INFORMATION TECHNOLOGY AUDIT REPORT

ON THE

MANAGEMENT OF IT SECURITY

OF

SELECT PUBLIC BODIES (RGD & JUTC)

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.

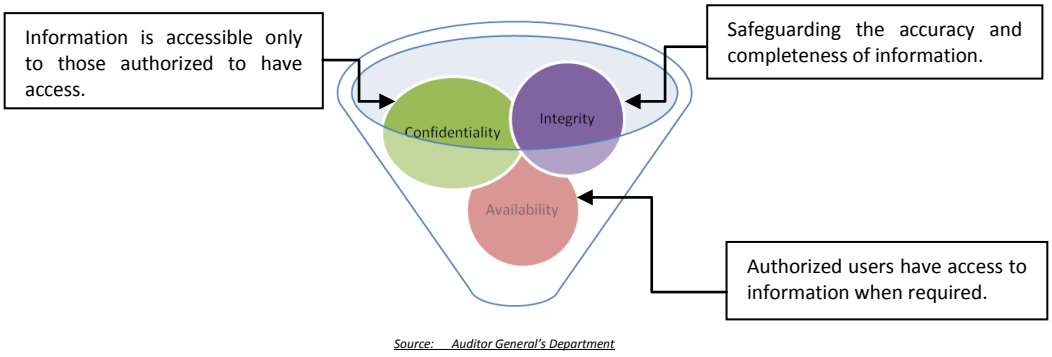
This report was prepared by the Auditor General's Department of Jamaica for presentation to the House of Representatives.

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

Information Security



Source: Auditor General's Department

AUDITOR GENERAL'S OVERVIEW

Despite the significant benefits to be derived from the use of information technology (IT), IT environments are characterized by a variety of risks including accidental loss of information, technological failures, compromise of data integrity, unauthorized access and misuse of information and system resources. With the increased use of information and communication technology (ICT) by public sector agencies, it has become necessary to respond to these risks in order to safeguard the confidentiality, integrity and availability of information and information systems from technology related threats.

Two major public sector agencies that have significantly increased their reliance on IT are the Registrar General's Department (RGD) and the Jamaica Urban Transit Company (JUTC). The RGD has increasingly incorporated technology in its operations, especially in the recording of Births, Deaths and Marriages while the JUTC has increased its reliance on technology in the collection and accounting for revenue through its *Electronic Fare Collection System*. Going forward it is anticipated that the RGD will have responsibility for civil registration and other civil identification functions under the National Identification System (NIDS) while the JUTC has targeted greater technological integration in its fleet maintenance, vehicle location and monitoring, and cashless fare collection. Given their reliance on technology in current and future operations, there is a need to have appropriate systems in place to safeguard their IT assets and maintain data integrity in order to achieve their strategic objectives. This will require the implementation of an appropriate IT security management system.

I commissioned an IT audit of the two public bodies to determine the effectiveness of their IT security controls and IT security management systems and processes. The audit revealed that both entities have recognized the need for improvements in their IT security and steps are being taken to review and improve their IT security controls. Nevertheless, they remain vulnerable to information security threats due to inadequacies in their information system security controls and IT governance.

This report is intended to assist both agencies to strengthen their IT control environment in order to reduce the likelihood and or impact of IT security risks on their operations. It is therefore crucial that the management of the RGD and the JUTC carefully review the recommendations contained in this report with a view to strengthening their control systems by adopting the measures outlined.

I wish to thank the management and staff of the RGD and the JUTC 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

In today's increasingly computerized environment Ministries, Departments and Agencies (MDAs), which are reliant on computer systems for their operations must protect their systems against a variety of threats which range from unauthorized remote access (commonly known as hacking), loss of data, system disruptions, and physical damage to IT equipment to manipulation of information for fraudulent purposes. MDAs must ensure that their IT systems operate efficiently whilst ensuring that critical resources are protected against IT security threats. Given this increased reliance on technology there is a need to have effective systems in place to safeguard the confidentiality, integrity and availability of information.

We undertook an IT audit of two public bodies, namely the Registrar General's Department (RGD) and the Jamaica Urban Transit Company (JUTC) to determine the effectiveness of their IT security controls and IT security management systems and processes. We also assessed the effectiveness of their IT governance and their compliance with relevant standards that are applicable to Information and Communication Technology (ICT) operations within each entity.

Key Audit Question

Was an effective information security management system in place to safeguard the confidentiality, integrity and availability of information from IT threats?

What we found

Both entities were vulnerable to information security threats due to inadequate information system security controls and inadequate IT governance.

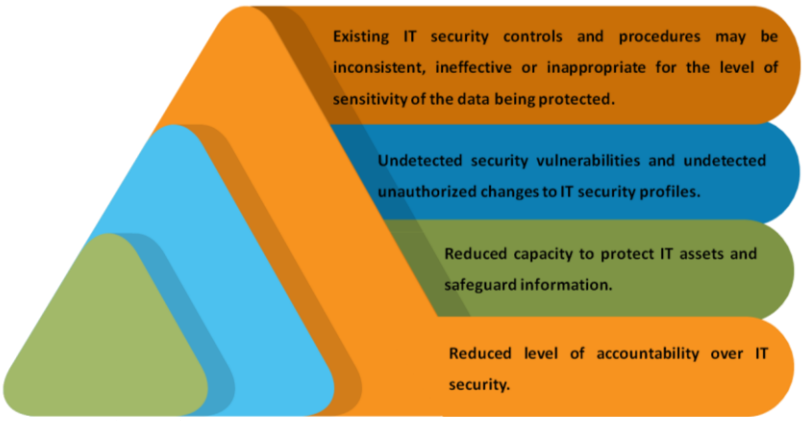
Both entities have a high IT risk exposure and may not be able to respond appropriately in the event of a threat affecting their IT environment.

Inadequate Information Security Management System (ISMS)

1. Information systems that maintain and process highly sensitive and confidential information require effective data protection and security controls as well as appropriate policies to reduce the risk of unauthorised access, exposure or loss. Although RGD had developed security policies for its network and servers and JUTC had developed a "Computer, Network & Internet Acceptable Usage Policy"***, neither entity had established an enterprise IT security policy to manage access to all their IT resources and to ensure appropriate preservation of data confidentiality, integrity and availability***. Additionally, the RGD, which is responsible for the safe custody of vital records including birth, death and marriage records, did not develop a data classification system in order to establish appropriate baseline security controls for the protection of its data.

2. ***Neither entity had established an IT security function to ensure that there was a consistent and co-ordinated approach to IT security across each organization***. While members of their IT department performed some IT security related functions, the IT security roles and responsibilities were not clearly defined, in particular the roles and responsibilities of management, users and IT personnel. Additionally, the organizations did not have an effective system in place to conduct security screening of potential IT employees, sensitize staff about IT security or monitor the activities of users with administrator privileges on their network.

Figure 1: Implications of Inadequate ISMS



Source: Auditor General Department

3. Both agencies indicated that there were broad security measures in place to protect their IT assets, however, they acknowledged the need to improve their ISMS and has committed to doing so in the shortest possible time.

IT Risk Assessment - JUTC

4. The JUTC has an increased IT risk exposure and may not be able to respond appropriately in the event of a threat affecting its IT environment due to the absence of a current and comprehensive IT risk assessment to determine the vulnerabilities associated with its IT environment and threats to its IT resources in order to develop appropriate responses. A

draft risk assessment was started in 2015, however, the document has not been finalized and approved by the JUTC's management. The JUTC has since indicated that steps will be taken to complete the IT risk assessment and improve its overall risk management.

Inadequate Oversight of RGD's ICT Operations

5. ***RGD did not have an executive level committee as part of its IT governance structure that included all relevant organizational stakeholders to provide strategic direction for ICT across the entity***. There was therefore an increased risk that not all IT decisions were based on the RGD's business goals and not all relevant stakeholders were involved in the IT decision-making process. ***There was also no system in place to provide management with independent assurance on the efficiency and effectiveness of its IT controls***. Consequently, one of the most significant aspects of its operations was not subjected to regular, independent reviews to ensure that management was aware of weaknesses or critical risks associated with its IT systems. The Agency has since indicated that efforts will be made to establish a committee to provide oversight of its IT function and its "internal audit department is currently undergoing training to improve their competencies to perform in depth audits of the IT department".

Inadequate Environmental Controls in RGD's Server Room

6. All computer equipment operates under potentially unstable environmental conditions and therefore, appropriate and effective controls that monitor and prevent damage caused by environmental factors should exist to reduce the risk of loss and downtime. ***We found that the safety of RGD's server room might be compromised due to the absence of appropriate equipment to monitor the room's environmental condition such as its temperature and humidity.*** The server room was also not equipped with a smoke detector to provide an alert in the event of a fire. This increased the risk of damage to the RGD's most critical computer equipment resulting in the possible loss of vital records and disruption in operations. The RGD indicated that steps will be taken to address these concerns, however, no timeline was provided.

What should be done

1. RGD and JUTC should strengthen their information system security and related controls and IT governance to safeguard the confidentiality, integrity and availability of their information and information systems from IT security threats that may compromise their operations.

2. JUTC should implement a robust IT risk management system to ensure that IT risk assessments are conducted at planned intervals in order to identify appropriate risk responses and implement relevant IT security controls.

PART ONE

Audit Objective, Scope and Approach

1.1 In keeping with her constitutional mandate, the Auditor General commissioned an IT audit of the Registrar General's Department (RGD) and the Jamaica Urban Transit Company (JUTC) to determine the effectiveness of their IT security controls and IT security management systems and processes. We also assessed the effectiveness of IT governance within both entities and 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 Information System Security 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 information security across major security domains including:

- IT Security Policies
- Information Security Risk Management
- Human Resources Security
- Access Control
- Physical and Environmental Security

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

Registrar General's Department (RGD)

Background

2.1 The Registrar General's Department (RGD) was established in 1879 with a mandate to register all births, deaths, marriages and adoptions in Jamaica through the General Records Office. It is also responsible for the safekeeping of public records such as Resident Magistrate and Supreme Court wills, Certificates of Citizenship and Naturalization as well as Acts of Jamaica through the Island Record Office. The RGD became an Executive Agency in 1999 and expanded its scope of services to include genealogical research, registry weddings, drafting of deeds poll and asset lien verification. The aim of the RGD is to capture and preserve the records of all life events occurring within the boundaries of Jamaica to support national planning and development.

Table 1: Income from Operations

Income Source	2016/2017[1]	2015/2016[2]	2014/2015[2]
Certificate Production	371,985,027.00	381,819,938.00	355,061,472.00
Record Updating	119,398,300.00	119,810,500.00	98,349,715.00
Registration Fees	10,800,900.00	11,462,100.00	11,502,900.00
Marriage Ceremonies	16,790,200.00	17,378,850.00	15,607,150.00
Express Fee	188,196,050.00	199,115,950.00	188,074,725.00
Income from Island Record Office	60,750,476.00	58,695,580.00	51,818,921.00
Other Operating Fees	10,044,588.00	15,868,378.00	10,578,880.00
	777,965,541.00	**804,151,296.00**	**730,993,763.00**

Source: RGD Financial Statements

2.2 The RGD has increasingly incorporated technology in its operations to improve access, efficiency, customer service and its business processes. The Agency's IT related priority plans and programmes include:

- Establishing an electronic database of vital records through the digitization of current paper records and the electronic capture of all birth, death and marriage records.
- Development of an application to facilitate online verification of its certificates.
- Upgrade of its Birth, Death and Marriage System (BDMS) to improve efficiencies in its operations.

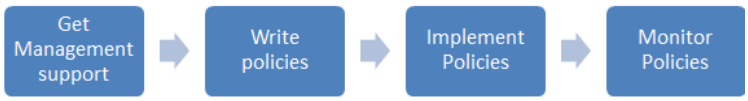
[1] *Unaudited Financial Statements*
[2] *Audited Financial Statements*

2.3 The BDMS is deployed over the Agency's IT network and is therefore inherently vulnerable to unauthorized access, manipulation and disclosure of confidential information. Given the RGD's increased reliance on technology in its operations, especially in the recording of Births, Deaths and Marriages, there is a need to safeguard the confidentiality, integrity and availability of information from IT related threats, taking into account the various security related vulnerabilities. This will require establishing and maintaining IT security roles and responsibilities, policies, standards and procedures.

Information Security Policy

2.4 An Information Security Policy (ISP) is a formal statement that defines management's intentions on information security and provides general direction for protecting the confidentiality, integrity and availability of information. The policy should set out the organization's approach to managing its information security objectives. The ISP should be communicated to all employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader.

Figure 2: Information Security Policy



Source: http://resources.infosecinstitute.com/information-security-policies/

2.5 With the RGD's growing reliance on IT, information security must be a high priority and policies must be established to reduce the risk of unauthorised access, exposure or loss of data processed by its IT systems. Although RGD had developed security policies for its network and servers, ***it did not establish an enterprise ISP*** that took into account its current 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.

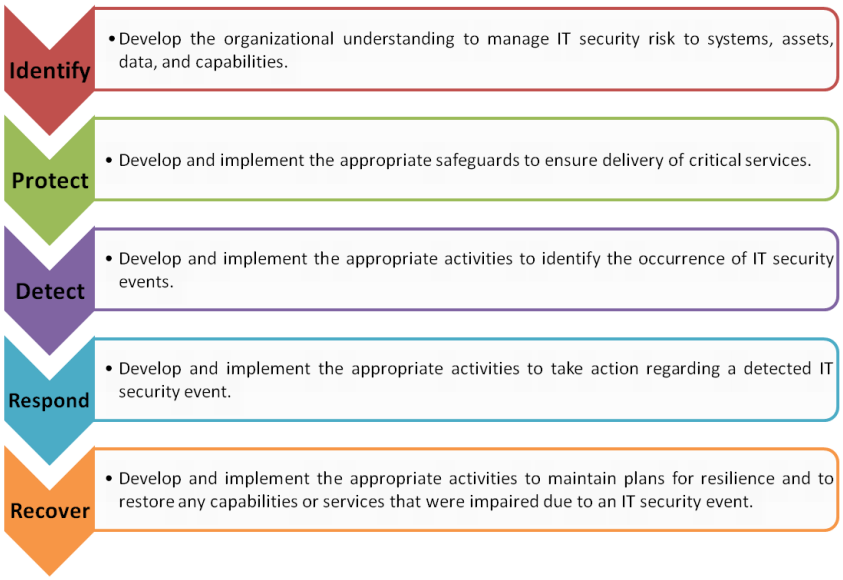
2.6 The absence of a comprehensive and up to date approved ISP increases the RGD's vulnerability to information security threats and reduces its capacity to protect its IT assets/resources and safeguard the information contained within its IT systems. Furthermore, there is an increased risk that IT security controls and procedures may be inconsistent and ineffective leading to a weakened IT control system, unauthorised access, exposure or loss of data processed by the RGD's IT systems.

2.7 The RGD subsequently indicated that a *draft ISP* has since been created in collaboration with an IT consultant from the *National Identification Project*. We were advised that the document is currently under review and will be submitted for approval, however, no timeline was provided.

Inadequate IT Security Management Function

2.8 An effective security management function is necessary to implement information security related policies and plans and for implementing the various IT security related processes such as access controls and network security. It requires coordinated and integrated action from top down.

Figure 3: IT Security Functions



Source: National Institute of Standards and Technology (NIST)

2.9 Despite acknowledging in its Strategic Business Plan, the need to develop and implement an IT security mechanism and appoint an IT Security Manager, ***RGD did not establish an IT security management function to ensure that there was a consistent and co-ordinated approach to IT security across the organization.*** While members of the IT department performed some IT security related functions, the IT security roles and responsibilities were not clearly defined, in particular the roles and responsibilities of management, users and IT personnel. This increases the risk of security vulnerabilities remaining undetected and reduces the RGD'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 RGD.

2.10 The RGD subsequently indicated that the Information Systems Manager currently performs the tasks for managing IT security, however, because it is a "*fulltime activity*" the Agency is "considering the creation of a new position to perform these duties". The Agency further advised that our recommendation will be taken into consideration when creating the Job Description for the new position.

Inadequate IT Personnel Clearance Procedures

2.11 Background checks in the IT recruitment process is a key control in the general IT control environment and if applied consistently will lead to an overall strengthening of an

organization's IT security management. Background checks should be conducted for employees, contractors and vendors in keeping with the sensitivity and critical nature of their functions.

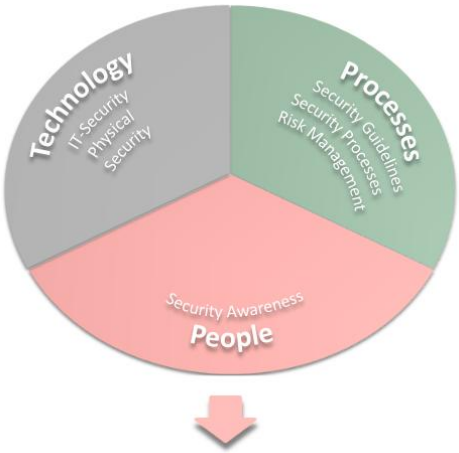
2.12 ***We found that the RGD did not establish a system for conducting mandatory background checks on its current/potential IT employees in order to verify their credentials, employment history or to determine whether these persons pose a possible security risk***. The RGD's policy is to screen successful applicants to confirm the validity of the information provided. However, the process lacked consistency and seemed to have been applied arbitrarily. For example, of the nine IT employee files reviewed, only two contained evidence of reference checks and there was no evidence that they were subjected to any form of criminal background checks. The absence of consistent and comprehensive background checks in the IT recruitment process increases the risk that the RGD may employ persons who pose a possible IT security threat, resulting in a compromise of its IT security.

2.13 The Agency indicated that "background checks were not necessary for most of the IT staff since they were promoted from within the Agency", however, the recommendations "will be taken into consideration when reviewing the policies of the HR Department".

Inadequate IT Security Training and Sensitization for End-users

2.14 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.

Figure 4: IT Security Awareness



Source: http://wmc-direkt.de/en/consulting/awareness/

2.15 Despite its increasing reliance on IT, the ***RGD did not establish a programme for creating user awareness and training to sensitize end-users about IT security***. The absence of a

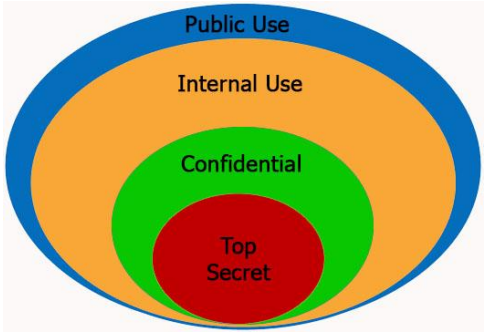
security awareness training and sensitization programme increases the RGD's vulnerability to IT security threats and may result in a breakdown of the Agency's IT control system.

2.16 RGD indicated that its IT staff was exposed to periodic training and other capacity building exercises, however, further efforts will be made to ensure that IT personnel and end users are sufficiently trained in IT security.

Absence of a Data Classification System

2.17 Effective data protection and security requires the establishment a data classification scheme that applies throughout the entire organisation, based on the level of importance and sensitivity of the Agency's data. This scheme should include details about data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements, importance and sensitivity. The data classification scheme should be used as the basis for applying controls such as access controls, archiving or encryption.

Figure 5: Data Classification



Source: http://www.latestnews.sg/the-ultimate-guide-to-setting-up-a-reliable-data-classification-scheme/

2.18 Although the RGD is responsible for the safe custody of certain vital records including birth, death and marriage records, ***it did not develop a data classification system in order to establish appropriate baseline security controls for the protection of its data***. Consequently, the RGD is more vulnerable to information security threats because certain IT security controls may not be appropriate for the level of sensitivity of the data being protected. The absence of a data classification scheme may also lead to inconsistent information for decision-making.

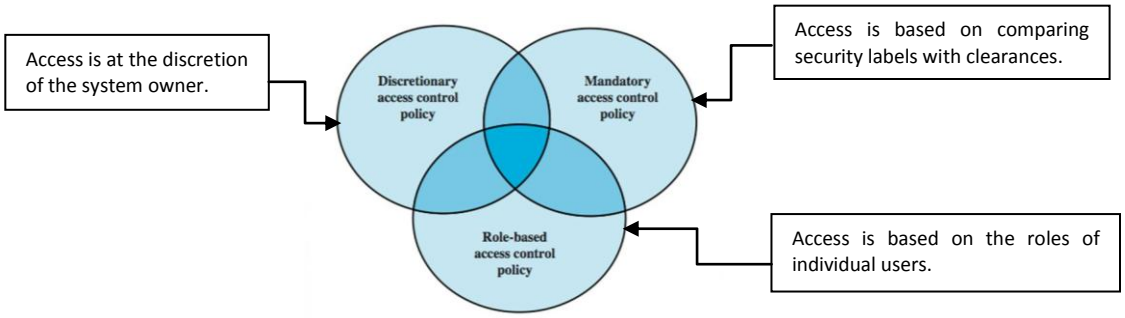
2.19 The Agency indicated their agreement with the finding and advised that the recommendation will be implemented. Additionally, we were informed that "a draft policy has been created and is currently under review".

Access Control Policy

2.20 Access controls provide the first line of defence against unauthorized users. Access control policies should be based on the established levels of data sensitivity and used as a basis for access control decisions and user privileges based on employee job roles and functions.

We found that the RGD did not have an approved comprehensive access control policy in place to manage access to its IT resources and to ensure appropriate preservation of data confidentiality, integrity and availability. This increased the RGD's vulnerability to security breaches.

Figure 6: Access Control Policies



Source: http://slideplayer.com

2.21 The Agency indicated their agreement with the finding and advised that the recommendation will be implemented. Additionally, we were informed that "a draft policy has been created and is currently under review".

Inadequate Controls over Administrator Accounts and Activities

2.22 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. ***The RGD 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 was an increased risk of unauthorized changes to the RGD's IT security profiles and access control parameters going undetected.

2.23 The RGD indicated their agreement with the finding and advised that the recommendation will be implemented. The Agency further advised that its "IT department is currently reviewing *administrator* access" to its systems and changes have since been made to its policy to "ensure that administrator rights are reserved with the necessary controls in place when used".

Inadequate Environmental Controls in RGD's Server Room

2.24 Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel. The environment has several key control elements including, temperature and humidity controls, power supply controls, working space controls, fire protection systems, and physical security systems. All computer equipment operates under potentially unstable environmental conditions and therefore, appropriate and effective controls that monitor and prevent damage caused by environmental factors should exist to reduce the risk of loss and downtime.

2.25 **We found that the safety of the Agency's server room might be compromised due to the absence of appropriate equipment to monitor the room's environmental condition such as its temperature and humidity.** The server room was also not equipped with a smoke detector to provide an alert in the event of a fire. This increased the risk of damage to the RGD's most critical computer equipment resulting in the possible loss of vital records and disruption in operations. The RGD indicated their agreement with the finding and advised that the recommendation will be implemented.

Inadequate Oversight of RGD's ICT Operations

Absence of an IT Oversight Committee

2.26 RGD's heavy reliance on IT to achieve its mandate requires the establishment of 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.

2.27 Despite its increasing reliance on technology, the ***RGD did not have an appropriate oversight committee that provided advice to those charged with governance*** on areas such as the alignment of IT with the RGD's business 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 RGD's business goals and not all relevant stakeholders were involved in the IT decision-making process. In response, the RGD indicated that it will "make every effort to establish such a committee".

Independent Review of IT Controls

2.28 RGD needs to evaluate its IT control environment as part of its overall controls and IT governance review in order to provide independent advice to management on the efficiency and effectiveness of its overall IT control system.

2.29 ***We found no evidence to indicate that the RGD had established any mechanism, such as periodic internal IT audits, to evaluate its IT controls on a regular basis to determine their effectiveness or efficiency***. Consequently, one of the most significant aspects of the RGD's operations was not subjected to regular, independent reviews to ensure that management was aware of weaknesses or 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 help to ensure compliance with IT control procedures that have been implemented within the organization.

2.30 The Agency has since indicated that "the internal audit department is currently undergoing training to improve their competencies to perform in depth audits of the IT department".

PART THREE

Jamaica Urban Transit Company (JUTC)

Background

3.1 The JUTC is a wholly owned company of the Government of Jamaica and was incorporated on July 13, 1998 with the mandate to provide a safe, reliable, modern, professional, efficient, and cost effective transportation service to the Kingston Metropolitan Transport Region (KMTR). The JUTC currently holds the exclusive licence to provide public passenger transportation service in the KMTR. It provides two general types of transportation services, namely: *Regular Service*, which includes normal (adult) and concessionary passengers; and *Premium Service*, which also includes express. Both types of services have a flat fare structure, which means that the fare charged for the services is independent of the distance travelled.

3.2 One of the JUTC's key strategic objectives is to increase and improve the use of technology in its operations. The aim is to facilitate the improved provision of real-time information in relation to its service and operations, and allow for improved all-round efficiency especially in decision-making and service delivery. In keeping with this objective, the JUTC introduced an Electronic Fare Collection System in 2002 utilizing a prepaid card in an effort to improve the passenger entry, accountability and revenue collection. The system was upgraded in the 2013/2014 financial year and currently it is the only method of payment accepted from concession passengers.

3.3 Given the JUTC's increased reliance on technology in its operations, especially in the collection and accounting for revenue, there is a need to safeguard the confidentiality, integrity and availability of information from IT threats, taking into account the various security related vulnerabilities. This will require establishing and maintaining IT security roles and responsibilities, policies, standards and procedures.

Absence of an Information Security Policy

3.4 An Information Security Policy (ISP) is a formal statement that defines management's intentions on information security and provides general direction for protecting the confidentiality, integrity and availability of information. The policy should set out the organization's approach to managing its information security objectives. The ISP should be communicated to all employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader.

3.5 With the JUTC's growing reliance on the Electronic Fare Collection System, information security must be a high priority and policies must be established to reduce the risk of unauthorised access, exposure or loss of data processed by the system. However, the ***JUTC did not establish an ISP*** that took into account its current IT environment, strategies and

risks, the response mechanism for dealing with security breaches especially those relating to cyber-security, the assignment of general and specific responsibilities for information security management and the impact of relevant legislation such as the Cybercrimes Act. The absence of an ISP increases the JUTC's vulnerability to information security threats and reduces its capacity to protect its IT assets and safeguard the information contained within its IT systems. Furthermore, there is an increased risk that IT security controls and procedures may be inconsistent and ineffective leading to a weakened IT control system.

3.6 The JUTC indicated that there are broad security measures in place to protect its IT assets, however, the company acknowledged the absence of a formal ISP and stated their intention to formulate one in the shortest possible time.

Inadequate IT Security Management (ITSM) Function

3.7 An effective ITSM function is necessary to implement IT security related policies and plans and for implementing the various IT security related processes such as access controls and network security. It requires coordinated and integrated action from top down.

3.8 The ***JUTC did not establish an ITSM function to ensure that there was a consistent and co-ordinated approach to IT security across the organization***. The company 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 pro-active manner across the company. While members of the IT department performed some IT security related functions, the IT security roles and responsibilities were not clearly defined, in particular the roles and responsibilities of management, users and IT personnel. This increases the risk of security vulnerabilities remaining undetected and reduces the JUTC'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 JUTC.

3.9 The JUTC has since advised us that the IT security function will be taken into consideration when the formal IT security policy is developed.

Inadequate Personnel Clearance Procedures

3.10 Background checks in the IT recruitment process is a key control in the general IT control environment and if applied consistently will lead to an overall strengthening of the JUTC's IT security management. Background checks should be conducted for employees, contractors and vendors in keeping with the sensitivity and critical nature of their functions. ***The JUTC did not establish a system for conducting background checks on its current/potential employees in order to verify their credentials, employment history or to determine whether these persons pose a possible IT security risk***. There was no documented background check policy and potential employees were not subjected to any form of criminal background checks. Furthermore, with the exception of the IT Manager, IT personnel were not required to sign a confidentiality or non–disclosure agreement.

3.11 The absence of consistent and comprehensive background checks in the IT recruitment process increases the likelihood that the JUTC may employ individuals who pose a potential IT security risk, leading to a possible compromise of its IT security. The company's IT control system is further weakened by the lack of a confidentiality or non–disclosure agreement for all IT personnel.

3.12 The JUTC has since indicated that a background check policy will be drafted and submitted to its Board for approval and steps have already been taken to ensure that members of its IT department sign a non-disclosure agreement.

Inadequate IT Security Training and Sensitization for End-users

3.13 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 increasing reliance on IT, the JUTC did not establish a programme for creating user awareness and training to sensitize end-users about IT security.*** Additionally, we saw no evidence of any specific IT staff development and training programme to address the needs of the JUTC's IT staff. The absence of a security awareness training and sensitization programme increases the JUTC's vulnerability to IT security risks and may result in a breakdown of the company's IT control system.

3.14 The JUTC accepted that there is room for improvement in its sensitization methods and indicated that it will introduce more formal IT security sensitization measures going forward. Additionally, the company's *"new IT Manager has been tasked with formulating a training plan and identifying relevant courses"* for all IT personnel.

Access Control Policy

3.15 Access controls provide the first line of defence against unauthorized users. Access control policies should be based on the established levels of data sensitivity and used as a basis for access control decisions and user privileges based on employee job roles and functions.

3.16 The ***JUTC did not have an approved comprehensive access control policy in place to manage access to all of the company's IT resources and to ensure appropriate preservation of data confidentiality, integrity and availability***. The JUTC had developed a *"Computer, Network & Internet Acceptable Usage Policy"* that provided guidance on areas such as the use of electronic mail and the internet, passwords and general access to computer resources. However, the document did not address other critical areas such as user access management, network access, remote access and access to the various applications in use at the JUTC. Furthermore, the "Computer, Network & Internet Acceptable Usage Policy" may also be out-dated having not been updated since 2004. The absence of an approved comprehensive access control policy increases the JUTC's vulnerability to security breaches.

3.17 The JUTC indicated that despite the absence of a formal policy it is the "*operating practice for user access and privileges to be granted solely on a request from the Human Resources Department and in conjunction with the employees' job description and assigned location"*. Nevertheless, the company indicated that steps will be taken to develop an Access Control Policy to strengthen its current operating practices.

Inadequate Monitoring of Access Logs

3.18 Logs are generally used to record user activities, exceptions, faults and information security events on a network or application. The maintenance of access logs is essential for ensuring that network users are accountable for their actions on the network. ***The JUTC did not have a system in place to ensure that its access and related logs were reviewed periodically to identify unusual or suspicious activities***. A review of the JUTC's system logs revealed 367 cases of unsuccessful log-on attempts, however, there was no evidence that these incidences were investigated to determine their cause or impact on the JUTC's network. The JUTC's failure to systematically monitor and review its access logs increases the risk of unauthorized access and other IT security breaches going undetected.

3.19 The JUTC indicated that *"unsuccessful log on attempts usually occur when users forget their password, the password expires before being reset or an employee returns from vacation and an inactive password does not work"*. The company, however, stated that they are putting a process in place to review the logs periodically.

Inadequate Controls over Administrator Accounts and Activities

3.20 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 JUTC 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 JUTC's IT security profiles and access control parameters going undetected.

3.21 The company indicated that steps will be taken to improve the monitoring of these accounts.

IT Risk Assessment

3.22 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.

Figure 7: IT Risk Assessment Process

Source: http://www.preventbd.com/crisis-management-risk-assessment

3.23 Though JUTC has increased its reliance on technology, ***it did not complete the development 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***. A draft risk assessment was started in 2015, however, the document has not been finalized and approved by the JUTC's management. The JUTC therefore, has an increased risk exposure and may not be able to respond appropriately in the event of a threat affecting its IT environment.

3.24 The JUTC has since indicated that "*this shortcoming was identified by the Audit and Risk Assessment Committee of the Board in 2017*". The Committee subsequently mandated the establishment of an internal Executive Risk Management Committee to among other things complete the draft IT risk assessment. Additionally, the JUTC has committed to ensuring that going forward it has an approved risk register and each Division Head is expected to re-assess risks in their unit accordingly.