INFORMATION SYSTEMS REVIEW
OF THE
TRANSPORT AUTHORITY

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

April 2012

TABLE OF CONTENTS

AUDITOR GENERAL'S OVERVIEW

In recognition of the growing importance of information technology to the operations of the Transport Authority and in keeping with my constitutional mandate, I commissioned an information systems audit of the Authority to determine whether adequate systems, policies and procedures were in place to enable a credible, efficient and effective level of service to its customers.

The audit involved a review of the Authority's general computer controls, systems and procedures as well as application controls relating to its Licence Management Information System (LMIS). We assessed the effectiveness of the Authority's control environment and its impact on the level of service delivery.

The mandate of the Transport Authority is to regulate and monitor public passenger and commercial transport throughout the island of Jamaica. This is achieved through, among other activities, the licensing of all public passenger and commercial vehicles operating in the island and the screening of drivers of public passenger vehicles by way of a badge identification system.

The Authority collaborated with Fiscal Services Limited (FSL) to develop and implement a Licence Management Information System (LMIS) to manage and improve its licence production and distribution processes. It has also sought to increase the use of technology in its administrative and operational functions. However, the Authority has not concurrently implemented certain key IT and other controls to reduce its significant IT related risks.

Our review revealed significant weaknesses in the areas of physical and information system security, environmental security, badge processing, cash management, management of seized vehicles and business continuity planning. These deficiencies, if left unresolved could severely compromise the Authority's ability to achieve its mandate. The Authority's physical and information system security is of particular concern to us because previous audits have identified related weaknesses but very little improvement has taken place in relation to the underlying controls.

It is therefore crucial that the management of the Transport Authority 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 the Transport Authority for the courtesies extended to my staff during the audit.

Pamela Monroe Ellis, FCCA, FCA, CISA
Auditor General

EXECUTIVE SUMMARY

The Transport Authority is the agency charged with the responsibility for the licensing of all public passenger and commercial vehicles and the regulating and monitoring of public transportation in Jamaica. The Authority was established in 1987 as a statutory body and it is governed by its principal Act, the Transport Authority Act. At the time of the audit, the Authority operated under the Ministry of Transport, Works and Housing and had a net asset base of $314M and an operating surplus of $175M as at March 31, 2011. The Authority's records also show a total of 47,748 "active" road licences covering both public passenger and commercial carrier vehicles.

The principal objective of the Transport Authority is to regulate and monitor public transportation in the urban areas of the Kingston Metropolitan Transport Region (KMTR), Montego Bay Metropolitan Transport Region (MMR) and all other urban and rural routes and areas in the island of Jamaica. One of the key activities used to achieve this objective is the licensing of all public passenger vehicles and commercial carriers island-wide.

The Authority has taken steps to automate its entire licensing process by developing a Licence Management Information System (LMIS) to improve the efficiency of the licence application, processing and delivery procedures. It has also sought to increase the use of technology in both its administrative and field operations by, for example, increasing the use of electronic surveillance in its monitoring and enforcement activities.

It is therefore critical that the Authority implement a strong control environment especially as it relates to its Information Technology resources to ensure that its systems are not compromised.

Our audit focused on assessing the efficiency and effectiveness of the Transport Authority's general computer controls as well as the application controls relevant to its Licence Management Information System (LMIS) to determine whether systems, policies and procedures are in place to preserve the integrity and confidentiality of data/information, the achievement of its business objectives and the safeguarding of its assets. Other medium-high risk areas that are not directly related to the Authority's computer environment were also reviewed and the findings are included in this report.

The audit did not include any network penetration testing and physical inspections were limited to the Authority's Head Office and its Operations Division. Our assessment was based on the review of internal and external documents, analysis of the LMIS and related data, observations of processes and procedures and interviews with senior officers and staff of the Transport Authority.

KEY FINDINGS

CASH MANAGEMENT

1. **The LMIS has failed to enforce certain critical business rules relating to the management and control of revenue**. Even-though Cashiers are required to record the cash in hand at the end of each day, the LMIS does not enforce this rule. Instead, reconciliations are done manually, resulting in the LMIS displaying numerous instances of variances between the system generated totals and the amount of money each Cashier has in hand even-though these amounts may have been reconciled manually. This affects management's ability to efficiently track all collections because time is spent reviewing both computerized and manual records as opposed to utilizing all the features of the LMIS to conduct their review and reconciliation.

BADGE PROCESSING

2. **There is no direct inter-connectivity or interface between the Authority's badge processing system, the LMIS and the Jamaican Driver's Licence System (DLS).** This increases the risk that badges may be printed for individuals who have not submitted a legitimate application. This also limits the Authority's ability to determine the legitimacy of an applicant's driver's licence, consequently, increasing the risk of individuals submitting fraudulent licences with their applications.

3. **We found that the controls over the badge production process were inadequate** as there is no system in place to ensure that all printed badges are routinely compared with the relevant applications to ensure that both sets of information are consistent or that there is a legitimate application for each badge printed. Furthermore, the system does not maintain a record of the badges printed, reprinted or spoiled. This weakens management's ability to effectively control and monitor the badge production process and increases the risk of badges being printed without a legitimate application.

   The management of the Authority advised us that steps are being taken to upgrade the LMIS to address the weaknesses identified with its current badge processing system.

ACCESS CONTROLS & NETWORK SECURITY

4. **There was a breakdown in the monitoring and control systems in relation to the Authority's physical security environment** as there was no designated official responsible for ensuring that the Authority's access cards are activated and deactivated in a timely manner. Additionally, no formal record of communication between IT and HR concerning authorization for activation and deactivation is maintained. Consequently, we found that access cards for 26 former employees were not deactivated and could therefore still be used to access the Authority's premises. A total of 16 access cards were found in the possession of the acting Systems Administrator even-though the physical cards are not required for deactivation and of this amount, seven were still active and **two were last used subsequent to the respective employee's departure from the Authority.** Subsequent checks revealed that all active cards for former employees have either been de-activated or re-assigned and are no longer in the possession of the Systems Administrator.

5. **There were inherent weaknesses in the Authority's access control software**, for example, the system does not permit the *"card enrolment date"* to be updated where an access card is reassigned to another employee. Therefore, where a card has been reassigned, the system will not record the date of the reassignment, only the date of the original assignment. The system also does not record the date the card status changed from "*ON*" to "*OFF*" or vice-versa. **We identified 10 cases where employees with an assigned access card had *"enrolment dates"* which were prior to their dates of employment.** The Authority has since advised us that steps will be taken to replace its current access control system with an enterprise system that will be installed at all its locations.

6. **We found that the monitoring of the Authority's network and related activities was inadequate and could expose the entity to an increased risk of network attack or sabotage.** Currently, the Authority does not have a system in place to monitor the activities of privileged users and administrators to ensure that they are not abusing or misusing their access rights. Other activities such as network monitoring, firewall activity review and review of user accounts were not conducted in accordance with a specified schedule but were performed on an ad hoc basis and the results of the reviews were not normally documented. **This led to the network user accounts of 16 former employees remaining active up to three years after separation and of that amount, five employees' accounts had logon activities on the network subsequent to their date of termination**. **Additionally, nine former employees had an active user status on the LMIS**. The Authority's failure to deactivate the accounts of former employees in a timely manner increases the risk of unauthorised access to its systems and data, including confidential or sensitive customer information. Subsequent checks revealed that these active user accounts have now been de-activated.

   The management of the Authority has since advised us that they intend to strengthen the controls over its network activities.

LMIS USER GROUPS

7. **There was a breakdown in the controls relating to segregation of duties**, as there were at least 87 officers who were assigned to multiple *User Groups* within the LMIS that may not be consistent with their regular job functions. For example, we identified seven officers who were assigned to both the *Accounts* and the *Accounts Supervisors* Group and one officer to both the *Cashier* and the *Supervisors* Group thus creating the possibility for these persons to authorize or override their own transactions. This may also cause errors or irregularities to go undetected.

8. **Some members of staff had excessive user privileges** such as members of the Information Technology (IT) division who were assigned to numerous operational user groups contrary to the principles of good business practices and control. This undermines the Authority's internal control mechanism because these users have privileged access and can manipulate the organisation's computer systems. This is even more critical because the activities of privileged users are not monitored or reviewed.

   The Authority has since taken steps to reduce the number of groups privileged users are assigned to.

ENVIRONMENTAL SECURITY

9. **Our audit revealed weaknesses in the controls relating to the Authority's server room, emergency alarm system, fire prevention and detection mechanism and its back-up power supply.** There is currently no smoke detector, automatic fire alarm or other fire suppression system except fire extinguishers installed at the Transport Authority thus increasing the risk of major damage and disruption in the event of a fire. We also identified a defect in the emergency alarm system that could be used to circumvent the use of the access cards for entry to the Authority's premises. The management of the Authority has since advised us that they intend to address the environmental security weaknesses identified.

BUSINESS CONTINUITY MANAGEMENT

10. **The Transport Authority does not have a formal system in place to conduct periodic testing of its disaster recovery plans to ensure that the procedures remain relevant and effective in the event of a disaster**. There is also no formal procedure to ensure that back-up media for the LMIS and its other systems are regularly tested to determine the integrity and completeness of the back-up files. This may lead to complications and delays in the event of an unplanned disruption especially if backup media are corrupted or other circumstances have changed subsequent to the last review of the plan.

MULTIPLE LEGAL CLAIMS

11. **The acts or omissions of the Authority's agents have resulted in an excessive number of claims primarily for damages relating to unlawful seizure and detention of motor vehicles.** Up to December 2011, the Authority had paid out approximately $18M covering both legal fees and settlements relating primarily to claims brought against it by motorists. At the time of the audit, the Authority's records revealed that there were a further 58 "active" cases of legal claims brought against it. In one instance, a vehicle was seized and subsequently ordered to be released by the police but was eventually sold at auction by the Transport Authority. The Supreme Court ruled in favour of the Claimant and to date a total of $9.1M has been paid to him. Furthermore, the Authority has estimated that if the remaining claims were to be successful, the potential damages and costs could be approximately $13.8M.

    While the Authority has strengthened its legal department to deal with court matters and other legal proceedings, there is no evidence that a comprehensive strategy exists to target the incidences of unlawful seizures and detention of motor vehicles by its Inspectors, in order to reduce the risk of further increase in such claims.

    The Authority has since advised us that a review of the seizure process has been implemented with a view to mitigating the risk of unlawful seizures.

GOVERNANCE & HUMAN RESOURCE MANAGEMENT

12. **Our review identified weaknesses in the composition and functions of the Authority's Audit Committee as well as inadequacies surrounding the appointment process and policy oversight of the previous Board.** This resulted in the implementation of at least nine significant policy documents without any formal Board review or approval.

13. **The Authority's staff complement of 292 employees was not approved by the Cabinet Office or the Ministry of Finance**. Staff costs including salaries and allowances for the financial year ended March 31, 2011 was $446.6M (2010: $404.1M) representing 69% (2010: 69%) of operating expenses.

14. **We found that the Transport Authority operates a number of employee benefits facilities such as staff loans but these have not been approved by the Ministry of Finance.** Staff loans, as at March 31, 2011 was $4.2M (2010: $2.5M), an increase of 66% over the previous year.

15. **There were weaknesses in the Authority's personnel clearance procedures**, for example, the Authority does not routinely verify the authenticity of the certificates of qualifications received from current or prospective employees. It is therefore unable to independently determine whether these persons have satisfied the Authority's qualification criteria.

    The management of the Authority has promised to address the above weaknesses.

RECOMMENDATIONS

1. The management of the Authority should ensure that the LMIS enforce all business rules relating to collecting and accounting for revenue; including forcing a reconciliation of amounts on hand with the system-generated receipts and making a supervisor confirmation of the amounts held on hand by the Cashier mandatory within the LMIS. The Authority should also investigate the variances identified to determine if any irregularities exist.

2. The Authority should investigate all cases of unusually long active cashier sessions to determine the reason(s) for such a prolonged active status for each user. Additional safeguards should also be implemented to prevent a recurrence of these breaches.

3. The Authority should ensure that the current badge processing module being developed within the LMIS can interface directly with the Driver's Licence System in order to confirm the validity of an applicant's driver's licence. Systems should also be developed to ensure that management is able to exercise effective control over the badge production process and reduce the risk of badges being printed without the necessary supporting documents.

4. We also recommend that appropriate systems and procedures be implemented to ensure that the activities of privileged users and administrators and network activities including firewall activities are monitored and reviewed on a timely basis. The Authority should also ensure that a system is in place to deactivate all former employees' physical and logical access rights in a timely manner.

5. The Authority should immediately review the composition of each User Group to determine whether the respective members need access to the resources of those groups. The practice of assigning individuals to supervisory and non-supervisory groups at the same time should be discontinued and members of the IT division should not have any operational privileges that may undermine the Authority's internal controls.

6. The Authority should develop and adopt a comprehensive Environmental Security Policy that define standards for all its facilities, covering site selection and construction, personnel health and safety, mechanical and electrical systems, and protection against environmental factors such as fire and flood so as to reduce the risk of loss or damage to the Authority's assets. It should also ensure that systems and procedures are implemented to address the specific environmental control weaknesses outlined in this report.

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

8. The Authority should develop a specific set of strategies in collaboration with the Ministry of Transport, Jamaica Constabulary Force (JCF), the Island Special Constabulary Force (ISCF) and

the Island Traffic Authority (ITA) aimed at reducing the incidences and the risk of unlawful seizures and detention of motor vehicles in order to reduce future liabilities.

9. Seized vehicles that are held for an inordinately long period increase the risk that disposal by way of sale will be uneconomical due to their decline in value and associated storage and disposal costs. The Authority should therefore ensure that an efficient system is in place to track all vehicles seized and to activate the disposal process for such vehicles that have been held for six months as outlined in the Transport Authority Act. Additionally, all proceeds from the sale of seized vehicles should be paid over to the Accountant General in accordance with section 13 (3A) of the Act.

10. The Board is accountable for the development of the Authority's operational policies and we therefore recommend that appropriate steps be taken to ensure that all such policies and procedures are brought to the attention of the Board for review and ratification. The Authority should ensure that an appropriate system is implemented to facilitate Board review of new or amended policies/procedures before they are adopted.

11. The existence of an Audit Committee contributes to good corporate governance, being an independent instrument of control and review. In order to remove or reduce any real or perceived lack of objectivity/independence, we recommend that the mandate of the Authority's Audit Committee be consistent with the provisions of Section 9 of the PBMA Act. This section provides general guidelines on the duties of Audit Committees within public bodies and it will assist the Committee to maintain the desired level of independence and objectivity.

12. The management of the Authority should seek the assistance of the Cabinet Office or the Ministry of Finance to immediately regularize their unapproved organisation structure and employee benefit schemes.

13. The management of the Transport Authority should ensure that a system is place to routinely verify the academic and other credentials of current or prospective employees to guard against persons with fictitious certifications. It should also strengthen its existing mechanism to ensure that all employees submit a Police Record as required and sign a copy of the Official Secrets Act Declaration in order to help preserve the confidentiality and integrity of certain aspects of the organisation's operations.

PART ONE INTRODUCTION

Audit Scope and Methodology

1.1 In recognition of the growing importance of information technology to the operations of the Transport Authority and in keeping with my constitutional mandate, I commissioned an information systems audit of the Authority to determine whether adequate systems, policies and procedures were in place to enable a credible, efficient and effective level of service to its customers.

1.2 The audit involved a review of the Authority's general computer controls, systems and procedures as well as application controls relating to its Licence Management Information System (LMIS). We assessed the effectiveness of the Authority's control environment and its impact on the level of service delivery.

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

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

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

1.4 Information systems controls involve specific activities performed by people (manual) or by systems (automatic) to ensure the confidentiality and integrity of data as well as the continuity of Information and Communication Technology systems. These controls can be divided into two broad categories: application controls and general controls. Application controls apply to specific software programs or "Applications". These Applications or Programs are used to facilitate key business processes within an organization, e.g. Payroll

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

and Accounts are typical processes that are dependent on software applications. Application controls are designed to ensure the complete and accurate processing of data from input to output. They ensure that only authorized data is accepted and that output is reliable. On the other hand general computer controls apply to computing systems as a whole. These comprise the processing environment including management of computer resources, file access, change control, contingency planning and backup.

1.5 Weak general controls could cause application controls to be ineffective because application controls are dependent on general controls. Strong general computer controls constitute a prerequisite for the establishment of a reliable information systems environment that effectively supports the objectives of an organisation.

1.6 Our audit focused on assessing the efficiency and effectiveness of the Transport Authority's general computer controls as well as the application controls relevant to its Licence Management Information System (LMIS) to determine whether systems, policies and procedures are in place to preserve the integrity and confidentiality of data/information, the achievement of its business objectives and the safeguarding of its assets. This involved the review and testing of controls in the following areas:

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

1.7 We also applied various data analysis techniques to test the accuracy, completeness and integrity of the data within the LMIS.

1.8 The planning process involved gaining a thorough understanding of the mandate, role and functions of the Transport Authority and the nature and extent of the use of Information and Communication Technology in its operations. This information allowed us to formulate a risk based approach in determining the specific areas to be targeted for review.

1.9 The audit did not include any network penetration testing. Additionally, physical inspections were limited to the Authority's Head Office at 119 Maxfield Avenue, Kingston 10 and its Operations Division located at 107 Maxfield Avenue, Kingston 10. Our assessment was based on the review of internal and external documents, analysis of the LMIS and related data, observations of processes and procedures and interviews with senior officers and staff of the Transport Authority.

Background

1.10 The Transport Authority was established in 1987 as a corporate body under Section 3(1) of the Transport Authority Act 1987 to monitor and regulate public passenger and commercial transport throughout the island of Jamaica. Under the Act, the Authority assumed the functions formerly performed by:

- Licensing Authorities or specially constituted Licensing Authorities under the Road Traffic Act;
- Public Passenger Transport (Corporate Area) Board of Control constituted under the Public Passenger Transport (Corporate Area) Act; and
- Public Passenger Transport (Rural Area) Board of Control constituted under the Public Passenger Transport (Rural Area) Act

1.11 The Authority currently operates under the Ministry of Transport, Works and Housing and its operations are regulated by:

- The Transport Authority Act
- The Road Traffic Act
- The Public Passenger Transport Regulations and Acts (Rural & Corporate Area)
- The Public Bodies Management and Accountability Act

1.12 The principal objective of the Transport Authority is to regulate and monitor public transportation in the urban areas of the Kingston Metropolitan Transport Region (KMTR), Montego Bay Metropolitan Transport Region (MMR) and all other urban and rural routes and areas in the island of Jamaica. These activities include:

- Licensing of all public passenger vehicles and commercial carriers island-wide;
- Maintaining a transport register;
- Conducting technical surveys for granting licences and determining routes;
- Scheduling of routes and preparing timetables; and
- Investigation of complaints

1.13 The mandate of the Authority is implemented through its Kingston Head Office (KRO) and three regional offices;

- Western Regional Office (WRO);
- North East Regional Office (NRO); and
- Southern Regional Office (SRO)

1.14 In 2004 the Authority collaborated with Fiscal Services Limited (FSL) to develop and implement a Licence Management Information System (LMIS) with the aim of[5]:

a. Reducing the time spent by taxpayers applying for road licenses in the offices of the Transport Authority and, in travelling between that organization and the Jamaica Tax Collectorates in order to secure road licenses and commercial carrier and public passenger plates;

b. Expediting the licence processing and delivery time;

c. Improving data integrity and consistency within and between the motor vehicle data maintained by the Jamaica Tax Collectorates in the Automated Motor Vehicle System (AMVS) and that of the LMIS;

d. Improved operational efficiencies and controls in the processing of road licence applications and the accounting for fees collected, through:

- Automated interfaces with the TRN[6], AMVS and TCC[7] systems to validate documents presented by applicants;
- Automated interface with the Authority's general accounting system for the posting of charges relating to fees collected;
- Automated interface and controls between the "Cashiering" and the "Licence Printing" modules of the system.

1.15 In 2008, the online payment and application submission module (LMIS Online) was implemented. Through this facility, applicants for Commercial Carrier (CC) licences are able to submit applications and make related payments via the Internet.

1.16 The Transport Authority disclosed that it costs the entity approximately $600,000 per annum to maintain the LMIS.

1.17 At the time of the audit, data from the LMIS revealed that there were approximately 47,748 "active" road licences covering both public passenger and commercial carrier vehicles as shown in **Table 1.** Of this amount, 25,811 or 54% were carrier licences and 21,937 or 46% were public passenger licences.

[5] http://www.fsl.org.jm/systems/licensing-management-information-system

[6] Taxpayer Registration Number

[7] Tax Compliance Certificate

Table 1: No. of “active” Licences by Licence Type

Licence Type	No. of Licences
Private Carrier	19,517
Public Carrier	6,294
Route Taxi (KMTR)	262
Route Taxi (Rural Taxi)	13,217
Rural Stage Carriage	3,052
JUTC Stage Carriage	94
Hackney Carriage (Metered)	1,594
Hackney Carriage (Un-Metered)	19
Contract Carriage (Car)	1,029
Contract Carriage (Bus)	2,660
Express Carriage	10
Total	**47,748**

Source: LMIS

PART TWO Cash Management

Unusually Long Active Cashier Sessions

2.1 A cashier station, if being used by a cashier, should be rendered useless to any other Cashier unless the previous Cashier terminates their session. Each day that a Cashier logs in, the LMIS automatically makes a log in the database. At the end of each day, the Cashier is required to execute the Cashier End of Day Procedure. This involves the Cashier specifying the total collections at the end of each day which should reconcile with the system totals.

If the Cashier does not perform the end of day routine, the Cashier should be forced, upon logging on to the system the next day, to execute the end of day procedure. In addition, another Cashier should not be able to access the workstation unless the previous Cashier executes the End of Day process.

2.2 A review of the Cashier Session table in the LMIS revealed that there were eight active Cashier sessions that have been initiated for an inordinately long period contrary to the Authority's operational procedures (**Table 2).** This may also indicate a system weakness because all Cashiers should be forced to log out at the end of each day and prevented from using the system the following day if they have not.

Table 2: Long Active Cashier Sessions

Session Date	Station No.
02/08/2005	77
04/13/2011	197
05/16/2011	196
05/30/2011	192
08/10/2011	61
09/01/2004	62
09/03/2011	79
09/17/2010	109

Source: LMIS

2.3 We advised the Authority to investigate these cases to determine the reason(s) for such a prolonged active status for each user. The Authority has since requested FSL's assistance in launching an investigation into this matter.

Lodgement Variances

2.4 The lodgement table in the LMIS keeps an audit trail of all collections made by each Cashier. It records and displays the amount of money that each Cashier should have based on computer-generated totals of payments accepted by the system. In conducting the End of Day procedure, each Cashier should enter the amount of money on hand and the system will automatically calculate and display the variance between the money collected and the amount entered by the Cashier.

2.5 A review of all lodgement records in the LMIS revealed that the Cashiers were not required to reconcile cash in hand with the LMIS on the system even-though the system was specifically designed with a Cashier module to facilitate such reconciliations. Instead, the reconciliations are done manually at the end of each day. Consequently, the LMIS reflects numerous instances of lodgement variances between the system generated totals and the amount of money each Cashier has in hand even-though these lodgements may have been reconciled manually.

2.6 The manual reconciliation process appears to be time consuming, utilizes excessive paper and relies on the users to perform the control at their own pace and on their own timing rather than being forced by the system. This also affects management's ability to efficiently track all collections, having to review both computerized and manual records as opposed to utilizing all the features of the LMIS to conduct their review.

2.7 The fact that the LMIS does not enforce this business rule increases the risk that Cashiers may not consistently perform the end of day reconciliation and may in fact log out and log in the next day without performing the reconciliation as required. We therefore urge the management of the Authority to ensure that the LMIS enforce all business rules relating to collecting and accounting for revenue in order to reduce the risk of errors or irregularities and increase efficiency.

PART THREE Badge Processing

Inadequate Controls over Badge Processing

3.1 Under section 22 of the Road Traffic (Taxis & Contract Cars) Regulations, drivers and conductors of public passenger vehicles are required to wear badges while operating these vehicles. Furthermore, a person shall not employ any individual to drive a taxi on a road unless that person so employed is the holder of a taxi driver's badge. The grant of a taxi driver's badge shall be conditional on the Licensing Authority being satisfied that the applicant for a badge is of good character and fit to act as a taxi driver.

3.2 The badge application process involves the completion of the relevant form, payment of the appropriate fee, providing a recent Police Record as well as a valid PPV Driver's Licence. A review of this system revealed the following weaknesses:

i. The badge processing system does not interface directly with the LMIS thus increasing the risk that badges may be printed for individuals who have not submitted a legitimate application. The Authority has recognized this weakness and is currently in the process of developing a badge processing module within the LMIS to address this problem.

ii. The badge processing system does not interface directly with the Government's Driver's Licence System located at the Tax Administration Jamaica thus limiting the Authority's ability to determine the legitimacy of an applicant's driver's licence. This increases the risk of individuals submitting fraudulent driver's licences with their applications.

iii. Currently, there is no system in place to ensure that all printed badges are routinely compared with the relevant applications to ensure that both sets of information are consistent or that there is a legitimate application for each badge printed. This is presently done on an ad hoc basis.

iv. The system currently used to produce the driver and conductor badges does not maintain a record of the badges printed, reprinted or spoiled. This weakens management's ability to effectively control and monitor the badge production process and increases the risk of badges being printed without a legitimate application.

3.3 We advised the Authority to ensure that the badge processing module being developed within the LMIS can interface directly with the Driver's Licence System in order to confirm the validity of an applicant's driver's licence. Systems should also be developed to ensure that management is able to exercise effective control over the badge production process and reduce the risk of badges being printed without the necessary supporting documents. The Authority has since committed to utilizing its present electronic interface with the Tax

Administration of Jamaica to verify the authenticity of each applicant's driver's licence. It has also promised that the proposed badge processing module will address some of the above weaknesses.

PART FOUR Access Controls & Network Security

4 The objective of physical security and access controls is to prevent or deter theft, damage, and unauthorized access, and to control movement of network-related equipment and devices. Some physical controls also prevent unauthorized access to data and software. General physical controls that can be used to protect office equipment and computer networks include personnel badges, which help employees identify authorized personnel, alarms and guards, which deter theft of network equipment.

4.1 Logical access controls are used to ensure that access to systems, data, and programs is limited to appropriate users and IT support personnel. Application security should consider privacy and confidentiality requirements, authorization and authentication processes, business access requirements, user training, and monitoring. Access controls provide the first line of defence against unauthorized users who gain entrance to a system's programs and data.

4.2 When information technology systems are developed, appropriate security access controls need to be developed. Additionally, existing security processes, procedures, and controls may need to be reviewed. The goal of application security is to safeguard information against unapproved disclosure or modification, and damage or loss.

Inadequate Controls over Access Cards

4.3 Physical access to the Authority's head office premises is regulated by an access control system that requires the use of an access card. Each member of staff is assigned an access card granting them access to specific areas of the premises according to the group they are assigned to. A review of the controls relating to the Authority's physical access control system revealed the following areas of concern:

i. The Authority's *Security Policies and Procedures Manual* does not adequately outline the procedures to be followed for the issue, return, activation and deactivation of the access cards. It also does not state who the responsible officers are for the administration of the system and what records should be maintained for the purposes of review, monitoring and control.

Currently, the cards are activated and deactivated by any member of the IT division on the advice of a member of the Human Resource (HR) division. There is no designated official in either division who is responsible and therefore accountable for ensuring that the access cards are activated and deactivated in a timely manner. Additionally, no **formal record** of communication between IT and HR concerning authorization for activation and deactivation is maintained.

ii. Our review revealed that access cards for **26 former employees** were not deactivated and could therefore still be used to access the Authority's premises.

Of this amount, six cards were found in the possession of the acting Systems Administrator as shown in **Table 3**.

Table 3: Former Employees with Active Access Cards

POSITION	DATE OF SEPARATION
Summer Employee	Sep-11
Area Supervisor	10-Jan-11
Temporary Employee	18-Feb-09
Accounting Technician 3	21-Apr-11
Summer Employee	19-Aug-11
Clerk	05-Aug-11
Statistician	15-Apr-11
Summer Employee	19-Aug-11
Accountant	21-Apr-11
Route Inspector	18-May-11
Route Inspector	22-Apr-10
Area Supervisor	27-Dec-08
Route Inspector	21-Oct-08
Office Attendant	01-Oct-08
Clerk*	**29-Jun-11**
Office Attendant*	**12-Sep-11**
Administrative Assistant*	**16-Nov-09**
Licensing Clerk	01-Jul-11
Route Inspector	31-Mar-11
Finance Manager*	**11-Apr**
Route Inspector	11-Sep-11
Filing Clerk*	**30-Jul-11**
Former Bodyguard*	**Not seen**
Clerk	10-Aug-11
Route Inspector	26-Oct-08
Ministry of Transport and Works Official	Not seen
*** Cards found in the possession of the acting Systems Administrator**	

Source: Transport Authority Access Control System

iii. At the time of the audit, 16 access cards were found in the possession of the acting Systems Administrator even-though the physical cards are not required for deactivation. Of this amount, seven were still active and two were last used subsequent to the employees' departure from the Authority as shown in **Table 4.**

Table 4: Cards in the Possession of the Acting Systems Administrator

CARD No.	STATUS	LAST USED	SEPARATION DATE
3377148	ON	12/09/2011	12/09/2011
3377191	OFF	12/08/2011	Not seen
3377180	OFF	29/07/2011	01/08/2011
3377129	OFF	14/06/2011	15/06/2011
3377128	ON	28/06/2011	29/06/2011
3377181	ON	29/04/2011	Apr-11
3580006	**OFF**	**30/08/2011**	**26/08/2011**
494073	ON	22/09/2011	N/A
277280	OFF	15/06/2011	N/A
3377143	ON	04/02/2011	Not seen
290942	**ON**	**29/07/2011**	**01/07/2011**
276977	ON	No record	16/11/2009
277282	OFF	29/07/2011	30/07/2011
290948	OFF	23/07/2011	27/08/2011
276997	OFF	No record	21/12/2007
276978	OFF	No record	N/A

Source: Transport Authority Access Control System

iv. The access control system does not permit the *"card enrolment date"* to be updated where an access card is reassigned to another employee. Therefore, where a card has been reassigned, the system will not record the date of the reassignment, only the date of the original assignment. The system also does not record the date the card status has changed from "*ON*" to "*OFF*" or vice-versa. We identified 10 cases where employees with an assigned access card had *"enrolment dates"* which were prior to their dates of employment as shown in **Table 5.**

Table 5: Cards with Enrolment Dates Prior to the Assignee's Employment Date

CARD NO.	LOCATIONS/ DEPT.	EMPLOYMENT DATE	ENROLMENT DATE
3377158	HRM & A.	11.07.2011	06.06.2011
3377173	Finance & Planning	15.08.2011	28.02.2011
4904004	Head Office	21.09.2011	16.03.2010
3377146	Central Administration	21.03.2011	15.07.2009
3377126	Head Office	02.04.2011	24.06.2009
494006	Licensing	01.09.2011	16.03.2010
3377112	SRO	04.07.2011	04.05.2009
3377190	NERO	04.07.2011	16.03.2010
3377136	Property & Facilities	11.07.2011	15.07.2009
3377162	Internal Audit	01.07.2011	28.02.2011

Source: Transport Authority Access Control System

4.4 The Authority has since promised to strengthen the controls over physical access and monitoring by among other things, reviewing its security policy and administration with a view to addressing the weaknesses identified. Additionally, the Authority has taken steps to replace its current access control system with an enterprise system that will be installed at all its locations. Furthermore, we subsequently confirmed that the active cards for former employees have now been de-activated or re-assigned and are no longer in the possession of the Systems Administrator.

Inadequate Controls over Network Access and Activities

4.5 The Transport Authority does not have a system in place to monitor the activities of privileged users and administrators to ensure that they are not abusing or misusing their access rights. Other activities such as network monitoring, firewall activity review and review of user accounts were not conducted in accordance with a specified schedule but were performed on an ad hoc basis and the results of the reviews were not normally documented.

We also found that the relevant records containing authorisation for adding or removing network users were in some cases either not maintained or not consistently maintained. This increases the risk of network errors or irregularities going undetected and consequently undermines the Authority's internal control mechanism.

4.6 For example, due to the Authority's failure to monitor and review its network user accounts, **the accounts of 16 former employees were not de-activated.** Of that amount, **five employees' accounts had logon activities on the network subsequent to their date of termination**.

4.7 Additionally, we found **nine former employees with an active user status on the LMIS**.

4.8 This weakness was also highlighted by the Authority's external auditors in their audit of its financial statements for the year ended March 31, 2011. The Authority's failure to deactivate the accounts of former employees in a timely manner increases the risk of unauthorised access to its systems and data, including confidential or sensitive customer information.

4.9 We recommended that appropriate systems and procedures be implemented to ensure that the activities of privileged users and administrators and network activities including firewall activities are monitored and reviewed on a timely basis. The Authority should also ensure that a system is in place to deactivate all former employees' user accounts in a timely manner.

4.10 The Authority has since implemented a schedule of monthly network reviews, which will be linked to the performance appraisal of the Network Administrator. It also plans to empower its internal audit function to assist in the monitoring of network related activities. Additionally, the active user accounts of all former employees identified during the audit have now been de-activated.

PART FIVE LMIS User Groups

Inadequate Segregation of Duties

5.1 Segregation of duties is one of the key concepts of internal controls. It reduces the risk of both erroneous and inappropriate actions and contributes to an organization's system of checks and balances. The objective of segregation of duties is to separate the following responsibilities in each business process:

- Custody of assets
- Record keeping
- Authorization
- Reconciliation

Ideally, no individual employee should be able to simultaneously:

- Initiate a transaction
- Approve a transaction
- Record a transaction
- Reconcile balances
- Handle assets
- Review reports

5.2 In a computerized environment, segregation of duties is achieved through the creation of User Groups. User Groups are arranged according to department, function/role, project, or other teaming relationships. This measure effectively restricts the use of computer system resources to authorized users as well as ensures that each user privilege is consistent with their job function/role.

5.3 While we did not observe any case of a transaction being initiated and approved by the same individual, we found that a number of officers were assigned to multiple User Groups that may not be consistent with their regular job functions. For example, we identified seven officers who were assigned to both the *Accounts* and the *Accounts Supervisors* Group and one officer to both the *Cashier* and the *Supervisors* Group thus creating the possibility for these persons to authorize or override their own transactions. This may also cause errors or irregularities to go undetected.

Table 6: Users in Multiple Groups

No. of Users	No. of Groups
1	10
1	9
8	5
36	4
41	3

Source: LMIS

5.4 Additionally, we also found that members of the Information Technology (IT) division were assigned to numerous operational user groups contrary to the principles of good business practices and control. This undermines the Authority's internal control mechanism because these users have privileged access and can manipulate the organisation's computer systems. This is even more critical because the activities of privileged users are not monitored or reviewed.

5.5 We advised the Authority to immediately review the composition of each User Group to determine whether the respective members need access to the resources of those groups. The practice of assigning individuals to supervisory and non-supervisory groups at the same time should be discontinued and members of the IT division should not have any operational privileges that may undermine the Authority's internal controls.

5.6 The Authority has noted our concerns and has promised that there will be closer monitoring and review of the activities of privileged users. It has also committed to improving its internal audit IT capacity to assist in this process. Our follow-up also confirmed that at least one member of the IT department now has access to fewer groups than before.

PART SIX Environmental Security

Inadequate Environmental Controls

6.1 Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel[8].

The environment has several key control elements including, temperature and humidity controls, power supply controls, working space control, fire protection systems, and physical security systems. All network 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.

6.2 Our review involved identifying and testing the Authority's general environmental controls as well as specific controls relating to its IT equipment and facilities. This revealed weaknesses in the controls relating to the Authority's server room, emergency alarm system, fire prevention and detection mechanism and its back-up power supply.

6.3 There is currently no smoke detector, automatic fire alarm or other fire suppression system except fire extinguishers installed at the Transport Authority. Furthermore, no Fire Drills were held at its offices located in Kingston until December 2011. The Authority reported that Drills were conducted at its three regional offices in 2008; however, no documentary evidence was maintained to record the results of each exercise.

6.4 The security of the Authority's server room may be compromised due to the following factors:

a. The floor of the room is not raised in accordance with best practice but is on the same level as the rest of the first floor. This increases the risk of water damage, as some of the servers are not elevated.

b. The server room was used to store obsolete/unserviceable items thus creating potential fire hazards. There was no fire extinguisher, smoke detector, fire alarm or other fire suppression system located in the room, consequently, increasing the risk of major damage in the event of a fire.

6.5 The Authority has installed an emergency alarm system, which can only be triggered by someone in close proximity. The system has not been subject to any recent routine

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

inspection or servicing. Testing of the alarms revealed that they were neither centralized nor audible in some areas. When an alarm has been activated, there should be a sound signal as well as an automatic opening of the door(s) relating to those locations. If the sound component is defective but the doors continue to open, this could be used to circumvent the use of the access cards for entry.

6.6 The Authority's back-up power supply consists of an Uninterrupted Power Supply (UPS) system and a stand-by Generator. We could not determine whether the Generator was being serviced regularly, as the relevant records were not maintained. The unit was also inadequately protected from environmental damage and unauthorised access due to the absence of a secured entrance. The UPS was also not adequately secured because it is currently located in an area that is accessible to any member of staff on that particular floor.

6.7 The Authority should develop and adopt a comprehensive Environmental Security Policy that define standards for all its facilities, covering site selection and construction, personnel health and safety, mechanical and electrical systems, and protection against environmental factors such as fire and flood so as to reduce the risk of loss or damage to the Authority's assets. It should also ensure that systems and procedures are implemented to address the specific weaknesses outlined above.

6.8 These limitations have contributed to the Authority's decision to renovate its head office and in doing so, the Authority has promised to address the environmental security weaknesses identified. However, in the interim, the Authority plans to take steps to improve its environmental security by, among other things, installing smoke detectors and reviewing the security of the server room. Subsequent to our initial physical inspection, the Authority has now properly secured its stand-by generator and intends to reconfigure a room exclusively for its UPS.

PART SEVEN Business Continuity Management

Inadequate Testing of Business Continuity Procedures

7.1 The need for providing continuous IT services requires developing, maintaining and testing IT/business continuity plans, utilising offsite backup storage and providing periodic continuity plan training[9]. 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 or be unavailable when an emergency arises. Therefore, best practice requires that contingency plans be reviewed and tested at regular intervals[10].

7.2 The Transport Authority currently has a *Disaster Preparedness and Emergency Management Manual* to guide its management of unplanned service disruptions. However, there is no formal system in place to conduct periodic testing of the Authority's disaster recovery plans to ensure that the procedures remain relevant and effective in the event of a disaster. There is also no formal procedure in place to ensure that back-up media for the LMIS and its other systems are regularly tested to determine the integrity and completeness of the back-up files.

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

7.4 The Authority has advised us that it will take steps to implement our recommendations.

[9] COBIT 4.1-DS4: Ensure Continuous Service

[10] ISSAI 5310: Information System Security Review Methodology

PART EIGHT Legal Claims

Multiple Legal Claims against the Authority

8.1 Section 13 of the Transport Authority Act empowers a Transport Authority Inspector to seize any vehicle that is being used contrary to the terms of its licence or is being operated as a public passenger vehicle without a licence issued for such operation or use. Inspectors also have the power to prosecute any person for any contravention of a relevant road traffic enactment and to serve on such a person any process, summons or document relating to such prosecution or contravention.

8.2 At the time of the audit, the Authority's records revealed that there were 58 "active" cases of legal claims brought against the Authority. The claims were primarily for damages relating to unlawful seizure and detention of motor vehicles and assault. In one instance, a vehicle was seized and subsequently ordered to be released by the police but was eventually sold at auction by the Transport Authority. The Supreme Court ruled in favour of the Claimant and to date a total of $9,189,807.21 has been paid to him.

8.3 Up to December 2011, the Authority had paid out approximately $18M covering both legal fees and settlements relating primarily to claims brought against it by motorists. Furthermore, it has estimated that if the remaining claims were to be successful, the potential damages and costs should be approximately $13.8M.

Table 7: Legal Fees and Settlements

Period	Legal Fees	Settlements	Total
Year ended March 31, 2008	812,400.00	441,500.00	**1,253,900.00**
Year ended March 31, 2009	513,902.00	143,168.29	**657,070.29**
Year ended March 31, 2010	3,023,794.00	307,500.00	**3,331,294.00**
Year ended March 31, 2011	1,383,059.37	2,595,914.38	**3,978,973.75**
April to December 2011	2,949,698.80	5,904,807.20	**8,854,506.00**
Total	**8,682,854.17**	**9,392,889.87**	**18,075,744.04**

Source: Transport Authority Legal Department

8.4 While the Authority has strengthened its legal department to deal with court matters and other legal proceedings, there is no evidence that a comprehensive strategy exists **to target the incidences of unlawful seizures and detention of motor vehicles by its Inspectors**, in order to reduce the risk of further increase in such claims.

8.5 We therefore recommend that a specific set of strategies be developed in collaboration with the Ministry of Transport, Jamaica Constabulary Force (JCF), the Island Special Constabulary Force (ISCF) and the Island Traffic Authority (ITA) aimed at reducing the incidences and the risk of unlawful seizures and detention of motor vehicles.

8.6 The Authority has since advised us that a review of the seizure process has been implemented with a view to mitigating the risk of unlawful seizures. It will also further strengthen its legal department to ensure that seizures of motor vehicles are done in accordance with the relevant law.

PART NINE Seized Vehicles

Disposal of Seized Vehicles

9.1 Section 13 (3) (c) of the Transport Authority Act provides that, where a vehicle has been seized ***"if the vehicle remains in the possession of the police or the Authority for more than six months the vehicle may, subject to such conditions as may be prescribed under the Road Traffic Act, be sold by the police or the Authority to recover the cost of storage."*** Additionally, section 13 (3A) of the Act requires that the proceeds of sale of a vehicle seized shall be paid to the Accountant General. All vehicles which may be sold under section 13 (3) (c) shall be sold by public auction at such time as the Authority thinks necessary. Where vehicles remain unsold after they have been put up for sale by public auction, the Authority may, if it thinks fit, sell those vehicles by private treaty or cause them to be destroyed or otherwise disposed of as it thinks fit.

9.2 The Authority reportedly conducted a disposal exercise of 698 seized vehicles in November and December 2008. This involved the public auction of 304 vehicles, sale by way of sealed bids of 205 vehicles and sale by way of private treaty of 189 vehicles as shown in ***Table 8***.

Table 8: Disposal of Seized Vehicles by the Transport Authority

No. of Vehicles	Method of Disposal	Proceeds*
304	Auction Bids	23,707,867.43
205	Sealed Bids	3,986,105.75
189	Private Treaty	840,000.00
698		**28,533,973.18**

**** Proceeds include GCT.***

Source: Transport Authority Auction Records

9.3 Of the 698 vehicles sold, 12 vehicles were returned to the Authority and the bidders refunded a total of $1,075,820.00 (inclusive of GCT) because the vehicles sold either were subject to a lien or could not otherwise be transferred by the Inland Revenue Department (IRD) to the successful bidders. Subsequently, however, the Authority has implemented a system to ensure that "clearance" is received from the relevant authorities such as the IRD and the Police, before seized vehicles can be auctioned or otherwise disposed of.

9.4 Of the 205 vehicles sold by way of sealed bids, 114 were sold to the same company for a total of $483,200 and 17 were sold for less than the highest bid received as shown in ***Table 9***.

Table 9: Vehicles Sold For Less than the Highest Bid Received

Vehicles	Bid 1	Bid 2	Bid 3	Bid 4	Successful Bid
Toyota Corolla	**50,000**	40,500	40,000		40,500
Toyota Corolla	51,550	50,000	**55,000**	40,000	51,550
Nissan Sunny	**51,000**	20,000			20,000
Daihatsu	**20,000**	10,000			10,000
Nissan AD Wagon	**25,000**	20,000			20,000
Toyota Corolla	**25,250**	20,000			20,000
Toyota Corolla	**30,000**	25,000	20,000		25,000
Daihatsu	**120,000**	90,000	60,000		90,000
Nissan AD Wagon	**12,000**	7,000	6,000		6,000
Nissan Station Wagon	**10,000**	6,300			6,300
Toyota Corolla	**85,000**	50,000	61,000		50,000
Toyota	**15,000**	1,800			1,800
Suzuki	**50,000**	40,000	20,000		20,000
Suzuki Pick-up	**55,000**	30,000	25,000		30,000
Nissan Sunny	**35,000**	30,000	30,000		30,000
Daihatsu	**50,000**	30,000			30,000
Nissan Super Salon	**100,000**	90,000			90,000

Source: Transport Authority Auction Records

9.5 We also observed that no funds were paid over to the Accountant General because the estimated storage costs of approximately $72.3M was over 2½ times more than the disposal proceeds, resulting in a net cost to the Authority.

9.6 In 2010, 709 vehicles were identified for auction, however, according to the Authority no auction has been held since 2008 due in part to a failure by the police to "sign off" on the vehicles prior to sale. Furthermore, the Authority has estimated that based on the current motor vehicle valuations and their associated storage costs, it would be uneconomical to proceed with any auction. Consequently, the Authority has decided to introduce an amnesty instead of disposal by way of public auction.

9.7 Seized vehicles that are held for an inordinately long period increase the risk that disposal by way of sale will be uneconomical due to their decline in value and associated storage and disposal costs. The Authority should therefore ensure that an efficient system is in place to track all vehicles seized and to activate the disposal process for such vehicles that have been held for six months as outlined in the Transport Authority Act.

PART TEN Governance & Human Resource

10.1 Corporate governance is the system by which corporations are directed and controlled. This includes developing relevant policies and procedures to enable an organisation to achieve its objectives and safeguard its assets. The Transport Authority's corporate governance structure is guided by the Transport Authority Act, the Public Bodies Management and Accountability Act and relevant guidelines issued by the Ministry of Finance. We reviewed the Authority's current policies and procedures to determine whether they are consistent with the various regulatory requirements or with generally accepted principles of good governance.

No Gazetting of Board Appointment

10.2 The First Schedule of the Transport Authority Act outlines the constitution of the Authority. Section 1(1) states that ***"the Authority shall consist of five ex officio members and not less than two or more than four appointed members."*** Additionally, Section 7 requires that ***"the names of all members of the Authority as first constituted and every change in the membership thereof shall be published in the Gazette."***

10.3 Despite numerous requests and checks, we found no evidence that the appointment of the Board of Directors with effect from June 27, 2011 was published in the Gazette as required by Section 7 of the First Schedule of the Act. Furthermore, the management of the Authority has not included, as part of its standard procedures, systems to ensure that Board appointments comply fully with the provisions of the Transport Authority Act. This is because the Ministry of Transport usually process all documents relating to Board appointments.

10.4 Therefore, steps should be taken by the management of the Authority to ensure that all future Board appointments are done in accordance with the provisions of the Transport Authority Act.

10.5 The Authority has since accepted our finding and recommendation.

Policies and Procedures Lacked Board Approval

10.6 The Public Bodies Management and Accountability Act provides general corporate governance guidelines for the effective management of a public body such as the Transport Authority. Section 6 of the Act outlines the general responsibilities of every Board appointed to manage the affairs of each public body. Section 6(b) requires that ***"every board shall develop adequate information, control, evaluation and reporting systems within the body"*** to facilitate the efficient and effective management of its operations. Therefore, one important part of a Board's mandate is to provide policy direction in order to assist the organisation in achieving its objectives.

10.7 Our review revealed that there was no system in place to ensure that all policies and procedures adopted by the Authority were ratified/reviewed by the Board of Directors (or sub-committee) prior to their implementation. This resulted in the implementation of at least nine significant policy documents without any formal Board review or approval.

10.8 The Board is accountable for the development of the Authority's operational policies and we therefore recommend that steps should be taken to ensure that all such policies and procedures be brought to the attention of the Board for review and ratification. Furthermore, the Authority should ensure that an appropriate system is implemented to facilitate Board review of new or amended policies/procedures before they are adopted.

10.9 The Authority has since advised us that the Sub-Committees of the new Board of Directors are currently reviewing all Policies and Procedures with a view to having them ratified.

Audit Committee Was Not Properly Established

10.10 Section 8(1) of the PBMA Act states that ***"...every public body that has four or more directors shall establish an audit committee consisting of not less than three directors."*** During the period October 2007 to December 2011, the Authority's Board consisted of four or more directors. Therefore, based on the provisions of the PBMA Act, its Audit Committee should consist of at least three directors excluding the Managing Director.

10.11 Based on the evidence presented to us, the Authority's Audit Committee only operated with three or more directors as members for the period October to November 2010. Outside of that brief period, the establishment of the Audit Committee was not in accordance with the requirements of the PBMA Act because it was made up of fewer than three directors.

10.12 Going forward, the management of the Authority should advise the Board of its obligation to comply with the requirements of the PBMA Act in the appointment of an Audit Committee.

10.13 The Authority has accepted our recommendation.

Audit Committee Lacked Independence

10.14 The main role of the Audit Committee is to provide independent, effective oversight on the financial reporting process and internal controls of an organisation. The Committee should not have any executive powers and shall not be responsible for the preparation of financial statements or the implementation of proper systems of internal controls. It is usually responsible for overseeing and assessing the adequacy and scope of the arrangement for the management of the internal and external audit functions.

10.15 The existence of the Audit Committee contributes to good corporate governance, being an independent instrument of control and a review organ thereby improving both efficiency and accountability.

10.16 We, however, found that the independence of the Audit Committee in performing its oversight responsibilities might be compromised because it is also involved in the management of fixed assets. In fact, the Committee's title is the ***Audit and Fixed Asset Management Committee*** with a mandate to among other things establish policies/procedures and performance standards for the management of fixed assets.

Some of these activities relating to fixed assets management are outside the scope of an independent audit function and are usually the purview of management. Consequently, this may create a self-review threat resulting in a lack of objectivity on the part of the Audit Committee.

10.17 In order to remove or reduce any real or perceived lack of objectivity/independence, we recommend that the mandate of the Authority's Audit Committee be consistent with the provisions of Section 9 of the PBMA Act. This section provides general guidelines on the duties of Audit Committees within public bodies. It will also assist the Committee to maintain the desired level of independence and objectivity.

10.18 The Authority has since advised us that the new Audit Committee will focus independently and exclusively on audit matters while the Finance Committee will now deal with Fixed Asset Management.

Unapproved Staff Establishment

10.19 An organisation's approved establishment details the number and categories of staff necessary for the efficient and effective operations of the entity. Throughout the public sector, it is the responsibility of the Corporate Management Division (CMD) of the Cabinet Office to review, evaluate and approve the staff establishment for most public sector entities.

10.20 We observed that the Authority's staff complement of 292 employees was not approved by the Cabinet Office or the Ministry of Finance. This issue was highlighted in a 2008 organisational review conducted by the CMD and recommendations were made at the time to regularize the situation. However, the Authority did not respond formally to the CMD's findings and the recommendations have not been implemented. Staff costs including salaries and allowances for the financial year ended March 31, 2011 was $446,630,277 (2010: $404,117,410) representing 69% (2010: 69%) of operating expenses.

Table 10: Transport Authority Staff Complement

No. of Staff	Category
112	Route Inspectors & Senior Inspectors
180	Management, Administrative and Support Staff
292	

Source: Transport Authority Human Resource Division

10.21 The management of the Authority has informed us that their operations are in need of "realignment" and that this process has already started. We, however, recommend that the Authority seek the assistance of the Cabinet Office or the Ministry of Finance to regularize this situation and implement an approved staff establishment.

The Management of the Authority has accepted our recommendation.

Unapproved Employee Benefit Schemes

10.22 Section 20 of the PBMA Act requires that in relation to emoluments, the Board of a public body shall act in accordance with such guidelines as are issued from time to time by the Minister responsible for the public service. This generally requires a public body to obtain the approval of the Ministry responsible for the public service to operate certain employee benefit schemes.

10.23 We found that the Transport Authority operates a number of employee benefits facilities such as staff loans but these have not been approved by the Ministry of Finance. The Authority submitted a request for approval in 2009, however, apart from acknowledging receipt, the Ministry of Finance has not provided any subsequent updates neither have we seen any follow-up by the Transport Authority. Staff loans as at the financial year ended March 31, 2011 was $4,237,072 (2010: $2,553,246), an increase of 66% over the previous year.

10.24 We advised the Authority to follow-up with the Ministry of Finance to have its employee benefit schemes approved and regularized. The Transport Authority has accepted our recommendation.

Inadequate Personnel Clearance Procedures

10.25 Best practice in relation to personnel clearance procedures include individual background checks for criminal convictions, past employer and reference verifications as well as confirmation of certificates of qualifications submitted by current/prospective employees.

10.26 The Transport Authority adopts some of these procedures as part of its employment screening process. Currently, for new employees, the Authority requires the following records prior to employment:

- Recommendation from previous employer
- Copies of qualifications and certifications etc
- Police Record
- Other recommendations from a Minister of Religion or Justice of the Peace

Additionally, all employees are required to sign the Official Secrets Act Declaration, which is the basic standard confidentiality agreement throughout the public sector.

10.27 On the other hand, the Authority does not routinely verify the authenticity of the certificates of qualifications received from current or prospective employees. It is therefore unable to independently determine whether these persons have satisfied the Authority's qualification criteria.

10.28 From the sample of employees selected, we could not determine whether 16 persons met the minimum requirements for employment, as the relevant certificates were not on their respective files.

10.29 Additionally, there was no police record for seven employees and no signed copy of the Official Secrets Act Declaration for 10 members of staff.

10.30 The management of the Transport Authority should therefore ensure that a system is place to routinely verify the academic and other credentials of current or prospective employees to guard against persons with fictitious certifications. It should also strengthen its existing mechanism to ensure that all employees submit a Police Record as required and sign a copy of the Official Secrets Act Declaration in order to help preserve the confidentiality and integrity of certain aspects of the organisation's operations. The Authority has accepted our recommendations.