AUDITOR GENERAL'S DEPARTMENT
INFORMATION TECHNOLOGY AUDIT REPORT
JAMAICA CUSTOMS AGENCY

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

Vision

Promoting a better country through effective audit scrutiny of Government operations.

Table of Contents

This page was intentionally left blank

Auditor General's Overview

The Jamaica Customs Agency (JCA) is mandated to assess and collect duties, fees, and penalties due on imported merchandise. It also has the responsibility of facilitating international trade while ensuring the protection of Jamaica's borders against illicit imports. JCA's services are therefore a significant source of tax revenue and contributor to national security and development.

The efficient execution of the JCA's functions is highly dependent on the use of Information Technology(IT) in its core processes. Given this dependence and the value of IT investments made over the years, the agency should implement the necessary controls to ensure that IT risks are managed in a structured manner. The JCA should also ensure that it can appropriately respond and continue to offer critical services in spite of technological disruptions.

In light of this, I commissioned an IT audit to determine whether the JCA has an effective Business Continuity Management System to ensure the timely resumption of critical services in the event of any serious interruptions. The audit revealed that the JCA did not have a Business Continuity Plan and its IT disaster recovery planning was limited to the failure of one application, though the agency was reliant on information maintained on several other systems. Consequently, the JCA may not be able to resume operations in a timely manner resulting in lengthy delays in the customs and clearance process for goods and passengers. We also found that though IT was a key business enabler, the JCA did not have an IT governance mechanism to ensure the systematic management of risk, proper resource allocation and the alignment of IT strategies with corporate objectives.

This report is intended to assist the JCA in improving its oversight of the IT function, risk management and continuity planning in order to reduce the likelihood and or impact of major disruptions on its operations. The management of the JCA is urged to implement the recommendations made in this report with a view to strengthen the agency's controls and ensure the continuity of critical business services to its customers.

I wish to thank the management and staff of JCA for the courtesies extended to my staff during the audit.

Pamela Monroe Ellis, FCCA, FCA
Auditor General

Executive Summary

The Jamaica Customs Agency (JCA) is charged with the collection of revenue, protection of Jamaica's borders against illicit imports and the facilitation of trade. JCA's vision is to become "A modern Customs Administration, delivering excellent service, fostering compliance and contributing to national development and protection of the society. The achievement of this vision is largely dependent on Information Technology (IT) thus the agency must implement strong controls to ensure the confidentiality and integrity of its data and information. Further, the JCA must ensure the availability of critical information systems to both internal and external customers to achieve strategic objectives and fulfil its vision.

An audit was commissioned to determine whether the Jamaica Customs Agency (JCA) has an effective Business Continuity Management System to ensure the timely resumption of critical services in the event of any serious interruptions. The audit involved a review of the entities general controls, systems and procedures in particular those relating to IT governance and business continuity for the financial years 2014/2015 to 2016/2017.

Key Audit Question

Does the JCA have an effective business continuity management system to ensure the timely resumption of critical services in the event of any serious interruptions?

What we found

Inadequate Information Technology Oversight

1. Oversight of the Information Technology (IT) function is typically achieved through the establishment of board and senior management committees responsible for providing strategic direction and ensuring the alignment of IT strategies with business objectives. We found that though the Information Management Unit (IMU) reported its operational performance to the executive management and Ministry of Finance and the Public Service, the JCA did not have an IT Steering Committee or equivalent to oversee the management of IT service delivery and projects. An IT Steering Committee, as recommended by best practice, would be responsible for determining IT investment priorities based on business strategies, IT project tracking, service level monitoring and improvements. However, the agency did not establish a committee to perform such functions and ensure the strategic alignment. For instance, we noted that the IMU developed an ICT strategic plan for the 2013/14 to 2015/16 financial years, however there was no evidence of formal review by a senior management committee to ensure consistency with the JCA's strategic priorities or availability of the resources required to execute the 20 strategies planned. Our examination of the plan revealed that the IT strategies were aligned to objectives that differed from the agency's strategic objectives for the respective financial years. We were also not assured that the impact on service delivery was independently assessed given the secondment of six officers to the ASYCUDA project. There were also no subsequent updates to the ICT strategic plan to reflect the ICT strategies pursued for the 2016/17 and 2017/18 financial years.

2. Additionally, our review of the plan revealed that the related costs were determined, however it did not identify the funding sources, capacity and human resource requirements for the execution of the strategies in keeping with international best practice. We were also not provided with periodic performance reports or any evidence that the JCA's management monitored the IMUs performance against the targets as stated in the ICT strategic plan. *The JCA has since indicated that it will establish an "ICT Strategic Committee" by October 2019*.

The absence of an oversight and monitoring function increases the risks that IT strategies may be pursued based on independent decision making by the IMU rather than through the involvement of relevant stakeholders. Additionally, inadequate monitoring may result in improper resource allocation, project conflicts and poor service delivery to internal and external customers. Further, IT investments may be made without a proper assessment of the relevant risks, resource requirements and value to the organisation as a whole.

Draft IT Policies and Weak System Settings

3. Management should develop appropriate policies and procedures to ensure that its directives are carried out. In addition, the development of operational procedures and proper communication ensures that risks are minimized and that the overall strategic objectives of the organization are achieved. However, we found that though the JCA had taken some steps to implement this control, the nine IT policies developed were not approved by management and thus not communicated to staff. The policies were reviewed by the IMU revision committee between August 2016 and January 2017 but final approval was not obtained as the Approval Committee consisting of executive JCA

members was disbanded and its functions transferred to the Executive Services Unit. *Subsequent to our audit, an ICT Policy Review Committee was formed resulting in the Commissioner approving seven of the reviewed policies along with four others. The JCA also advised that a "Laptop and Tablet User Agreement Policy" is scheduled for approval by October 31, 2019, while its "Application Acquisition and Development Policy" is being redrafted.*

4. Despite the JCA's reliance on its information systems and the need to ensure the confidentiality and integrity of customer data, we also found that critical network server policies were insufficient to ensure information security[1]. *The JCA has since taken the necessary corrective actions to reduce its network security risks.*

Unapproved IT policies and ineffective network settings represent vulnerabilities within the JCA's IT environment that may be exploited thereby increasing the likelihood of unauthorised access, unauthorised network changes and data loss. Additionally, these weaknesses threaten the JCA's ability to ensure the confidentiality and integrity of data as well as the availability of its systems to stakeholders.

Unstructured IT Risk Management

5. The management of IT risks is essential to information security and business continuity, especially where an organization is highly dependent on information technology to achieve its strategic objectives. Effective IT risk management should therefore be integrated with an entity's enterprise risk management framework to ensure that a systematic approach is taken in identifying, assessing and mitigating IT risks. However, our audit revealed that while the JCA had implemented elements of the World Customs Organization (WCO) risk management procedures in its core operations, the entity could not demonstrate that IT risks were managed in a structured manner. The JCA did not provide documentary evidence that security assessments were performed for critical systems and locations or that vulnerabilities and threats relevant to its IT assets were assessed.

The lack of formal IT risk management indicates that a systematic approach is not being used in the identification, assessment and mitigation of IT risks. Consequently, the agency cannot be assured that controls are being employed in areas of significant risks. Further, in the event of a disruption the JCA's current risk response may not be sufficient to ensure the availability and timely recovery of its systems.

6. *The JCA has since indicated that an appropriate standard will be identified to develop and implement an IT risk register before the end of the 2019/2020 financial year.*

[1] *The details of the weaknesses identified were excluded from the report due to the information security risks.*

Absence of Management Commitment to Business Continuity Planning

7. Business Continuity Management (BCM) is a holistic management process that identifies the potential threats to an organization and impacts to business operations in order to implement appropriate mitigating strategies and ensure an effective response to disastrous events. Management is therefore required to demonstrate its commitment and leadership in the process by clearly communicating its intent and objectives, assigning roles and responsibilities and ensuring the availability of the necessary resources. However, the commitment of JCA's management was not evident as the agency did not define its business continuity policy, objectives, scope and budget necessary to guide and support its business continuity and disaster recover planning. The JCA also did not clearly identify the responsible officers and their roles in the BCM process. In addition, we found no evidence that the agency developed or adopted a framework to guide the approach being taken to plan, execute, communicate and test the BCP and IT Disaster Recovery Plan. *Subsequent to audit, the JCA established a committee with responsibility for the agency's business continuity planning. The agency also advised that it intends to make provisions for the BCP in its budget for the 2020/2021 financial year.*

Without top management's involvement, the business continuity planning process may not achieve its objectives as staff are not likely to participate in the activities and may perceive them as insignificant or unrelated to the achievement of performance targets. Consequently, the JCA will be unable to collectively respond to a major disruption in a timely manner.

Inadequate Business Continuity and Disaster Recovery Planning

8. Business continuity and disaster recovery planning should be conducted by all organizations as a corrective control to reduce the likelihood and impact of a disruption on critical business processes. Proper planning therefore requires the development, maintenance and testing of Business Continuity and IT Disaster Recovery Plans. The plans should be prepared based on the risks to the organization, potential business impacts, requirements for resilience, alternative processing and the recovery capability of all critical IT services. The JCA did not have a Business Continuity Plan. Additionally, the agency's draft IT Disaster Recovery Plan only related to the Automated System for Customs Data (ASYCUDA) World application though reliance was placed on 15 legacy systems for historical data used for valuations, the establishment of risk patterns and backup transaction processing. The development of the plan was also not informed by a risk assessment and Business Impact Analysis (BIA), which would allow the JCA to determine the significant risks to be managed, critical services, acceptable downtime and data loss.

9. Additionally, we noted that the plan, which has been in a draft state for approximately 17 months, did not identify the key contacts, critical processes, required resources (financial and non-financial) and alternate processing sites. Also, the plan only considers recovery procedures in the event of a system failure and excludes likely risks such as the loss of internet connectivity and power. For instance, between August 2015 and July 2017, the JCA recorded 40 incidents that negatively affect the availability and performance of the ASYCUDA application, of which 23 per cent were due to

disruptions in the internet connection. T*he JCA has since drafted a business continuity plan but intends to engage a consultant to assist in its business continuity and disaster recovery planning.*

As the risk assessment and Business Impact Analysis were not conducted, the JCA may not have appropriately identified its risks and critical business processes to ensure that effective mitigating and recovery strategies are implemented. Additionally, failure to prepare a comprehensive Business Continuity Plan and IT Disaster Recovery Plan may result in recovery delays, below target revenue collections and reputational damage to the organization.

.

What should be done

1. An IT governance framework should be adopted to ensure that IT resources are directed and controlled in a manner that ensures proper risk management, performance measurement and the alignment of IT strategies with the JCA's strategic objectives. The framework should encourage the establishment of oversight committees and the development of appropriate policies, roles and responsibilities to ensure accountability and the use of IT resources to deliver value to all stakeholders.

2. The Information Management Unit (IMU) should develop an IT risk management framework that ensures the systematic identification, assessment and mitigation of risks to the achievement of the agency's strategic objectives.

3. Management should adopt a framework to guide the structured development of the agency's Business Continuity Plan (BCP) and IT Disaster Recovery Plan (IT DRP). The framework should encourage a systematic approach to identifying significant risks and critical business processes to ensure that the required resilience of the IT infrastructure is determined and appropriate strategies are employed to prevent or minimise the impact of a major disruption. The BCP and IT DRP should clearly outline the roles and responsibility of the planning team, recovery team and external service providers, key contacts, recovery procedures, alternate processing sites and key dependencies for critical systems. Plans should also be tested to ensure that recovery can be achieved in the established recovery time and manner.

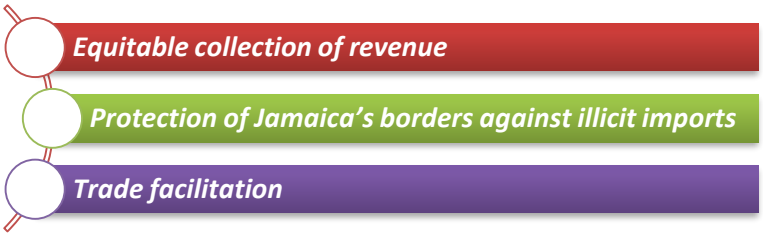
Part One

Introduction

Background

1.1 The Customs Department was established under Section 12 of the Revenue Administration Act, with responsibility for the collection of all customs duties and other related revenue on behalf of the Government of Jamaica. On April 2, 2013, the Department was designated with the status of Executive Agency in accordance with the Executive Agencies Act, 2002, as it is envisaged that the transition will assist the organization to achieve its mandate, improve accountability and efficiency through the flexible management of its resources. The agency is a Principal Receiver of Revenue (PRR) and contributes an average of 35 per cent in national tax revenue annually.

1.2 The Jamaica Customs Agency (JCA) has three specific mandates[2]:



1.3 JCA's mandates are executed by conducting the following activities:

- Assessing and collecting customs duties, fees, and penalties due on imported merchandise.
- Interdicting and seizing contraband, including narcotics and illegal drugs.
- Processing passengers, baggage, cargo and mail.
- Detecting and apprehending persons engaged in fraudulent practices designed to circumvent Customs related laws.
- Protecting the general welfare and security of Jamaica by enforcing import and export restrictions and prohibitions, including money laundering.
- Protecting Jamaica's industries, labour and intellectual property rights by enforcing Jamaica's laws intended to prevent illegal trade practices, including provisions related to quotas; the Anti-Dumping Act; and by providing Customs Records for copyrights, patents, trademarks.

1.4 Though traditionally a highly paper based organization, the JCA has over the years sought to improve the efficiency of its operations through the implementation of approximately 17 information systems. In April 2014 the JCA through funding from the Inter-American Development Bank, commenced the phased implementation of the Automated System for Customs Data (ASYCUDA) World application to replace its legacy systems. ASYCUDA World is a web-based integrated customs management system developed by the United Nations Conference on Trade

[2] *JCA Strategic Business Plan 2013 - 2016*

and Development (UNCTAD) to, inter alia, improve the clearance of goods and increase revenue collections. The system allows customers such as importers, Customs Brokers and Shipping Agents, to electronically submit manifest, declarations, payments and other documents for review by Customs Officers. It also facilitates communication between the JCA and customers by sending notifications and allows users to track their transactions through the various stages of the process.

1.5 The benefits from the implementation of ASYCUDA and other technological investments will contribute to the achievement of "*National Outcome # 8 - An Enabling Business Environment"* of the Vision 2030 Jamaica - National Development Plan, which specifically identifies improved customs and clearance process for imports and exports as a key sector strategy.

Audit Scope and Methodology

1.6 In keeping with my constitutional mandate, an Information Technology audit was commissioned to determine whether the Jamaica Customs Agency (JCA) has an effective Business Continuity Management System to ensure the timely resumption of critical services in the event of any serious interruptions. We also assessed the adequacy of the JCA's Information Technology Governance and examined, on a test basis, evidence supporting compliance with relevant policies, laws and regulations applicable to the Information and Communications Technology (ICT) operations of the agency. The review spanned the 2014/2015 to 2016/2017 financial years.

1.7 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 (ISSAI) 5310: Information System Security Review Methodology 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).
- ISO 22301:2012 – Societal Security – Business Continuity Management System – Requirements issued by the International Organization for Standardization (ISO) and the International Electro-Technical Commission (IEC).

1.8 These standards and guidelines enabled us to test and compare the entities general computer controls against international benchmarks and widely accepted best practices within the Information and Communications Technology (ICT) sector.

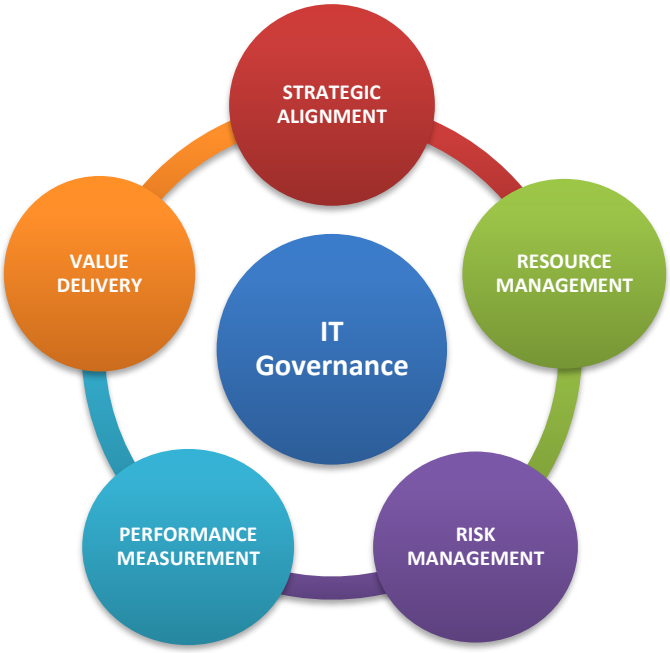
1.9 Our assessment was based on the review of general IT controls, external documents, physical examinations, interviews with senior management and staff, observations and analysis of other related information.

Part Two

Information Technology Governance

2.1 Information Technology (IT) Governance is a component of Corporate Governance, which focuses on the direction and control of IT resources to ensure that organizational goals are achieved in an efficient and effective manner. It is a combination of principles, strategies, activities and structures established to ensure that investments in IT generates value for stakeholders, risks are managed and performance is monitored. A good IT Governance mechanism should therefore provide an effective oversight of the IT function through clearly defined roles and responsibilities, performance measurement, risks management, an alignment of IT strategies with business strategies as well as the documentation of IT plans, policies and procedures.

Figure 1: Elements of IT Governance



Source: COBIT 4.1

2.2 IT Governance has a pervasive impact on any entity's IT environment and if improperly implemented may result in an ineffective use of information technology resources by an organization. Our review of the Jamaica Customs Agency (JCA) revealed that it has taken some steps towards good governance, however improvements are required in the oversight, strategic alignment and management of IT risks to ensure that IT investments deliver value to all stakeholders and contributes to the fulfilment of the agency's mandate.

Information Technology Oversight and Strategic Planning

2.3 As an executive agency, the governance of the Jamaica Customs Agency (JCA) includes reporting to an advisory board and to the Minister of Finance based on a performance agreement. According to the JCA's framework document, *the board should advise the Chief Executive Officer (CEO) on the agency's corporate and operational plans, performance indicators and targets*[3]. Periodic reviews of the corporate and operational plans should also be carried out by an Executive Management Team, which is accountable to the CEO for the general performance of the agency against its targets. In addition, the JCA reports the status of major ICT deliverables to the Strategic Planning Unit of the Ministry of Finance and the Public Service. However, we noted that the JCA did not implement specific measures to monitor and ensure the strategic alignment of the Information Technology (IT) activities with the organization's strategic goals and objectives.

2.4 International best practice recommends the establishment of an IT Steering Committee consisting of executive, business and IT management that is responsible for determining IT investment priorities based on business strategies, IT project tracking, service level monitoring and improvements. It is also recommended that IT strategic plans be developed to manage and direct all IT resources in line with business strategies and priorities. Accordingly, IT strategic plans should clearly define how IT goals will contribute to strategic objectives, the related costs and risks of an organization. The plan should include an investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements[4]. Further, the plan should be reviewed by the IT steering committee to ensure alignment with the organizations objectives and the availability of required resources.

2.5 Though the JCA's executive management team reviews the operational performance of the Information Management Unit (IMU) it is neither responsible for overseeing the management of IT service delivery and projects nor ensuring that IT strategies and business objectives are aligned. As a result, we noted that the IMU developed an ICT strategic plan for the 2013/14 to 2015/16 financial years, however there was no evidence of formal review and approval to ensure the alignment of the 20 strategies planned with the agency's strategic priorities or availability of the required resources for each. We also noted that the IT strategies were aligned to objectives that were not consistent with the JCA's strategic objectives for the respective financial years. While the strategic plan reflected the associated costs, it did not identify the funding sources, capacity and human resource requirements for the execution of the strategies in keeping with best practice. We were also not assured that the impact on service delivery was independently assessed, given the secondment of six officers to the ASYCUDA project. Additionally, the IMU did not provide any reports to the executive management on its performance against the targets as stated in the ICT strategic plan. There were also no subsequent updates to reflect the ICT strategies pursued for the

[3] Statement extracted from the Jamaica Customs Agency Framework Document
[4] *COBIT PO4.3IT Strategic plan*

2016/17 and 2017/18 financial years. *The JCA has since indicated that it will establish an "ICT Strategic Committee" by October 2019.*

The absence of an oversight and monitoring function increases the risks that IT strategies may be pursued based on independent decision making by the IMU rather than through the involvement of relevant stakeholders. Additionally, inadequate monitoring may result in improper resource allocation, project conflicts and poor service delivery to internal and external customers. Further, IT investments may be made without a proper assessment of the relevant risks, resource requirements and value to the organisation as a whole.

IT Policies and Procedures

2.6 Generally, management must develop and appropriately communicate its policies and procedures to obtain reasonable assurance that the organization's objectives will be achieved. Policies represents the formal means by which management communicates its intent, while procedures provide guidance in implementing a policy. They are therefore critical to the effective management of the IT processes and associated risks. However, we found that this element of control was lacking as IT related policies though developed were not approved by management.

2.7 In recognition of the need for formal IT policies, the JCA's organizational structure includes a position titled "ICT Policies, Projects and RM Manager" that is responsible for establishing and maintaining appropriate and effective ICT policies. According to the job description dated August 13, 2014, the respective officer should lead the establishment and use of ICT policies as well as develop, document and communicate ICT policies. We found that an officer who was engaged on September 1, 2015 drafted nine policies and was in the process of drafting two others at the time of our audit (Table 1). Our examination revealed that the policies were reviewed by the IMU revision committee between August 2016 and January 2017, however they did not obtain final approval and thus were not communicated to staff. The policies referred to an Approval Committee consisting of executive JCA members but we were advised that the committee was disbanded and its functions transferred to Executive Services Unit.

Table 1: Information Technology Policies Drafted

No.	Policy	Status	Last revision date
1.	Acceptable Use Policy	Draft Completed	August 25, 2016
2.	Internet Usage Policy	"	August 25, 2016
3.	Password Policy	"	August 25, 2016
4.	Clean Desk Policy	"	August 17, 2016
5.	Laptop and Tablet User Agreement Policy	"	August 12, 2016
6.	Email and Communication Policy	"	August 17, 2016
7.	Application Acquisition and Development Policy	"	December 6, 2016
8.	Electronic Records and Information Management Policy	"	October 14, 2016
9.	Human Resource Security Policy	"	January 21, 2017
10.	Physical Access Control Policy	In Progress	-
11.	Ethics Policy	"	-

Source: Jamaica Customs Agency

2.8 A review of the Account Policies on the server operating system was also conducted to determine whether the settings were sufficient to ensure information security. Despite the confidential nature of the importer data and reliance on information systems to accurately account for the JCA's revenue, we identified several weaknesses that separately or combined may result in unauthorised access and exploitation of the agency's network.[5]

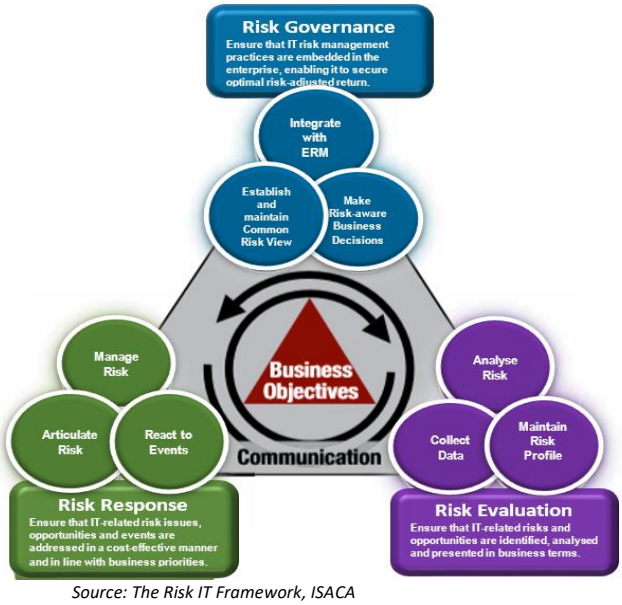
> Unapproved IT policies and ineffective network settings represent vulnerabilities within the JCA's IT environment that may be exploited thereby increasing the likelihood of unauthorised access, unauthorised network changes and data loss. Additionally, these weaknesses threaten the JCA's ability to ensure the confidentiality and integrity of data as well as the availability of its systems to stakeholders.

2.9 *Subsequent to the audit, an ICT Policy Review Committee was formed resulting in the Commissioner approving seven of the mentioned policies along with four others between April and September 2018. The JCA also advised that the "Laptop and Tablet User Agreement Policy" is scheduled for approval by October 31, 2019, while the "Application Acquisition and Development Policy" is being redrafted. Additionally, the JCA has taken the necessary corrective actions to reduce its network security risks.*

IT Risk Management

2.10 International best practice encourages the development of an IT risk management framework that is aligned to the organization's enterprise risk management framework[6]. By developing a framework, management demonstrates that a systematic approach will be used to identify and assess risks as well as implement mitigating strategies to minimise risks to an acceptable level.

Figure 2: IT Risk Process



Source: The Risk IT Framework, ISACA

[5] *The details of the weaknesses identified were excluded from the report due to the information security risks.*
[6] *CoBiT 4.1 - PO9 Assess and Manage IT Risks*

2.11 An effective risk management approach is also fundamental to business continuity planning as it allows an organization to identify vulnerabilities and threats to IT resources that support critical business processes. The organization would also be able to develop action plans outlining mitigating strategies that would be employed to protect its assets. However, our audit revealed that though the JCA had implemented elements of the World Customs Organization (WCO) risk management procedures in its core operations, the entity could not demonstrate that IT risks were managed in a structured manner. For instance, the agency was not able to provide formal security assessments of critical systems and locations or assessments of vulnerabilities and threats to its IT assets for review. *The JCA has since indicated that an appropriate standard will be identified to develop and implement an IT risk register before the end of the 2019/2020 financial year.*

The lack of formal IT risk management indicates that a systematic approach is not being used in the identification, assessment and mitigation of IT risks. Consequently, the agency cannot be assured that controls are being employed in areas of significant risks. Further, in the event of a disruption the JCA's current risk response may not be sufficient to ensure the availability and timely recovery of its systems.

Part Three

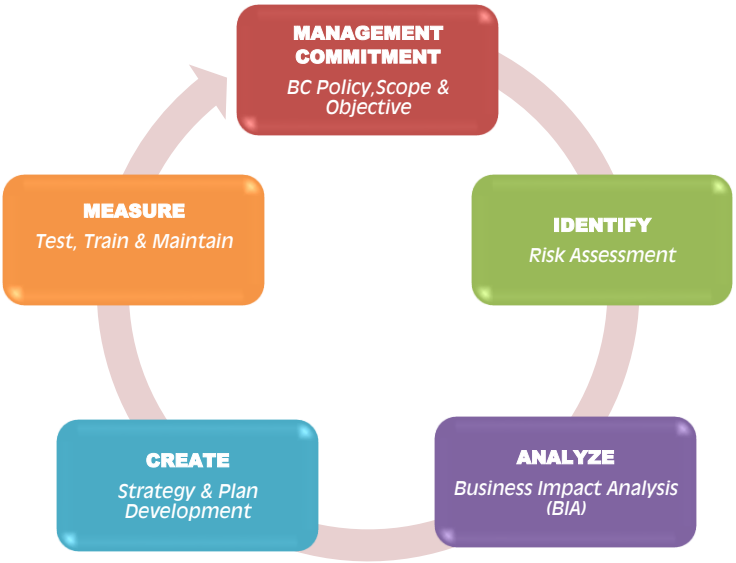
Business Continuity Management

3.1 In the execution of its mandate, the JCA generates on average 35 per cent of the government's revenue. The agency also plays a pivotal role in the nation's security as it is responsible for implementing effective controls to protect our borders from illicit imports, while facilitating trade. It is therefore imperative that the agency adopts a systematic approach to business continuity to ensure the restoration of its services within a reasonable time and with minimal impact on Jamaica's tax revenue, security and economy.

3.2 While disruptions may be in the form of system failures, business continuity is not the sole responsibility of the IT function but rather incorporates the entire organization to ensure an effective response and timely resumption of business activities. Accordingly, international best practice defines Business Continuity Management (BCM) as a holistic management process that identifies potential threats to an organization and the impacts to business operations. It provides a framework for the development of organizational resilience with the capability of an effective response that safeguards the interest of its key stakeholders, reputation, brand and value-creating activities.[7]

3.3 The BCM process is a structured approach to identifying risk, critical business activities and developing an appropriate strategy and plan to effectively respond to disastrous incidents. However, successful business continuity planning requires management to first demonstrate its commitment to the process by defining a policy, establishing clear objectives and ensuring the availability of the necessary financial and non-financial resources.

Figure 3: Business Continuity Management Process



Source: Auditor General's Department

[7] *ISO 22301:2012 - Societal security — Business continuity management systems — Requirements*

3.4 Our audit revealed that the JCA's business continuity management process had several weaknesses, which may result in extensive delays in the collection of revenue and clearance of imported goods.

Management Commitment to Business Continuity Planning

3.5 In an effort to ensure business continuity, management must demonstrate its commitment to the implementation of the Business Continuity Management System (BCMS) by developing a business continuity policy, establishing clear objectives that are aligned with the strategic direction of the organisation, assigning roles and responsibilities as well as ensuring that the necessary resources are available[8].

3.6 We found that the JCA's management had engaged in some continuity planning, however it did not define its policy, objectives, scope and make the necessary budgetary provisions to support the business continuity planning process. Though the Information Management Unit (IMU) and Occupational Health & Safety Unit (OH&SU) contributed to the disaster recovery and emergency management planning, the agency did not identify the officers responsible for the development of the Business Continuity Plan (BCP). We also found no evidence that the agency developed or adopted a framework to guide the approach that would be taken to plan, execute, communicate and test the BCP and IT Disaster Recovery Plan. *Subsequent to audit, the JCA established a committee with responsibility for the agency's business continuity planning. The agency also advised that it intends to make provisions for the BCP in its budget for the 2020/2021 financial year.*

Without top management's involvement, the business continuity planning process may not achieve its objectives as staff are not likely to participate in the activities and may perceive them as insignificant or unrelated to the achievement of performance targets. Consequently, the JCA will be unable to collectively respond to a major disruption in a timely manner.

Business Continuity and Disaster Recovery Planning

3.7 An organization's ability to provide continuous service is dependent on the proper development, maintenance and periodic testing of its Business Continuity and IT Disaster Recovery Plans. International best practice therefore recommends that organizations prepare IT continuity plans based on an understanding of risks, potential business impacts and requirements for resilience, alternative processing and the recovery capability of all critical IT services[9]. Our audit revealed that the JCA did not have a Business Continuity Plan and its IT Disaster Recovery Plan (IT DRP) only related to one of several applications used by the agency.

3.8 Prior to 2014, the JCA was largely a paper-based organization with some operational functions being partially automated through 17 distinct systems. However, in April 2014 the JCA commenced the phased implementation of the Automated System for Customs Data (ASYCUDA) application to improve service delivery, revenue collection and trade facilitation. ASYCUDA is an integrated web-based system that should allow the agency to transition to a paperless organization through the use

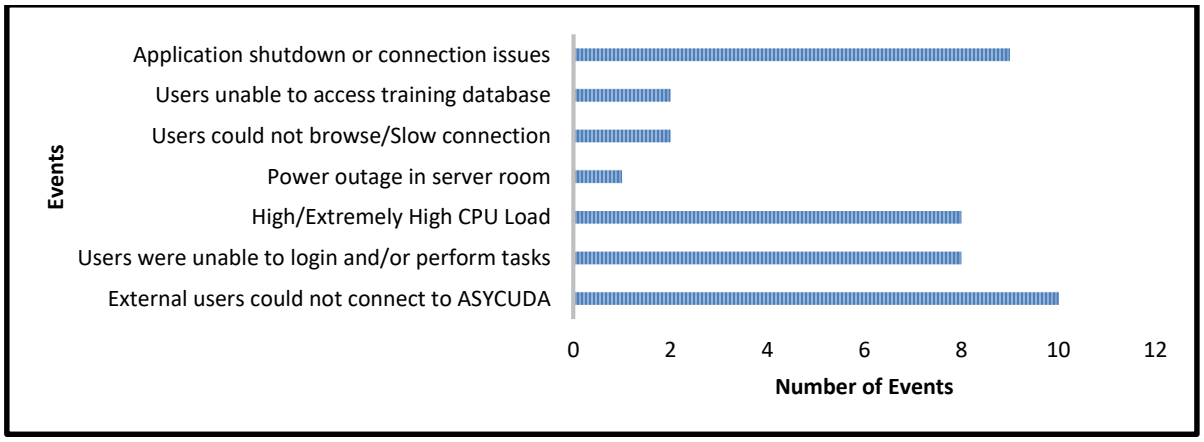
[8] *ISO 22313:2012 Societal security—Business continuity management systems—Guidance*
[9] *CoBiT 4.1 - DS 4.2 IT Continuity Plans*

of electronic documents in its core operational activities. Up to August 2017, the JCA had fully implemented modules for cargo reporting, cargo release and declaration processing.

3.9 We found that the IMU only drafted an IT Disaster Recovery Plan (IT DRP) for the ASYCUDA World application, despite the JCA's daily reliance on 15 legacy systems for historical data to assist with valuations, the establishment of risk patterns and backup transaction processing. We further noted that the development of the IT DRP was not informed by the results of a thorough risk assessment and Business Impact Analysis (BIA), which would allow the JCA to determine the significant risks to be managed, critical services, acceptable downtime and data loss.

3.10 Additionally, our review revealed that though the IT DRP was in draft for approximately 17 months, it did not identify the key contacts, critical processes, required resources (financial and non-financial) and alternate processing sites. We also noted that the plan only considers recovery procedures in the event of a system failure and excludes loss of internet connectivity and power, which are critical for web based systems and likely after a natural disaster in Jamaica. For instance, we noted that between August 2015 and July 2017, the JCA recorded 40 events/incidents in the ASYCUDA issues log that resulted in the unavailability and slow performance of the application (Figure 5). Of the total, approximately 23 per cent of the events were due to disruptions in the internet connection. Though the JCA has a secondary internet connection, the risk has not been formally assessed and the relevant recovery procedures and time were not documented in the IT DRP. T*he JCA has since drafted a business continuity plan but intends to engage a consultant to assist in its business continuity and disaster recovery planning.*

Figure 4: Summary of ASYCUDA incidents between August 2015 and July 2017



Source: JCA – ASYCUDA Issues Log

As the risk assessment and Business Impact Analysis were not conducted, the JCA may not have appropriately identified its risks and critical business processes to ensure that effective mitigating and recovery strategies are implemented. Additionally, failure to prepare a comprehensive Business Continuity Plan and IT Disaster Recovery Plan may result in recovery delays, below target revenue collections and reputational damage to the organization.

This page was intentionally left blank