INFORMATION TECHNOLOGY AUDIT REPORT

ON

INFORMATION TECHNOLOGY GOVERNANCE

OF

SELECT PUBLIC ENTITIES (JCF, JIS & MOFPS)

The Auditor General is appointed by the Governor General and is required by the Constitution, Financial Administration and Audit Act, other sundry acts and letters of engagement, to conduct audits at least once per year of the accounts, financial transactions, operations and financial statements of central government ministries and departments, local government agencies, statutory bodies and government companies.

The Department is headed by the Auditor General, Pamela Monroe Ellis, who submits her reports to the Speaker of the House of Representatives in accordance with Section 122 of the Constitution of Jamaica and Section 29 of the Financial Administration and Audit Act.

This report was prepared by the Auditor General's Department of Jamaica for presentation to the House of Representatives.

Auditor General of Jamaica
Auditor General's Department
40 Knutsford Boulevard
Kingston 5
Jamaica, W.I.
www.auditorgeneral.gov.jm

Our Vision:
A better country through effective audit scrutiny.

TABLE OF CONTENTS

AUDITOR GENERAL'S OVERVIEW

As public sector entities seek to improve efficiency through investments in Information Technology, they must also consider the effectiveness of their IT governance structure in ensuring the achievement of the related strategic objectives. IT governance, a subset of corporate governance, refers to the delivery of value through the strategic alignment of IT with business objectives, proper risk management and improved performance management. By establishing appropriate organisational structures, policies, roles and responsibilities, public sector entities will ensure the optimal use of resources, mitigation of IT risk and the delivery of value to stakeholders.

The audit of the Jamaica Constabulary Force (JCF), Jamaica Information Service (JIS) and Ministry of Finance and the Public Service (MoFPS) therefore sought to determine whether the entities have an effective IT governance mechanism in place to support the achievement of their strategic objectives and critical business requirements. Despite the significance of the entities core operational functions, IT plays a pivotal role in their strategic success through the adoption of various technologies to increase efficiency and create value. For instance, one of the JCF's key strategic priorities is modernization through technology by "applying appropriate technological solutions to improve business systems and processes in order to maximize productivity and improve efficiency". Similarly, a key priority of the JIS is to provide state-of-the-art media services for the government and other clients, built on an innovative information and communication technology (ICT) platform. While the Ministry of Finance and the Public Service has for decades invested in computerized inventory and financial management information systems. Given the reliance on information technology to achieve their strategic objectives, there is a need for the establishment of appropriate IT governance structure to minimize risk and generate value from the investments in IT projects.

Our audit revealed that the entities did not implement fundamental elements of IT governance to ensure the proper management of IT resources and alignment of IT strategies with business objectives. We also noted that formal IT risk assessment and information security management procedures were not prepared by the entities to ensure that risks were systematically identified and mitigated. However, the entities have recognized the need for improvements in these areas and will seek to adopt the recommendations made.

I wish to thank the management and staff of the JCF, JIS and MoFPS for the courtesies extended to my staff during the audit.

Pamela Monroe Ellis, FCCA, FCA
Auditor General

This page was intentionally left blank.

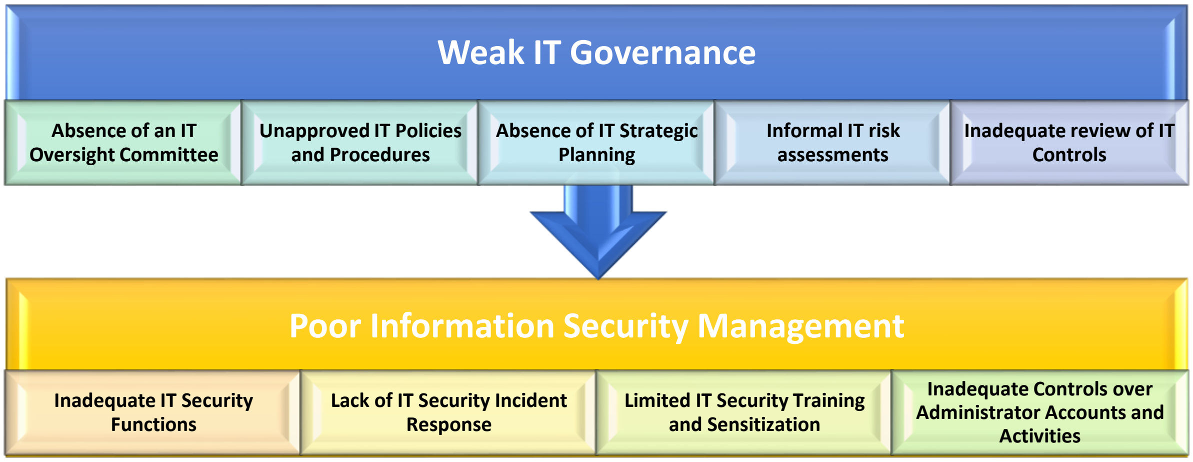
EXECUTIVE SUMMARY

The increased use of Information Technology (IT) by Ministries, Departments and Agencies (MDAs) in pursing their strategic goals has highlighted the need for a structured approach to the governance of public sector IT resources. This approach, known as IT governance, is a structure of relationships and processes used to direct and control the organization to ensure the alignment of business with IT strategies and delivery of value. Therefore, as MDAs become increasingly dependent on technology to achieve their goals they must implement the necessary controls to ensure expected return on IT investments, management of risks and the performance of the IT function.

Our audit sought to determine whether the Jamaica Constabulary Force (JCF), Jamaica Information Service (JIS) and Ministry of Finance and the Public Service (MoFPS) have effective IT governance mechanisms in place to support the achievement of their strategic objectives and critical business requirements. The audit involved a review of the entities general controls, systems and procedures in particular those relating to IT governance for the financial years 2013/2014 to 2016/2017. We examined, on a test basis, evidence supporting compliance with relevant standards that are applicable to Information and Communication Technology (ICT) operations within each entity.

Key Audit Question **Is there an effective IT governance mechanism in place to support the achievement of strategic objectives and critical business requirements?**

What we found



Weak IT Governance

- Absence of an IT Oversight Committee
- Unapproved IT Policies and Procedures
- Absence of IT Strategic Planning
- Informal IT risk assessments
- Inadequate review of IT Controls

Poor Information Security Management

- Inadequate IT Security Functions
- Lack of IT Security Incident Response
- Limited IT Security Training and Sensitization
- Inadequate Controls over Administrator Accounts and Activities

Absence of an IT Oversight Committee - JCF

1. A significant element of IT Governance is the establishment of an oversight executive committee with responsibility for the review and monitoring of the strategic planning, risk management, investment and resource allocation of the IT function. Additionally, the committee ensures the strategic alignment between IT strategies and business objectives of an organization. However, the JCF did not have an appropriate committee to ensure strategic alignment of the IT strategies being pursued and availability of suitable IT resources, skills and infrastructure to meet its strategic goals. Consequently, there is an increased risk that IT decisions will be made without the involvement of relevant stakeholders and consideration of the JCF's strategic priorities. The JCF has since taken steps to constitute its own ICT Steering Committee, however implementation of this phase of governance was deferred to January 2019.

Unapproved IT Policies and Procedures - JIS

2. Critical to IT governance is the development of IT policies and procedures to ensure that the IT function is appropriately directed and controlled. IT policies and procedures also ensure that there is appropriate use of the organization's technological resources as well as defined roles and responsibilities for all users. However, our audit of the JIS revealed that the agency did not have any approved policies or procedures to guide its IT operations. The agency drafted an Acceptable ICT User Policy and a Root Security Policy; however, there was no evidence that they were approved. These draft documents may also be out-dated, as they did not take the Agency's current IT environment and organizational changes into account. The absence of approved IT policies and procedures increases the risk of inconsistency in the performance of IT function, which may lead to a weakened IT control environment. The JIS subsequently indicated that the draft policies will be reviewed, updated and approved within the 2018/2019 fiscal year.

Absence of IT Strategic Planning - JCF

3. Given the increased dependence on technology to achieve strategic objectives, IT strategic plans must be developed to clearly define how IT goals will contribute to an organization's strategic objectives as well as the related costs and risks. The plan should include an investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. However, despite it being one of the key initiatives outlined in the JCF's Corporate Plan, a separate IT strategic plan outlining the general relationship between IT and the corporate strategies was not developed. The absence of an approved IT strategic plan increases the risk that the JCF may not achieve its strategic priority of modernization through technology as its IT strategies may not be aligned to business objectives resulting in the implementation of inappropriate technological solutions.

4. The JCF has since indicated that it "*had long recognized the weaknesses in its ICT governance structure and strategic planning and had in fact commissioned the preparation of a plan some* *time ago*". We were further advised that it has "*commenced the process to update the previous plan with new realities*"*.*

Informal IT Risk Assessment

5. IT risk assessments should be carried out to identify threats and vulnerabilities that will prevent an organization from achieving its strategic objectives. Management must therefore respond by implementing the relevant controls that will minimize the likelihood and impact of adverse events. However, our audit revealed that though the JCF, JIS and Ministry of Finance had increased reliance on technology, none of the entities formally conducted a detailed IT risk assessment to determine the vulnerabilities associated with their IT environments or threats to their IT resources in order to develop appropriate responses. Consequently, these Government entities may not have implemented sufficient controls to ensure that vulnerabilities are not exploited and that they would be able to appropriately respond to adverse events within their IT environments.

6. The JCF has since advised that "*the ICT Policy developed through internal and external consultations will be immediately revived and the Ministry of National Security's Internal Audit Unit tasked with periodically reviewing the control mechanisms mandated by the policy and to identify any risks which are inherent in its current operations*". The MoFPS and JIS have accepted the finding and intend to conduct comprehensive IT risk assessments within the 2018/19 and 2019/20 financial years, respectively.

Independent Review of IT Controls – JCF & JIS

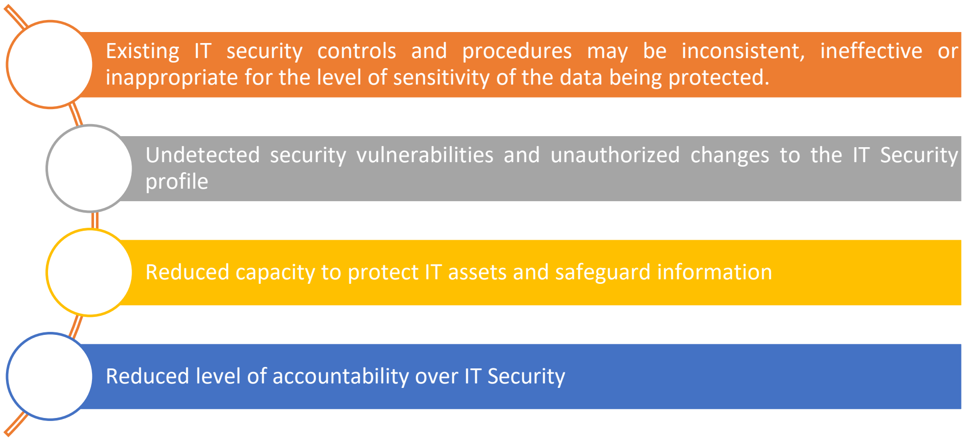
7. Both the JCF and JIS have identified information technology as a key business enabler. As such, they must ensure that IT is applied and managed in a manner that guarantees the attainment of strategic goals. In order to obtain that assurance, periodic evaluation should be performed to determine the effectiveness of IT controls in managing their assessed risks. However, we found no evidence that the management of the entities obtained regular, independent reviews to ensure the efficiency and effectiveness of the IT initiatives and controls implemented. This has weakened the entities overall IT control mechanism as periodic independent reviews should help to ensure compliance with IT control procedures and provide management with some level of assurance that the controls that have been implemented within the organization are working as intended.

8. In response, JIS indicated that *"there were no Internal Audit reviews due to the lack of personnel and resources for the department. We have now engaged the services of a Chief Internal Auditor effective 2018, which will see the resumption of the monitoring role of the IT control system. This will be included in the Audit Plan for the Internal Audit Unit going forward."*

Inadequate IT Security Function - MoFPS

9. We found that the MoFPS did not establish an IT security function to ensure that there was a consistent and coordinated approach to IT security across the organisation. Additionally, the Ministry did not assign specific responsibilities for managing IT security in the absence of a designated officer. Though members of the Information Systems Unit (ISU) performed some IT security related functions, the roles and responsibilities of management, system owners, users and IT personnel were not clearly defined. This increases the risk of security vulnerabilities remaining undetected and reduces the Ministry's capacity to protect its IT assets and safeguard the information contained within its IT systems. The absence of clearly defined IT security roles also reduces the level of accountability over IT security throughout the MoFPS.

Figure 1*: Implications of Inadequate ISMS*


Existing IT security controls and procedures may be inconsistent, ineffective or inappropriate for the level of sensitivity of the data being protected.
Undetected security vulnerabilities and unauthorized changes to the IT Security profile
Reduced capacity to protect IT assets and safeguard information
Reduced level of accountability over IT Security

Source: Auditor General Department

10. The Ministry has since indicated that it is currently restructuring its IT function and the *"job of an IT Security Specialist has been identified"*. MoFPS further advised that recruitment will be undertaken once approval to establish the post is received.

Inadequate IT Security Incident Response System - JIS

11. A proper Information Security Management System (ISMS) should not only be designed to identify weaknesses but must also include a structured approach to managing security incidents or breaches. This approach requires an organization to establish and maintain an effective IT security incident response mechanism to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, and reduce the likelihood of the incident reoccurring. However, we found that though the JIS had past security breaches such as website defacements, the Agency did not develop a formal incident response system to effectively respond to IT security incidents. This increased the risk of loss or damage to its ICT assets because potential security incidents may not be clearly defined, classified or communicated resulting in a lack of appropriate and timely response.

12. The JIS has since indicated that it *"works with the Jamaica Cyber Incident Response Team (CIRT) in determining risk, scope and response to security incidents. However, the Agency notes the recommendation to develop an IT security incident response system in-house. The Agency intends to improve our internal response mechanism for 2018-19 by keeping a log to track all incidents."*

Limited IT Security Training and Sensitization

13. All organizations should develop an information security training programme as a key component of their Information Security Management System to increase the awareness of staff to IT risks. The programme should include security best practices, IT security responsibilities of all staff, confidentiality standards, and ethical conduct. However, despite the entities increased reliance on IT, they did not establish a programme for creating user awareness and training to sensitize end-users. The absence of a security awareness training and sensitization programme increases the entities vulnerability to IT security risks and may result in a breakdown of its IT control system. The JIS agreed with the audit finding and has indicated that steps will be taken to formalize their current user awareness practices in keeping with the audit recommendation. While, the MoFPS indicated that despite not having a formal IT security awareness and training programme, *"several initiatives have been employed"* to increase IT security awareness. However, it will seek to formalize its IT security awareness and training programme within the 2018/2019 financial year. The JCF indicated that *"the matter of the ICT structure within the organization will be immediately reviewed by the new Commissioner of Police with a view to developing an ICT infrastructure capable of correcting and managing these areas of weakness. It is anticipated that the Commissioner will evolve an appropriate structure within six months"*.

Inadequate Controls over Administrator Accounts and Activities

14. In an effort to ensure information security, effective logical access controls should be implemented within all organizations. The controls should not be restricted to regular users but extended to administrators and other privileged users as they usually have extensive access to an organization's IT systems. These account types should be limited and their activities logged and monitored. However, our audit revealed that neither the JIS nor the JCF had a system in place to monitor the activities of users with administrator privileges to ensure that they were not misusing their access rights. Consequently, there is an increased risk of unauthorized changes to the entities IT security profiles and access control parameters going undetected. The JIS agreed with the audit finding and has since indicated that adjustments were made to its Domain auditing policy and an auditing software was installed to monitor the activities of Administrators. JIS also advised that going forward the department manager will conduct more frequent reviews. While, the JCF indicated that steps will be taken to strengthen this area within the next six months.

What should be done

1. The JCF, JIS and MoFPS should implement an IT governance framework to ensure the alignment of IT and business objectives, proper risk management, improved IT performance and service delivery. The framework should encourage the establishment of an oversight committee and the development of an appropriate organisational structure, policies, roles and responsibilities to ensure accountability and the use of IT resources to deliver value to stakeholders.

2. All entities should establish an Information Security Management System (ISMS) to ensure that risks are appropriately identified and mitigated to preserve the confidentiality, integrity and availability of their data and information systems. Additionally, the system should include an initial detailed risk assessment as well as periodic reviews to ensure that risks from changes in the IT environment are managed in a timely manner.

PART ONE

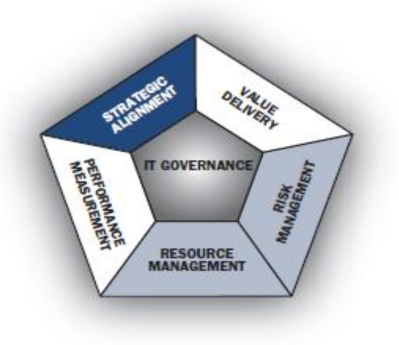
Audit Objective, Scope and Approach

1.1 In keeping with my constitutional mandate, I commissioned an IT audit of the Jamaica Constabulary Force (JCF), Jamaica Information Service (JIS) and Ministry of Finance and the Public Service to determine whether the entities have an effective IT governance mechanism in place to support the achievement of their strategic objectives and critical business requirements. We also examined, on a test basis, evidence supporting compliance with relevant standards that are applicable to Information and Communication Technology (ICT) operations within each organization.

1.2 The audit involved a review of each organization's general computer controls, systems and procedures in particular those relating to IT governance for the period April 2013 to March 2017. Our audit was conducted in accordance with International Standards of Supreme Audit Institutions (ISSAIs).

1.3 We assessed the following elements of IT governance across the three entities:

- IT strategic planning
- IT risk management
- IT policies, standards and procedures
- IT human resources management
- IT investment planning



Source: COBIT 4.1

1.4 Using a risk based audit approach, our assessment was based on the review of official documents, records and other related information, observations of processes and procedures, and interviews with senior officers and staff of each entity. We compared existing general computer controls against international benchmarks and widely accepted best practices within the ICT sector.

PART TWO Jamaica Constabulary Force (JCF)

Background

2.1 The Jamaica Constabulary Force (JCF) is responsible for the maintenance of law and order, the prevention and detection of crime, the investigation of alleged crimes, the protection of life and property and the enforcement of all criminal laws as defined by the Jamaican penal code. In order to deliver on its priorities and objectives, the JCF is structured along the following portfolio lines:

- Administration and Support Services;
- Operations;
- Crime;
- Security Services; and
- Inspectorate of Constabulary.

2.2 The JCF's Corporate Plan for the period 2015 to 2018 outlines six strategic priorities that will be pursued and implemented to enhance the performance and impact of the JCF. One of the key strategic priorities is the modernization of the JCF through technology by "applying appropriate technological solutions to improve business systems and processes in order to maximize productivity and improve efficiency". In order to achieve this modernization, the JCF plans to pursue the following strategic objectives:

- Utilize technology to improve business systems and processes that support the delivery of services in a more efficient and effective manner;
- Rationalize telephony services to reduce communication costs;
- Provide, coordinate, and facilitate the use of Information and Communications Technology in JCF activities;
- Review and simplify systems and processes for more effective and efficient use of resources;
- Leverage existing technological capabilities to automate and improve data-management and record keeping;
- Increase the use of technology in crime prevention, investigations, administration and operations.

2.3 The JCF's strategic objectives are consistent with the Vision 2030 National Development Plan (NDP) to strengthen the anti-crime capability of law enforcement agencies through improved communication and information technology infrastructure. Given the JCF's growing reliance on technology in its operations, there is a need to establish within the Department an effective IT governance mechanism to ensure the delivery of value, strategic alignment and effective risk management.

Absence of an IT Oversight Committee

2.4 As the JCF positions information technology as a strategic priority, there is a need to establish an appropriate IT governance structure to ensure that its IT strategy is aligned with its business goals. Such a structure usually comprises an executive level committee to secure the direct involvement of all relevant stakeholders to provide strategic direction for ICT across the organization. The general purpose of such a committee is to ensure that IT strategy is aligned with the strategic goals of the JCF as well as making recommendations and decisions regarding IT priorities, funding and other IT requirements.

2.5 Despite positioning ICT as a strategic priority, the JCF did not have an appropriate oversight committee that provided advice to the Police High Command on areas such as the alignment of IT with its strategic direction, the achievement of its strategic IT objectives or the availability of suitable IT resources, skills and infrastructure to meet its strategic goals. Consequently, there was an increased risk that not all IT decisions were based on the JCF's strategic goals and not all relevant stakeholders were involved in the IT decision-making process. In response, the JCF has since taken steps to constitute its own ICT Steering Committee, however implementation of this phase of governance was deferred to January 2019.

IT Strategic Planning

2.6 Effective IT governance involves developing an IT strategic plan to ensure that IT resources are managed and directed in a manner that aligns to the organisation's business strategies and priorities. The IT strategic plan should outline how IT goals will contribute to strategic objectives, including the related costs as well as associated risks. The plan should cover budgets, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The IT strategic plan provides the foundation for the development of more detailed IT operational plans for providing IT services and implementing IT projects over a shorter period.

2.7 Despite being one of the key initiatives outlined in its Corporate Plan, the JCF did not develop a separate IT strategic plan that outlined the general relationship between IT and the Department's strategic objectives or how IT goals will contribute to its business objectives. The absence of an approved IT strategic plan increased the risk that the Department may not achieve its strategic priority of modernization through technology because its IT strategies may not be aligned with its business objectives resulting in the implementation of inappropriate technological solutions that may fail to meet the Department's long-term goals.

2.8 The JCF subsequently indicated that it "*had long recognized the weaknesses in its ICT governance structure and strategic planning and had in fact commissioned the preparation of a plan some time ago*". The Department further advised that it has "*commenced the process to update the previous plan with new realities"*.

Independent Review of IT Controls

2.9 The JCF has increased its reliance on information technology as it is no longer merely a support function but is now a key strategic priority. How IT is applied and managed will have a significant effect on whether the Department attains its goal of modernization through technology. This would require the JCF to evaluate its IT control environment as part of its overall control mechanism and IT governance review. The main aim of this evaluation process is to provide independent advice to the JCF's management on the efficiency and effectiveness of the IT initiatives implemented.

2.10 We found no evidence to indicate that the JCF had established any mechanism to periodically evaluate its IT controls to determine their effectiveness or efficiency. Consequently, the JCF's management may not be aware of significant risks to its information technology systems. Additionally, the Department's overall IT control mechanism has been weakened due to the lack of monitoring to ensure compliance with IT policies, procedures and initiatives.

IT Risk Assessment

2.11 An IT risk assessment, which forms part of a wider enterprise risk assessment is undertaken to determine the possible threats faced by an organization's IT environment and infrastructure. These threats are assessed based on their likelihood of occurrence and their impact on operations. The outcome is used to develop and implement an appropriate response to reduce the likelihood of occurrence and or the impact of the risks on the organization. Some of the major IT risks include:

- Physical damage to information technology assets;
- Data loss and system unavailability;
- Loss of data integrity;
- Unauthorized access, manipulation or disclosure of confidential information;
- Failure to recover from system disruptions;
- Failure of IT projects.

2.12 Though the JCF has increased its reliance on technology, it did not develop an IT risk assessment to determine the vulnerabilities associated with its IT environment and threats to its IT resources in order to develop appropriate responses. The Department therefore, has an increased risk exposure and may not be able to respond appropriately in the event of a threat affecting its IT environment. The JCF subsequently indicated that "*the ICT Policy developed through internal and external consultations will be immediately revived and the Ministry of National Security's Internal Audit Unit tasked with periodically reviewing the control mechanisms mandated by the policy and to identify any risks which are inherent in current operations*".

IT Security Training and Sensitization

2.13 User awareness and training is an essential component of an organization’s IT security management system. Training programmes should include system security practices, IT security responsibilities of all staff, confidentiality standards, and ethical conduct. Despite its growing reliance on IT, the JCF did not establish a programme for creating user awareness and training to sensitize end-users about IT security. The absence of a security awareness training and sensitization programme increases the JCF’s vulnerability to IT security risks and may result in a breakdown of the Department’s IT control environment. In its response, the JCF indicated that *“the matter of the ICT structure within the organization will be immediately reviewed by the new Commissioner of Police with a view to developing an ICT infrastructure capable of correcting and managing these areas of weakness. It is anticipated that the Commissioner will evolve an appropriate structure within six months”*.

Inadequate Controls over Administrator Accounts and Activities

2.14 The accounts of administrators and other privileged users should be closely monitored because these accounts/users usually have extensive access to an organization’s information technology systems. There should be a limited number of such accounts and their activities should be logged and monitored. The JCF did not have a system in place to monitor the activities of users with administrator privileges to ensure that they were not misusing their access rights. Consequently, there is an increased risk of unauthorized changes to the Department’s IT security profiles and access control parameters going undetected. The JCF indicated that steps will be taken to strengthen this area within the next six months.

PART THREE Jamaica Information Service (JIS)

Background

3.1 The Jamaica Information Service (JIS), a Model B Executive Agency[1], is the public information arm of the Government of Jamaica (GoJ). The Agency's core activity is to produce information and communication projects in support of Government policies and programmes. JIS also provides advertising and public relation services to government and non-governmental agencies. The Agency's main media and communications services include:

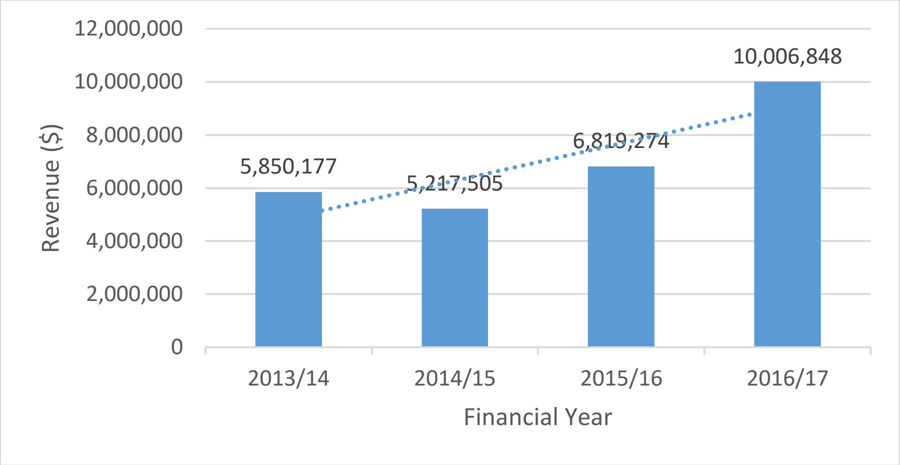
- Radio and TV Production
- Video Recording
- Website design, hosting and maintenance
- Online Advertising
- Streaming (live and delayed streaming of special events)
- Graphic Design
- Photography
- Printing Services

3.2 One of the Agency's key strategic goals is to provide state-of-the-art media services for the GoJ and other clients, built on an innovative information and communication technology (ICT) platform. The Agency also improved its computer service offerings and steadily increased its revenue largely from website design, hosting and maintenance services over the audit period. As at March 31, 2017 the Agency collected revenue of approximately $10 million, representing a 46.7% increase from the previous year (Figure 2). However, the Agency has identified weaknesses in its information technology (IT) infrastructure and aims to establish a more efficient and effective integration of ICT to drive business growth and productivity. This includes the development and implementation of an e-commerce platform to facilitate the sale of JIS products and services.

3.3 Given the Agency's increasing reliance on technology in its operations, there is a need to establish within the JIS an effective IT governance mechanism to ensure the delivery of value, strategic alignment and effective risk management.

[1] An executive agency is any public body established under the Executive Agencies Act for the enhancement of the effective and efficient delivery of goods and services to the public. A Model B agency remains a part of the consolidated fund and will be funded on a net basis through appropriations-in-aid.

Figure 2: Computer Services Revenue for FYs 2013/14 to 2016/17



Source: JIS Audited Financial Statements 2013-14 to 2016-17

Independent Review of IT Controls

3.4 Information Technology has become increasingly pervasive within the JIS and is no longer merely a support function but is now a key business enabler. How IT is applied and managed will have a significant effect on whether the Agency attains its strategic goals. Consequently, the JIS needs to evaluate its IT control environment as part of its overall controls and corporate governance review. The main aim of this evaluation process is to provide independent advice to the Agency's management on the efficiency and effectiveness of the IT initiatives implemented.

3.5 We found no evidence to indicate that the JIS had established any mechanism, such as a system of periodic internal IT audits, to evaluate its IT controls to determine their effectiveness or efficiency. Consequently, the Agency's ICT function was not subjected to regular, independent reviews to ensure that management was aware of critical risks associated with its IT systems. This has weakened the Agency's overall IT control mechanism because a system of periodic independent reviews should provide management with some assurance that the controls implemented are working as intended. In response, JIS indicated that *"there were no Internal Audit reviews due to the lack of personnel and resources for the department. We have now engaged the services of a Chief Internal Auditor effective 2018, which will see the resumption of the monitoring role of the IT control system. This will be included in the Audit Plan for the Internal Audit Unit going forward."*

IT Risk Assessment

3.6 An IT risk assessment, which forms part of a wider enterprise risk assessment is undertaken to determine the possible threats faced by an organization's IT environment and infrastructure. These threats are assessed based on their likelihood of occurrence and their impact on operations. The outcome is used to develop and implement an appropriate response to reduce the likelihood of occurrence and or the impact of the risks on the organization. Some of the major IT risks include:

- Physical damage to information technology assets;
- Data loss and system unavailability;
- Loss of data integrity;
- Unauthorized access, manipulation or disclosure of confidential information;
- Failure to recover from system disruptions;
- Failure of IT projects.

3.7 Though the JIS has increased its reliance on technology, it did not complete an IT risk assessment to determine the vulnerabilities associated with its IT environment and threats to its IT resources in order to develop appropriate responses. The Agency therefore, has an increased risk exposure and may not be able to respond appropriately in the event of a threat affecting its IT environment. The JIS agreed with the audit finding and indicated that the Agency will conduct an IT risk assessment for the 2019/2020 fiscal year.

IT Policies and Procedures

3.8 IT policies and procedures, like the IT strategic plan, are major components of an organization's IT governance function. IT policies and procedures are developed to ensure that there is appropriate use of the organization's information and communication technology services and resources. They also define the responsibilities of users and provide general direction for protecting the confidentiality, integrity and availability of corporate information.

3.9 Our review revealed that the JIS did not have any approved IT policies or procedures in place to guide its IT operations. Despite drafting an Acceptable ICT User Policy and a Root Security Policy, there was no evidence that they were approved by those charged with the governance of JIS. These draft documents may also be out-dated, as they do not take into account the Agency's current IT environment and organizational changes. The absence of approved IT plans, policies and procedures increases the risk of inconsistency in the performance of IT functions and operations, which may lead to a weakened IT control environment. The JIS subsequently indicated that the draft policies will be reviewed, updated and approved within the 2018/2019 fiscal year.

Inadequate IT Security Incident Response System

3.10 The need to maintain the integrity of information and protect IT assets requires an effective security management system. This system includes establishing and maintaining an effective IT security incident response mechanism to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, and reduce the likelihood of the incident reoccurring. Despite the occurrence of previous security incidents, such as the defacement of its website and five others hosted by the Agency in 2015, JIS did not develop an IT security incident response system to effectively respond. This increased the risk of loss or damage to its ICT assets because security incidents may not be clearly defined, classified or communicated resulting in a lack of appropriate and timely response.

3.11 In response, JIS indicated that it *"works with the Jamaica Cyber Incident Response Team (CIRT) in determining risk, scope and response to security incidents. However, the Agency notes the recommendation to develop an IT security incident response system in-house. The Agency intends to improve our internal response mechanism for 2018-19 by keeping a log to track all incidents."*

IT Security Training and Sensitization

3.12 User awareness and training is an essential component of an organization's IT security management system. Training programmes should include system security practices, IT security responsibilities of all staff, confidentiality standards, and ethical conduct. Despite its increasing reliance on IT, the JIS did not establish a programme for creating user awareness and training to sensitize end-users about IT security. The absence of a security awareness training and sensitization programme increases the Agency's vulnerability to IT security risks and may result in a breakdown of its IT control environment.

3.13 The Agency agreed with the audit finding and indicated that steps will be taken to formalize their current user awareness practices in keeping with the audit recommendation.

Inadequate Controls over Administrator Accounts and Activities

3.14 The accounts of administrators and other privileged users should be closely monitored because these accounts/users usually have extensive access to an organization's IT systems. There should be a limited number of such accounts and their activities should be logged and monitored.

3.15 The JIS did not have a system in place to monitor the activities of users with administrator privileges to ensure that they were not misusing their access rights. Consequently, there is an increased risk of unauthorized changes to the Agency's IT security profiles and access control parameters going undetected. The Agency agreed with the audit finding and has since indicated that adjustments were made to its Domain auditing policy and an auditing software was installed to monitor the activities of Administrators. JIS also advised that going forward the department's manager will conduct more frequent reviews.

PART FOUR Ministry of Finance and the Public Service

Background

4.1 The Ministry of Finance & the Public Service (MoFPS) has overall responsibility for developing the Government's fiscal and economic policy framework as well as the administration of public revenue and expenditure. The Ministry's priority goals include:

- Improving revenue administration by creating a simple, equitable, and competitive tax environment to ensure greater compliance and enhance growth;
- Strengthening the level of financial accountability and efficiency of the Public Sector;
- Strengthening the capacity of the Ministry to effectively regulate financial institutions and combat financial crimes;
- Improving the internal efficiency and effectiveness of the Ministry.

4.2 The main operational responsibilities of the Ministry include the management of revenues, the preparation and management of the national budget, public sector financial management, management of the public debt, compensation policy and conditions of service. In addition to the development and implementation of computer-based systems to meet the information technology needs of the ministry and its departments, the MoFPS is also responsible for managing the development and or implementation of several large scale information technology (IT) systems for use throughout the public sector. These include:

- Financial Management (FinMan) Accounting System;
- Central Treasury Management System (CTMS);
- BizPay payroll system;
- Electronic Public Procurement System (e-PPS);
- Human Capital Management Enterprise System (MyHR+);
- Public Employees Pension Administration System (PEPAS)

4.3 Given the Ministry's role in the development, implementation and oversight of these major information and communication technology (ICT) initiatives and their strategic importance to the public sector, there is a need to establish within the MoFPS an effective IT governance mechanism to ensure the delivery of value, strategic alignment and effective risk management.

IT Risk Assessment

4.4 An IT risk assessment, which forms part of a wider enterprise risk assessment is undertaken to determine the possible threats faced by an organization's IT environment and infrastructure. These threats are assessed based on their likelihood of occurrence and their impact on operations. The outcome is used to develop and implement an appropriate response to reduce the likelihood of occurrence and or the impact of the risks on the organization. Some of the major IT risks include:

- Physical damage to information technology assets;
- Data loss and system unavailability;
- Loss of data integrity;
- Unauthorized access, manipulation or disclosure of confidential information;
- Failure to recover from system disruptions;
- Failure of IT projects.

4.5 Though the MoFPS has increased its reliance on technology, it did not complete an IT risk assessment to determine the vulnerabilities associated with its IT environment and threats to its IT resources in order to develop appropriate responses. The Ministry therefore, has an increased risk exposure as sufficient controls may not be implemented to ensure that vulnerabilities are not exploited. Additionally, the MoFPS may not be able to appropriately respond to threats affecting its IT environment, which may result in operational inefficiencies in the administration of public expenditure, revenue and debt. The Ministry agreed with the audit finding and indicated that steps will be taken in the financial year 2018/2019 to conduct a comprehensive IT risk assessment.

Inadequate IT Security Function

4.6 The responsibility of managing IT security should be appropriately assigned either to a separate IT security manager role (depending on the size of the organization and the complexity of the IT infrastructure) or allocated to an existing senior level IT personnel. Effective information security requires coordinated and integrated action from top down. An effective IT security management function should be established to effectively implement information security related policies and plans and for implementing the various IT security related processes such as access controls and network security.

4.7 The Ministry's Information Systems Unit (ISU) consists of 22 approved post, however, we found that the MoFPS did not establish an IT security function to ensure that there was a consistent and co-ordinated approach to IT security across the organisation. The MoFPS did not assign specific responsibilities for managing IT security, as there was no designated officer (s) responsible for implementing and monitoring IT security policies and procedures in a proactive manner across the Ministry. While members of the Information Systems Unit (ISU) performed some IT security related functions, the IT security roles and responsibilities were not clearly defined, in particular the roles and responsibilities of management, system owners, users and IT personnel. This increases the risk of security vulnerabilities remaining undetected and reduces the Ministry's capacity to protect its IT assets and safeguard the information contained within its IT systems. The absence of clearly defined IT security roles also reduces the level of accountability over IT security throughout the MoFPS.

4.8 The Ministry has since indicated that it is currently restructuring its IT function and the *"job of an IT Security Specialist has been identified"*. MoFPS further advised that recruitment will be undertaken once approval to establish the post is received.

IT Security Training and Sensitization

4.9 User awareness and training is an essential component of an organization's IT security management system. Training programmes should include system security practices, IT security responsibilities of all staff, confidentiality standards, and ethical conduct. Despite its increasing reliance on IT, the MoFPS did not establish a programme for creating user awareness and training to sensitize end-users about IT security. The absence of a security awareness training and sensitization programme increases the Ministry's vulnerability to IT security risks and may result in a breakdown of its IT control system.

4.10 In its response, the Ministry indicated that, despite not having a formal IT security awareness and training programme, *"several initiatives have been employed"* to increase IT security awareness. However, it will seek to formalize its IT security awareness and training programme in financial year 2018/2019.