INFORMATION SYSTEMS REVIEW REPORT

OF THE

TAX ADMINISTRATION JAMAICA (TAJ)

ON ITS

IT GOVERNANCE AND BUSINESS CONTINUITY MANAGEMENT

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 and 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

TAJ'S ALIGNMENT TO VISION 2030

National Vision Statement:

"Jamaica, the place of choice to live, work, raise families and do business"

AUDITOR GENERAL'S OVERVIEW

The performance of Tax Administration Jamaica (TAJ) is critical to the development of an efficient and equitable tax system in keeping with one of the key national strategies under Jamaica's Vision 2030 National Development Plan (NDP). TAJ's mission is to collect the revenues due in an equitable and cost effective manner, foster voluntary compliance, provide excellent service to its customers through an engaged and empowered staff.

Information and Communication Technology (ICT) has become one of the key business enablers for Tax Administration Jamaica and TAJ relies significantly on ICT to deliver its core services. Given this level of reliance on ICT, it is critical that TAJ has the capability to continue the delivery of its services at acceptable pre-defined levels following a disruptive event. I commissioned an Information Technology Audit of TAJ to determine whether it has an effective Business Continuity Management system in place that will ensure the timely resumption of critical services in the event of any unplanned interruptions. The audit revealed that TAJ is exposed to a high risk of operational failure because it may not be able to restore normal services within a reasonable time if its IT systems are affected by a major disruption.

The audit identified weaknesses in TAJ's information technology control environment particularly relating to the areas of information technology governance and business continuity management. While there was general alignment between TAJ's IT strategies and its strategic business objectives, we found that those charged with governance did not provide effective oversight of TAJ's ICT policies, strategies and operations. Our review also revealed that TAJ was vulnerable to information security risks due to the absence of an updated and comprehensive information security policy.

This report is intended to assist TAJ to strengthen its information technology control environment so that it may continue on the path of developing an efficient tax system. It is therefore crucial that the Board and management of Tax Administration Jamaica carefully review the recommendations contained in this report with a view to strengthening its control systems by adopting the measures outlined.

I wish to thank the management and staff of TAJ 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

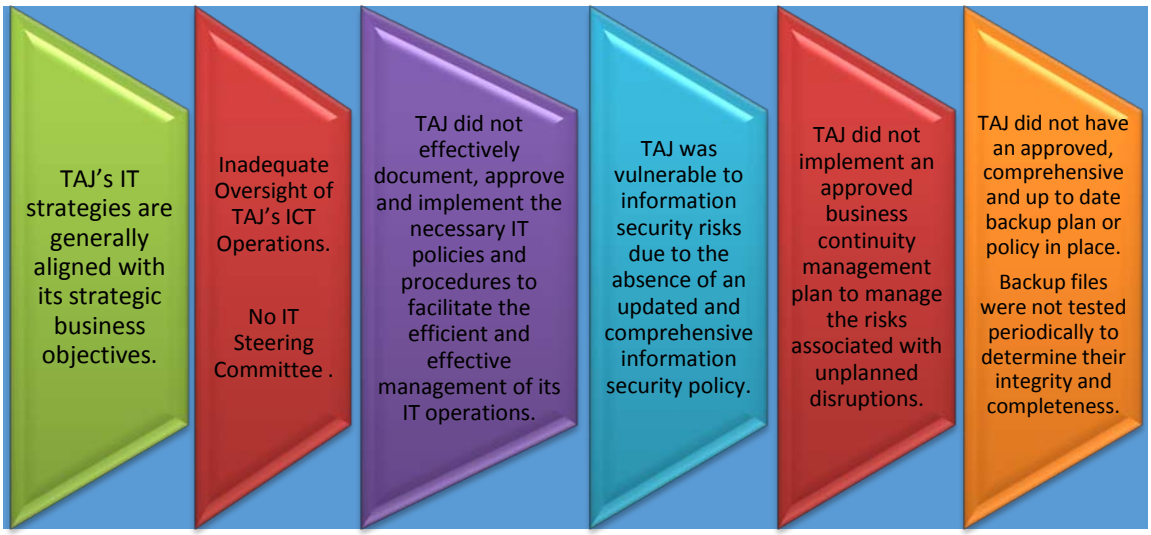
Tax Administration Jamaica (TAJ) is responsible for the administration and collection of domestic taxes, duties, rates and fees and the administration and enforcement of revenue laws. TAJ also provides document-processing services for Tax Compliance Certificates (TCC), Taxpayer Registration Numbers (TRN), Driver's Licences and Motor Vehicle Registration.

Information and Communication Technology (ICT) has always been one of the major components of the tax reform process and TAJ relies significantly on ICT to deliver its core services. For TAJ information technology is not merely a support function, it is a key business enabler. Given TAJ's reliance on ICT to deliver its services, it is critical that TAJ has the capability to continue the delivery of its services at acceptable pre-defined levels following a disruptive event. This will require the identification of potential threats, assessing their likely impact on business operations and develop strategies to respond and restore operations.

Key Audit Question

Does TAJ have an effective Business Continuity Management system in place that will ensure the timely resumption of critical services in the event of any major disruptions?

What we found



IT Strategic Planning

1. 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. We found that the TAJ's *Strategic Business Plan* incorporated its major IT strategies and outlined the general relationship between IT and the TAJ's strategic objectives, including the related costs as well as associated risks and mitigation strategies. A reasonable attempt was made to incorporate strategies focused on providing appropriate technological solutions to support TAJ's business objectives.

Based on the evidence provided, we have obtained reasonable assurance that the TAJ's IT strategies are generally aligned with its strategic business objectives.

Inadequate Oversight of TAJ's ICT Operations

Board of Management

2. The Tax Administration Jamaica Act establishes a Board of Management for TAJ to oversee the general administration of the Authority. The Board is required to meet at least six times in each year and minutes of each meeting shall be kept and confirmed as soon as practicable. However, despite several requests for minutes of the Board of Management meetings for the period under review, none was provided for audit inspection. Consequently, we were unable to determine the frequency of Board meetings, the nature of the matters discussed, decisions made or whether those charged with governance provided adequate oversight of IT related issues.

Information Technology Steering Committee

3. An organization like TAJ that places heavy reliance on information technology to achieve its mandate usually has an executive level or *IT Steering Committee* as an integral part of its information technology governance framework. The general purpose of the *IT Steering Committee* is to ensure that IT strategy is aligned with the strategic goals of the organization. This committee makes recommendations and decisions regarding IT priorities, funding and other IT requirements. Despite its heavy reliance on technology, TAJ did not have an *IT Steering Committee* that provided insight and advice to the Board of Management on areas such as the achievement of the TAJ's strategic IT objectives and the availability of suitable IT resources, skills and infrastructure to meet its strategic objectives. Consequently, we were unable to determine whether all relevant stakeholders were involved in the IT decision-making process and that all decisions were based on the TAJ's business goals. The TAJ has since indicated that it accepts our recommendation to set up an IT Steering Committee for the Authority.

Due to the absence of sufficient and appropriate evidence of IT governance from the Board of Management and the absence of a functional IT Steering Committee, we are unable to determine whether there was adequate oversight of the TAJ's ICT policies, strategies and operations by those charged with governance. Consequently, there is an increased risk that the TAJ's ICT infrastructure and control environment may not adequately support the organisation's business operations and meet its strategic objectives.

IT Policies, Procedures and Plans

4. IT plans, policies and procedures, like the IT strategic plan, are major components of an organization's IT governance function, which are developed to ensure that there is appropriate use of the organization's information and communication technology services and resources. These documents also define the responsibilities of users and provide general direction for protecting the confidentiality, integrity and availability of corporate information. Though TAJ developed at least twelve IT and IT related plans, policies and procedures, there was no evidence that these documents were presented to the Board for review and approval. Some of these draft documents have also become out-dated as they do not take into account the 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 TAJ has not effectively documented, approved and implemented the necessary IT policies and procedures to facilitate the efficient and effective management of its IT operations. Consequently, current IT practices may be inconsistent or contrary to the organization's objectives.

Inadequate Information Security Policy

5. TAJ's IT systems maintain and process highly sensitive and confidential taxpayer data. Therefore, information security must be a high priority and policies must be established to reduce the risk of unauthorised exposure or loss of this data. The TAJ's undated *Information Technology Security Policy* addresses some of the elements of information security. However, the policy does not take into account the current integrated IT environment, strategies and risks, the response mechanism for dealing with security breaches especially those relating to cyber-security, and the impact of relevant legislations such as the Cybercrimes Act and the Electronic Transactions Act. Additionally, the policy was not submitted to the TAJ's Board for approval and there was no evidence that the guidelines were communicated to all staff. TAJ indicated that they recognize the need for a current information security policy and that steps are being taken to sensitize staff on the importance of information security.

The absence of a comprehensive and up to date approved information security policy increases the TAJ's vulnerability to information security risks and reduces its capacity to protect its IT assets/resources and safeguard the information contained within its IT systems. A security breach may not only cause an unauthorised exposure, corruption or loss of data but could also result in a disruption in the TAJ's operations.

Inadequate Business Continuity Planning

6. Despite identifying *inadequate business continuity and disaster management* as an area of significant risk exposure that could lead to major disruption in its operations, TAJ did not implement an approved business continuity management plan to manage the risks associated with unplanned disruptions. A draft plan was prepared, however, no deadline was established for its finalization and submission to the Board for approval. This increased the risk of system unavailability because no documented standard procedure was in place to respond to unplanned disruptions. This contributed to the delayed restoration of the *Revenue Administration information System (RAiS)* in February 2017 following a system failure, resulting in a significant disruption and impact on Taxpayers, Tax Administration staff (including Cashiers) and other users such as financial institutions and government entities that rely on the system to process transactions. Even though some services were restored within 24 hours, it took the TAJ approximately 114 hours (approximately five days) to restore the production environment to full capability.

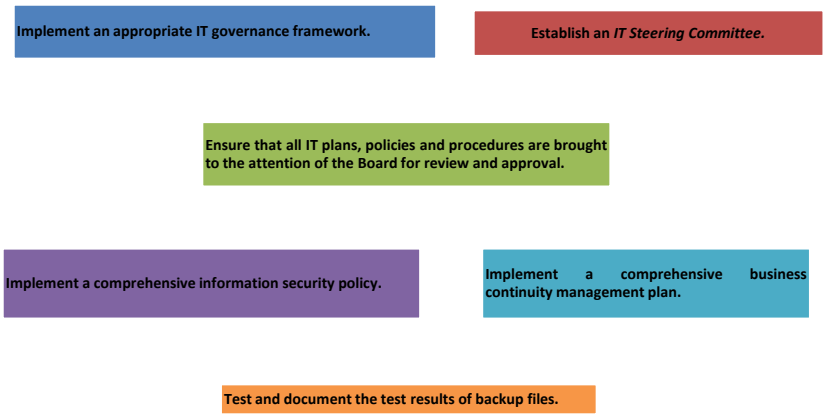
The TAJ's failure to approve and implement a current business continuity management plan has exposed the entire organization to the risk of operational failure because it may not be able to restore normal services within a reasonable time if its IT systems are affected by a major disruption.

Inadequate Data Back-up Policy

7. Based on the nature of TAJ's operations, a comprehensive and up to date data backup, storage and restoration plan, policy and procedure must be developed and implemented to facilitate the timely restoration of its systems to normal use after an unplanned disruption. The TAJ's IT systems and infrastructure must be organised to ensure that there is adequate redundancy, backup and restoration in the event of a disaster. Our review revealed that the TAJ did not have an approved, comprehensive and up to date backup plan or policy in place. Neither was there any system in place to ensure that backup media/data are tested periodically to determine the integrity and completeness of the backup files. Even though a backup schedule exists for the *Revenue Administration information System (RAiS)* and an *IT Contingency Plan* is being developed, the absence of a comprehensive backup plan/policy increases the risk of inconsistency in the performance of backup functions and procedures. Additionally, if the Authority fails to periodically test its backup systems and procedures this may lead to complications, delays or irrecoverable data loss in the event of an unplanned disruption especially if backup media are corrupted or certain members of staff are not available.

The TAJ's failure to approve and implement a comprehensive backup plan/policy and periodically test its backup systems has exposed the entire organization to the risk of operational failure because it may not be able to restore normal services within a reasonable time if its IT systems are affected by a major disruption.

What should be done



Information Technology Governance

1. Information technology governance and the effective application of an IT governance framework are the responsibilities of the TAJ's senior management and Board. We recommend that the Authority identify and implement an appropriate IT governance framework in order to reduce its exposure to IT risks and improve control and governance over its information technology and related systems. The framework implemented should ensure that those charged with governance provide adequate oversight of IT related issues.

2. TAJ should establish an *IT Steering Committee* (or equivalent) as an integral part of its information technology governance framework. The committee should be comprised of executive, business and IT management along with other critical organizational stakeholders to assist the Board in providing strategic direction for ICT across the entity. The *IT Steering Committee* should provide oversight over all IT operations and projects as well as insight and advice to the Board of Management on areas such as the alignment of IT with the TAJ's business direction, the achievement of the TAJ's strategic IT objectives and the availability of suitable IT resources, skills and infrastructure to meet its strategic objectives.

3. TAJ's Board of Management is responsible for overseeing the general administration of the Authority and shall review, evaluate, approve and monitor the implementation by the Authority of its corporate policies, operational, strategic and other corporate plans. We therefore recommend that appropriate steps be taken to ensure that all IT plans, policies and procedures are brought to the attention of the Board for review and approval. The Authority should also ensure that an appropriate system is implemented to facilitate Board review of new or amended IT plans, policies and procedures before they are adopted.

4. TAJ should develop a comprehensive information security policy that provides general and specific guidelines to ensure that the Authority's IT resources are adequately protected.

The policy should establish criteria for assigning technical access to specific IT assets including who will have access and what level of access they will be allowed. The policy should also take into account the current integrated IT environment, strategies and risks, the response mechanism for dealing with security breaches especially those relating to cyber-security, and the impact of relevant legislations such as the Cybercrimes Act and the Electronic Transactions Act. Additionally, the policy should be submitted to the TAJ's Board for approval and communicated to all staff.

Business Continuity Management

5. We recommend that TAJ finalize the development and implementation of a comprehensive business continuity management plan to manage the risks associated with unplanned disruptions. This should incorporate a comprehensive and up to date data backup, storage and restoration plan, policy and procedure to facilitate the timely resumption of its systems to normal use after an unplanned disruption. The business continuity management plan should take into account the risk of unauthorized system penetration, regular testing of recovery procedures and backup media, regular backup of critical systems as well as security procedures relating to the storage of backup files at off-site locations. The Authority should test and document the test results of its backup files and disaster recovery plans on a regular basis to ensure that all systems can be effectively and efficiently recovered and shortcomings adequately addressed prior to a disaster occurring.

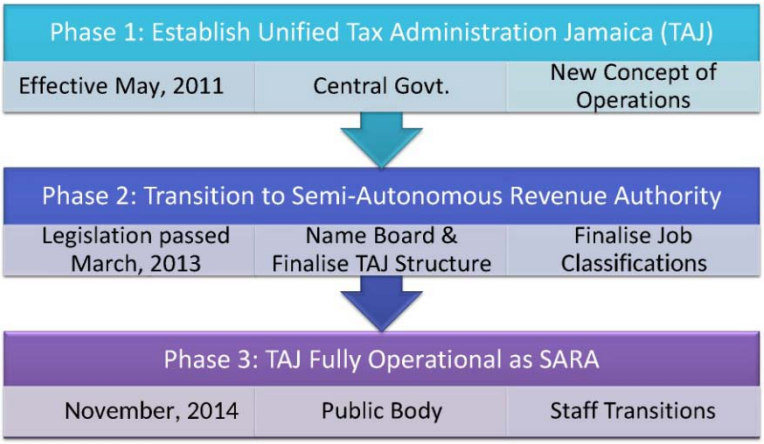
PART ONE

INTRODUCTION

Background

1.1 Tax Administration Jamaica (TAJ) was established to consolidate the activities of the former Inland Revenue Department (IRD), Taxpayer Audit and Assessment Department (TAAD) and Tax Administration Services Department (TASD). This consolidation started in 2011 under an amendment to the Revenue Administration Act. TAJ was subsequently established as a *body corporate* under the Tax Administration Jamaica Act, 2013 with responsibility for the administration and collection of domestic taxes, duties, rates and fees and the administration and enforcement of revenue laws. TAJ also provides document-processing services for Tax Compliance Certificates (TCC), Taxpayer Registration Numbers (TRN), Driver's Licences and Motor Vehicle Registration.

Figure 1: Tax Administration Jamaica Reform



Source: Tax Administration Jamaica

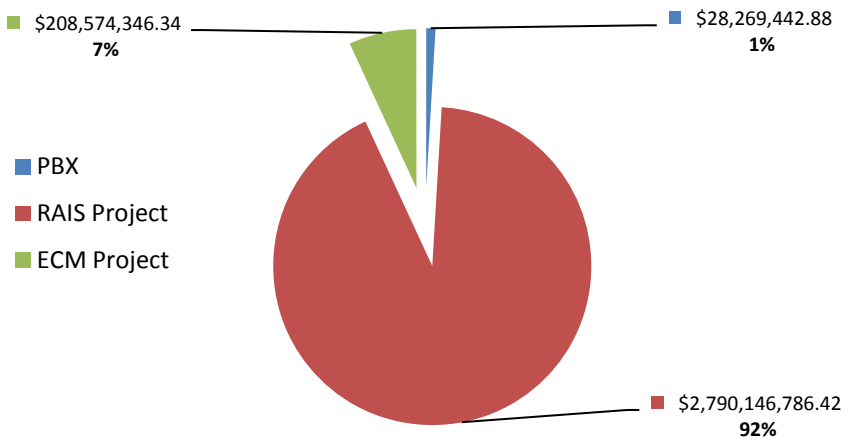
1.2 Information and Communication Technology (ICT) has always been one of the major components of the tax reform process and TAJ relies significantly on ICT to deliver its services. Some critical services that rely on ICT include:

a. Payment of Taxes
b. Filing of Tax Returns
c. Issue and validation of TCC and TRN (include validation by third parties)
d. Issue of Driver's Licences

TAJ is also enhancing its ICT systems to facilitate increased internet transactions and use of improved data analytics to guide its compliance programme.

1.3 In 2011, the Government of Jamaica (GOJ) with loan financing from the Inter-American Development Bank (IDB) embarked on an initiative to modernize the country's tax administration under the Fiscal Administration Modernization Program (FAMP). One aim of the project is to improve the TAJ's capacity by implementing systems to modernize its technological infrastructure including the acquisition of a new integrated taxation administration system. Up to February 17, 2017 total expenditure incurred under the FAMP in relation to the modernization of Tax Administration Jamaica was approximately USD $25.8 million (JA$3.0 billion). Majority of this expenditure, approximately USD$23.8 million (JA$2.79 billion), was spent on implementing the new Revenue Administration information System (RAiS).

Figure 2: FAMP Expenditure Relating to the Modernization of TAJ



Source: Tax Administration Jamaica

1.4 Given TAJ's reliance on ICT to deliver its services, it is critical that TAJ has the capability to continue the delivery of its services at acceptable pre-defined levels following a disruptive event. This will require the identification of potential threats, assessing their likely impact on business operations and develop strategies to respond and restore operations.

Audit Objective, Scope and Approach

1.5 In keeping with her constitutional mandate, the Auditor General commissioned an information technology audit of the Tax Administration Jamaica (TAJ) to determine whether the TAJ has an effective Business Continuity Management system in place that will ensure the timely resumption of critical services in the event of any disastrous interruptions. We also assessed the effectiveness of information technology governance within TAJ and examined, on a test basis, evidence supporting compliance with relevant laws and regulations that are applicable to Information and Communication Technology (ICT) operations within TAJ.

1.6 The audit involved a review of the TAJ's general controls, systems and procedures in particular those relating to Business Continuity and Disaster Recovery for the period April 2013 to March 2017. 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);
- International Standards of Supreme Audit Institutions issued by the International Organization of Supreme Audit Institutions (INTOSAI);
- Control Objectives for Information and related Technology (COBIT) issued by the IT Governance Institute;
- ISO/IEC 27000 family of standards dealing with Information Security Management issued by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC).

These standards and guidelines enabled us to test and compare the TAJ's general computer controls against international benchmarks and widely accepted best practices within the information and communication technology sector.

1.7 Our assessment was based on the review of official TAJ documents, records and other related information, observations of processes and procedures, and interviews with senior officers and staff of the TAJ.

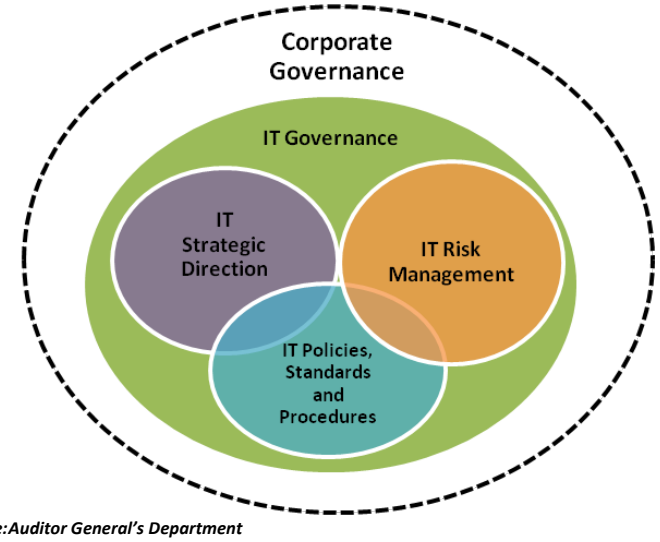
PART TWO

Information Technology Governance[1]

2.1 Corporate Governance is the system by which an organisation is directed and controlled to ensure that strategic goals are achieved, risks are managed and the use of resources is optimized. Good corporate governance will therefore require an organization to establish systems that promote compliance, accountability and transparency. With organizations becoming increasingly dependent on Information Technology (IT) to execute its strategy, the concept of good corporate governance is extended to the field of Information and Communications Technology (ICT).

2.2 IT Governance, a subset of corporate governance, refers to the delivery of value through the strategic alignment of IT with business objectives, risk management and improved performance management. IT governance is the process by which the senior management and those charged with governance of an organization ensure that ICT is optimally used to achieve the organization's business objectives while ensuring that the associated risks are effectively managed.

Figure 3: Relationship Between Corporate and IT Governance



Source:Auditor General's Department

2.3 Information Technology must be aligned with the corporate plan to enable the organization to take full advantage of its information technologies to achieve its corporate and operational objectives. Senior management commitment and control are prerequisites for the successful implementation of ICT. Inadequate management involvement may lead to a direction-less IT function, which does not serve the organisation's strategic and operational needs.

[1] *Board Briefing on IT Governance, 2nd Edition: IT Governance Institute*

2.4 Our review of the TAJ focused on the following elements of IT governance:

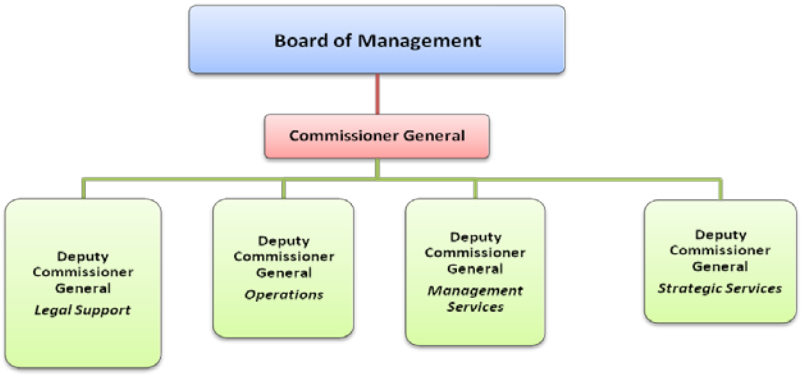
- IT strategic planning
- IT risk management
- IT policies, standards and procedures
- IT organization and management of operations
- IT human resources management
- IT security management

Inadequate Oversight of TAJ's ICT Operations

Board of Management

2.5 The TAJ's executive management comprises the Commissioner General supported by four Deputy Commissioners General with responsibility for operations, management services, legal services and strategic services respectively. The executive management reports to the Board of the Authority as stipulated by the Tax Administration Jamaica Act, 2013.

Figure 4: TAJ High Level Organisational Chart



Source: Tax Administration Jamaica

2.6 Section 6 of the Tax Administration Jamaica Act establishes a Board of Management for the TAJ consisting of nine members appointed by the Minister. The Board is responsible for overseeing the general administration of the Authority. This includes reviewing, evaluating, approving and monitoring the implementation of corporate policies, operational, strategic and other corporate plans. Additionally, Section 7 (6) (e) of the Tax Administration Jamaica Act stipulates that *"...the Board shall ensure, whether by way of meetings or otherwise, that the Minister and the Financial Secretary are kept abreast of matters relating to the administration and management of the Authority, including any need for financial, human, technological and other resource requirements necessary for the achievement of performance targets."*

2.7 The Tax Administration Jamaica Act also stipulates that the Board of Management should meet at least six times in each year for the transaction of its business and minutes of each meeting shall be kept and shall be confirmed as soon as practicable thereafter at a subsequent meeting. However, despite several requests for minutes of the Board of Management meetings for the period under review, none was provided for audit inspection. Consequently, we were unable to determine the frequency of Board meetings, the nature of the matters discussed, decisions made or whether those charged with governance provided adequate oversight of IT related issues.

Information Technology Steering Committee

2.8 Traditionally, an organization that places heavy reliance on information technology to achieve its mandate usually has an executive level committee as an integral part of its information technology governance framework. This committee, usually called an *IT Steering Committee*, is used to secure the direct involvement of senior management in directing and monitoring the use of IT in the organization. It is comprised of executive, business and IT management along with other critical organizational stakeholders to assist the Board in providing strategic direction for ICT across the entity.

2.9 The general purpose of the *IT Steering Committee* is to ensure that IT strategy is aligned with the strategic goals of the organization. It has overall responsibility for recommendations and decisions regarding IT priorities, funding and other IT and security requirements. The *Committee* is also responsible for tracking the status of IT projects and monitoring service levels. Despite its heavy reliance on technology, the TAJ did not have an *IT Steering Committee* that provided insight and advice to the Board of Management on areas such as the alignment of IT with the TAJ's business direction, the achievement of the TAJ's strategic IT objectives and the availability of suitable IT resources, skills and infrastructure to meet its strategic objectives. Consequently, we were unable to determine whether all relevant stakeholders were involved in the IT decision-making process and that all decisions were based on the TAJ's business goals. *The TAJ has since indicated that it accepts our recommendation to set up an IT Steering Committee for the Authority*.

Due to the absence of sufficient and appropriate evidence of IT governance from the Board of Management and the absence of a functional IT Steering Committee, we are unable to determine whether there was adequate oversight of the TAJ's ICT policies, strategies and operations by those charged with governance. Consequently, there is an increased risk that the TAJ's ICT infrastructure and control environment may not adequately support the organisation's business operations and meet its strategic objectives.

IT Strategic Planning

2.10 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.

2.11 Even though TAJ did not develop a separate IT strategic plan, the organisation incorporated its major IT strategies in its *Strategic Business Plan*. The TAJ's *Strategic Business Plan* outlined the general relationship between IT and the TAJ's strategic objectives, including the related costs as well as associated risks and mitigation strategies. A reasonable attempt was made to incorporate strategies focused on providing appropriate technological solutions to support TAJ's business objectives.

Based on the evidence provided, we have obtained reasonable assurance that the TAJ's IT strategies are generally aligned with its strategic business objectives.

IT Policies, Procedures and Plans

2.12 The Commissioner General, in carrying out the administration and management of the TAJ, is required to submit internal regulations, policies, strategic, corporate and other plans to the Board for approval in keeping with Section 11 of the Tax Administration Jamaica Act, 2013. The Board is responsible for overseeing the general administration of the Authority and *shall review, evaluate, approve and monitor the implementation by the Authority of its corporate policies, operational, strategic and other corporate plans* in keeping with Section 7 of the Tax Administration Jamaica Act, 2013.

2.13 IT plans, policies and procedures, like the IT strategic plan, are major components of an organization's IT governance function. IT plans, 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. However, our review revealed that the TAJ did not have any Board approved IT or IT related plans, policies or procedures in place to guide its IT operations. Despite developing at least twelve IT and IT related plans, policies and procedures ***(Table 1)***, there was no evidence that they were presented to the Board for review and approval. Some of these draft documents have also become out-dated as they do not take into account the 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 TAJ has not effectively documented, approved and implemented the necessary IT policies and procedures to facilitate the efficient and effective management of its IT operations. Consequently, current IT practices may be inconsistent or contrary to the organization's objectives.

Table 1: Draft Policies and Procedures

Policies/Plans/Procedures	Creation Date	Last Updated
ICT Contingency Plan	July 2013	April 28, 2016
ICT Policies	October 2012	October 2012
Information Technology Security Policy	Unknown	Unknown
Business Continuity Management Plan	Unknown	Unknown
Video surveillance and electronic access control policy, standards and procedures	March 26, 2014	March 26, 2014
Enterprise Risk Management Policy & Framework	May 2013	May 2013
Command Centre Standard Operating Policies and Procedures	June 2014	June 2014
Security Policy & Guidelines	Unknown	Unknown
Human Resource Policy	Unknown	Unknown
Occupational Safety and Health Policy	Unknown	July 2015
Disaster Preparedness Plan	May 2007	May 2007
Records Management Policy	May 2012	May 2012

Source:Tax Administration Jamaica

Inadequate Information Security Policy

2.14 An Information Security Policy is a formal statement that defines management's intentions on information security and provides general direction for protecting the confidentiality, integrity and availability of corporate information. The Information Security Policy should set out the organization's approach to managing its information security objectives. The policy should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) current and projected information security threat environment.

The Information Security Policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

c) processes for handling deviations and exceptions.

The Information Security Policy should be communicated to all employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader.

2.15 The TAJ's IT systems maintain and process highly sensitive and confidential taxpayer data. Therefore, information security must be a high priority and policies must be established to reduce the risk of unauthorised exposure or loss of this data. The TAJ's undated *Information Technology Security Policy* addresses some of the elements of information security. These include the definition and objectives of information security, the assignment of general and specific responsibilities for information security management and general guidelines on copyright and on certain specific IT resources/assets such as internet/email security. However, the policy does not take into account the current integrated IT environment, strategies and risks, the response mechanism for dealing with security breaches especially those relating to cyber-security, and the impact of relevant legislations such as the Cybercrimes Act and the Electronic Transactions Act. Additionally, the policy was not submitted to the TAJ's Board for approval and there was no evidence that the guidelines were communicated to all staff.

2.16 TAJ indicated that they recognize the need for a current information security policy and that steps are being taken to sensitize staff on the importance of information security.

The absence of a comprehensive and up to date approved information security policy increases the TAJ's vulnerability to information security risks and reduces its capacity to protect its IT assets/resources and safeguard the information contained within its IT systems. A security breach may not only cause an unauthorised exposure, corruption or loss of data but could also result in a disruption in the TAJ's operations.

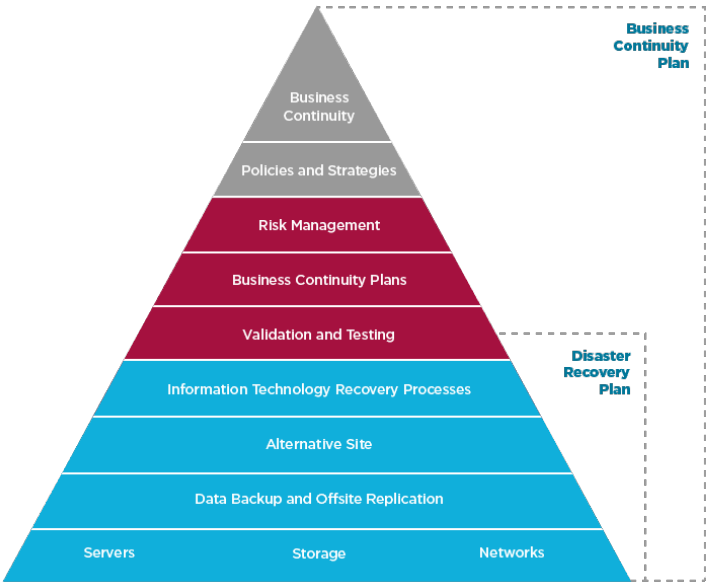
PART THREE

Business Continuity Management

3.1 The need for providing continuous IT services requires developing, maintaining and testing business continuity plans, utilising offsite backup storage and providing periodic continuity plan training[2]. 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 outdated when an emergency arises. Therefore, best practice requires that business continuity plans be reviewed and tested at regular intervals[3].

3.2 The general objective of developing and maintaining a business continuity plan is to maintain the integrity of the organisation's data together with an operational service and processing facility and if necessary, provide a temporary or restricted service until normal services can be resumed. The losses to an organisation that result from the unavailability of their business systems increase with time. The objective of business continuity planning is to make plans that are designed to reduce downtime and losses to the organisation. Plans therefore need to be detailed and outline the specific actions to be taken in order to restore key business activities in a variety of disaster scenarios.

Figure 5: Business Continuity and Disaster Recovery Planning



Source: www.boxuk.com

3.3 The TAJ currently relies on ICT to provide some of its most critical services such as payment of taxes, filing of tax returns, issuing and validation of TCC and TRN (including validation by third parties) and issuing of Driver's Licences. The Authority is also enhancing its ICT

[2] *COBIT 4.I-DS4: Ensure Continuous Service*
[3] *1SSAI 5310: Information System Security Review Methodology*

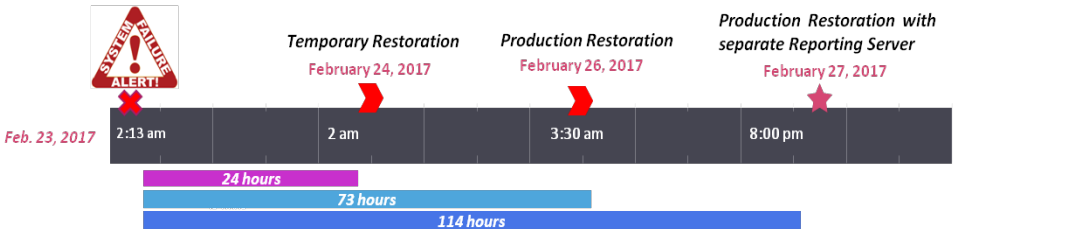
systems to facilitate increased internet transactions and use of improved data analytics to guide its compliance programme. Given TAJ's reliance on ICT to deliver its services, it is critical that TAJ has the capability to continue the delivery of its services at acceptable pre-defined levels following a disruptive event. This will require the identification of potential threats, assessing their likely impact on business operations and developing strategies to respond and restore operations.

Inadequate Business Continuity Planning

3.4 TAJ identified *inadequate business continuity and disaster management* as an area of significant risk exposure that could lead to major disruption in its operations. Despite this, the TAJ has not implemented an approved business continuity management plan to manage the risks associated with unplanned disruptions. A draft plan was prepared, however, no deadline has been established for its finalization and submission to the Board for approval. This increases the risk of system unavailability because no documented standard procedure is in place to respond to unplanned disruptions.

3.5 The risk of system unavailability was materialized in February 2017 when there was an interruption of the *Revenue Administration information System (RAiS)* and its dependent services resulting in a significant disruption and impact on Taxpayers, Tax Administration staff (including Cashiers) and other users such as financial institutions and government entities that rely on the system to process transactions. TAJ had to seek assistance from the system developer and other partners to restore operations. Some services were restored in 24 hours, however, it took the team approximately 114 hours (approximately five days) to restore the production environment to full capability.

Figure 6: RAiS Incident Timeline



Source: Tax Administration Jamaica

TAJ's review of the incident revealed several factors contributing to the delayed restoration. These include:

- Poor documentation of the production and disaster recovery setup.
- Absence of issue resolution thresholds for getting third party expertise involved.
- Absence of automatic notifications to the relevant persons within TAJ when a system failure has occurred.
- Absence of a checklist to determine when to switch to disaster recovery, and what is needed to do so.

The TAJ's failure to approve and implement a current business continuity management plan has exposed the entire organization to the risk of operational failure because it may not be able to restore normal services within a reasonable time if its IT systems are affected by a major disruption.

Inadequate Data Back-up Policy

3.6 Data held by TAJ on its IT systems represent one of its most vital assets. The IT systems and infrastructure must be organised to ensure that there is adequate redundancy, backup and restoration in the event of a disaster. TAJ must therefore have a comprehensive and up to date data backup, storage and restoration plan, policy and procedure to be able to quickly restore its systems to normal use after an unplanned disruption. The Authority must define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and its continuity plan.

3.7 Our review revealed that the TAJ did not have an approved, comprehensive and up to date backup plan or policy in place. Neither was there any system in place to ensure that backup media/data are tested periodically to determine the integrity and completeness of the backup files. Even though a backup schedule exits for the *Revenue Administration information System (RAiS)* and an *IT Contingency Plan* is being developed, the absence of a comprehensive backup plan/policy increases the risk of inconsistency in the performance of backup functions and procedures. Additionally, if the Authority fails to periodically test its backup systems and procedures this may lead to complications, delays or irrecoverable data loss in the event of an unplanned disruption especially if backup media are corrupted or certain members of staff are not available.

The TAJ's failure to approve and implement a comprehensive backup plan/policy and periodically test its backup systems has exposed the entire organization to the risk of operational failure because it may not be able to restore normal services within a reasonable time if its IT systems are affected by a major disruption.