJ) Trade Facilitation Systems:

- **i.** Bureau of Standards Trade System (BSTS);
- **ii.** Ministry of Agriculture Trade System (MOATS);
- **iii.** Ministry of Health Trade System (MOHTS);
- **iv.** Trade Board Information System (TBIS);

[16] Source: http://www.fsl.org.jm

v. Trade Registration System (TRS).

(c) Other Computerized Systems:

i. Automated Pension System (APS);
ii. Bank Reconciliation System (BRS);
iii. Financial Management Information System (FMIS);
iv. Jamaica Budget Information System (JaBIS);
v. Jamaica Constabulary Force Cashiering System (JCFCS);
vi. Licensing Management Information System (LMIS);
vii. NIS, HEART & JCF Data Subscription Services;
viii. Nurses & Midwives License Information System (NMLIS);
ix. Payroll System;
x. Securities Management System (SMS);
xi. Traffic Ticket Management System (TTMS).

(d) Infrastructure Systems:

i. FISCNET (A Wide Area Network to serve the communication needs of the Revenue Departments).