SPECIAL AUDIT REPORT ON THE MONTSERRAT FERRY SERVICE:

INFORMATION SECURITY AUDIT OF THE MONTSERRAT FERRY ONLINE BOOKING APPLICATION

Office of the Auditor General
Brades Main Road
Brades
Montserrat

February 2020

SPECIAL AUDIT REPORT ON THE MONTSERRAT FERRY SERVICE:

INFORMATON SECURITY (IS) AUDIT OF MONTSERRAT FERRY ONLINE BOOKING APPLICATION

This is a Report of the collaborative Information Security Audit and Financial Audit conducted by the Office of the Auditor General pursuant to Section 103 of the Montserrat Constitution Order 2010

Florence A. Lee,
Auditor-General,
Office of the Auditor-General,
February 2020

PREAMBLE

Vision-Statement

"To be a proactive Supreme Audit Institution that helps the nation make good use of its resources".

Mission-Statement

"The O.A.G. is the national authority on public sector auditing issues and is focused on assessing performance and promoting accountability, transparency and improved stewardship in managing public resources by conducting independent and objective reviews of the accounts and operations of central government and statutory agencies; providing advice; and submitting timely Reports to Accounting Officers and the Legislative Assembly".

The Goal

"To promote staff development, enhance productivity, and maintain a high standard of auditing and accounting in the public sector, thereby contributing to the general efficiency and effectiveness of public finance management."

AUDITOR GENERAL'S OVERVIEW

The Montserrat Public Service utilizes several Information Technology systems to improve efficiency and effectiveness of the services it offers to citizens. One such system is the Montserrat Ferry Online Booking Application, a service intended to make it easier and convenient for the travelling public to make reservations for the ferry service. Having knowledge of passenger numbers also makes it easier for the Access Division to manage the ferry operations and to schedule alternative means of travelling to and from Montserrat as the need arises.

We conducted a review of the application to assess and determine whether (1) there are adequate Outsourcing, IT Operations, Application, and Information Security controls in place, to ensure the security of the ferry online booking software, and (2) arrangements were to make certain there is continuance of this online booking service if the agreement with the contractor expired; their services were terminated; the company folded; or if their services were suspended or withdrawn.

Our review revealed that, in general, the Government of Montserrat (GOM) does not have an outsourcing policy in place to outline what functions are to be outsourced. In relation to the Montserrat Ferry Online Booking Application, there is no Service Level Agreement or Contract in place that defines the services the contractor is expected to perform.

Our recommendations which are intended to improve operations, once implemented include, the following. (1) GOM develop an outsourcing policy that clearly documents The IT functions that can be outsourced and what should remain in-house. (2) A Service Level Agreement should be developed which outlines the roles, responsibilities and services the contractor should perform. (3) As a mission critical software, we recommended that the Access Division consider the feasibility of purchasing the software and maintaining it in-house.

Florence Lee, CPA, BSc, MSc
Auditor General,
Office of the Auditor General,
Brades Main Road,
Brades,
Montserrat
26 February 2020

ABBREVIATIONS

AWS	Amazon Web Services
BCP	Business Continuity Plan
DITES	Department of Information Technology & e-Services
DRP	Disaster Recovery Plan
FISCAM	Federal Information System Controls Audit Manual
GoM	Government of Montserrat
IS	Information Security
ISAE	International Standard on Assurance Engagements
ISSAI	International Standard of Supreme Audit Institutions
IT	Information Technology
MCW	Ministry of Communication & Works
NIST	National Institute of Standards and Technology
OAG	Office of the Auditor General
OotP	Office of the Premier
PFMAA	Public Finance Management and Accountability Act
RBAC	Role-based Access
SLA	Service Level Agreement
SQL	Structured Query Language

CONTENTS

EXECUTIVE SUMMARY

Overview

1. The GoM, in its quest to make traveling to Montserrat by sea easier and more convenient, decided to launch the online ferry booking facility in 2016.

Main Findings

2. **Outsourcing**. The OotP, Access Division does not have a Service Level Agreement or Contract that defines what functions are to be outsourced, what must remain in-house, or the ownership of the application and the stored data. This is a very high-risk issue should the Lavabits fail to maintain the software, goes out of business, or folds, as the GoM does not retain business knowledge or ownership of the ferry online booking application and data.

3. **BCP/DRP** GoM has no published Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP), concerning the contingency operation of Montserrat Ferry Online Booking application.

4. **Information Security.** The noted environmental and physical controls at the ferry terminals were either very substandard or non-existent. There have not been any reports of any security related incidents or breaches pertaining to the Montserrat Ferry Online Booking application, since its initial debut in 2016.

5. **Application Controls**. There are adequate input and output validation controls in place, which ensures that the data being input or output is accurate, reliable, and complete when accepted by Montserrat Ferry Booking application, in a timely manner. The application's information is properly protected and secured against misuse via segregation of duties, different user roles, and access rights, available for each user profile.

Key Recommendations

There are several recommendations within the report; however, the following are our chief concerns:

(i) **Develop an Outsourcing Policy.** The GoM should develop a clear outsourcing policy that documents the IT functions that can be outsourced and what remains in-house. All of the roles and responsibilities between GoM and future vendors and contractors should be identified and defined. This includes a Service Level Agreement that defines the services the contractor will be expected to accomplish, and the technical parameters for those services, i.e., whatever items critical to the GoM.

(ii) **Software Purchase.** Access Division should assess the feasibility of purchasing the software and maintaining it, in-house. Should this option not be accepted by the supplier, then it should ask for the software to be lodged in an escrow agreement where the source code is stored with an independent third party.

Audit Conclusion

From the IS investigation, the Office of the Auditor General found that for the most part, the Montserrat Ferry Online Booking application was very robust and secure. The most pressing issues were in relation to Outsourcing and Business Continuity & Disaster Recovery.

THIS PAGE WAS INTENTIONALLY LEFT BLANK

CHAPTER 1 INTRODUCTION

Background

1. The Access Division falls under the responsibility of Office of the Premier (OotP). The principle objective of the unit was to develop an Access Strategy, which would address the island's Access issues and position it for sustained development in keeping with the sustainable development plan. The objectives of the Access Division are as follows:

a) Supply of adequate and consistent capacity by air and sea which is safe, efficient, reliable, and affordable.

b) Supply of consistent self-sustaining capacity by air and sea which is optimal, safe, efficient, reliable, and affordable.

2. An online booking system was established and in operation by November 2016. The travelling Public is now able to make reservations online, undertake advance bookings and pay online, all of which renders the entire booking and check-in process more efficient and customer-friendly.

3. As an initiative to improve the services it offers to its travellers, the Government of Montserrat (GoM) is placing more focus on the use of technology to aid in making some services more readily accessible to the public.

Management Responsibility

4. Management is responsible for ensuring that appropriate policies and effective controls exist to guide the facilitation of Montserrat Ferry Booking services. More specifically, management must ensure that policies and procedures exist to facilitate and to guide Outsourcing, IT Operations, Information Security, Business Continuity, and Application Controls. Management is also responsible for establishing appropriate Information Security (IS) controls and for ensuring that they function effectively.

Auditor's Responsibility

5. Our responsibility is to independently express a conclusion on the security and contingency strategies for the Montserrat Ferry Online Booking application and data based on our audit. Our work was conducted in accordance with International Standard of Supreme Audit Institutions (ISSAI) 100 and International Standard on Assurance Engagements (ISAE) 3000. These principles require that we comply with ethical requirements and plan and perform the audit so as to obtain reasonable assurance as to whether policies, procedures, and controls exist and are functioning effectively.

Audit Mandate

6. The Office of the Auditor General (OAG) is mandated through the Montserrat Constitution Order 2010 to perform the audit. This mandate is supported by ISSAI 1 and strengthened by the Public Finance Management and Accountability Act (PFMAA) 2009 which

makes the Auditor General responsible for the audit of the Public Accounts, Accounts of Government Ministries or Departments, Statutory Corporations and entities who are receiving or seeking grants from the public purse. The audit work was conducted in accordance with the Public Finance (Management and Accountability) Regulations 2008.

Audit Standards & Guidelines

7. The audit was conducted in accordance with the Auditing Standards issued by the International Organization of Supreme Audit Institutions (INTOSAI). The standards and guidelines used to assess the Montserrat Ferry Online Booking application included the use of ISSAI 5100 and 5300, FISCAM, NIST, together with the IDI Handbook for IT Audits.

Audit Objectives

8. The objectives of this IS audit, is to assess and determine whether:

(i) There are adequate Outsourcing, IT Operations, Application, and Information Security controls in place, to ensure the security of the ferry online booking software and the sensitive and personal information inputted/stored on it.

(ii) Provisions were made by the OotP, Access Division to make certain there is continuance of this online booking service if the agreement with Lavabits expired; their services were terminated; the company folded; or if their services were suspended or withdrawn.

Audit Scope and Methodology

9. The study will cover the period 2016 to 2018 and will focus on the examination of the policies, procedures, and controls that guide the operations, outsourcing, physical & environmental, logical access, security, and business continuance for the Montserrat Ferry Online Booking system.

10. A combination of techniques were utilised to gather information and assess whether relevant controls existed, were implemented, and if they were effective in ensuring that the Access Division's data is protected and that there is continuance of service. These included, but were not limited to, interviewing of the key stakeholders from Access Division, Lavabits, Jemmotte Shipping and Tours, Montserrat Port Authority, Jenny Tours, and the Antigua & Barbuda Customs & Excise and Immigration personnel. Other measures included issuance of questionnaires, review of documents, observation of the software, and inspection of assets and premises, in order to gather in-depth information about the Montserrat Ferry Online Booking system.

11. The findings of this report were discussed with the Permanent Secretary, OotP, and the Access Coordinator; their views were taken into consideration when finalising the report.

CHAPTER 2 DEVELOPMENT OF THE MONTSERRAT FERRY ONLINE BOOKING SYSTEM

Access Division, Ministry of Communications & Works (MCW)

12. Since the volcanic crisis and relocation to the northern section of the island, access into Montserrat by sea has always been, and still is, a bit of a challenge; particularly during the peak tourist periods of the year. One of the main challenges was obtaining tickets for the ferry service into Montserrat from Antigua; especially for the overseas travellers.

13. Consequently, in 2013, the then Access Coordinator, verbally solicited the services of the local software company Lavabits, to develop a software solution that would provide a convenient and simpler way of purchasing ferry tickets. At the time, the Access Division fell under the umbrella of the Ministry of Communications & Works (MCW).

14. Lavabits presented their Ferry Booking Proposal on 7 May, 2013 to the key stakeholders -representatives from the GoM and DFID.

Lavabits

15. Lavabits' proposed Ferry Booking system was designed to allow travellers to book and purchase their ferry tickets, online. The web-based nature of the system would allow travellers and the relevant stakeholders to have access to the system, anywhere in the world, on any Internet enabled device. Lavabits' would also provide maintenance services.

16. Each phase of the project would have three main components (i) front end (ii) a back end and (iii) a SQL (Structured Query Language) database for the storage and retrieval of the online ferry booking data.

Maintenance

17. A six-week testing period after the system was launched was initiated to resolve any technical issues, at no cost to the GoM. Lavabits contractual obligations would be fulfilled and completed and an extended maintenance package would be offered after the contract expires.

Hosting

18. Two hosting options were offered to MCW/Access Division by Lavabits (i) hosting without server maintenance EC$1,000.00, and (ii) hosting with server maintenance (security updates, backups, etc.) EC$3,300.00 annually.

Cost

19. The MCW and Access Division, presented Lavabits an initial payment in September, 2013; overall, the grand total for the development and implementation of the online ferry booking software, was EC$37,000.00.

Rollout of the Software

20. The Montserrat Ferry Booking application was officially launched in November 2016. This delayed rollout was a result of:

- Seeking the requisite approval from a financial institution and PlugnPay took longer than expected.
- The decision for the non-launching of the application during Montserrat's peak tourist periods.
- Constant delays in launching and testing of the pilot version.

21. There was also the setback of filling the vacancy for the Access Coordinator position. Additionally, the Access Division encountered a long interval for the provisioning of a new ferry after the expiration of the *Caribe Sun* contract.

Observations

22. **Transfer of Responsibility.** The responsibility for the Access Division was transferred from MCW over to the Office of the Premier (OotP).

23. **Additional Features.** Since its official launching in 2016, the ferry booking software has been updated with following additional features, at the bidding of the Access Coordinator:

I. The ability of ferry agents to check-in passengers and keep track of cargo; they can:

- scan/read passport and credit card information into the system
- issue boarding passes
- create, log, and retrieve ferry bookings/ticket purchases and cargo information
- cancel tickets on the spot if making bookings for passengers, in person
- change reservation date/time/destination
- generate and print summary Sales reports, only

II. In addition to the privileges/tasks that the ferry agents perform, the administrators also have the ability to:

- refund/reverse payments
- transfer ferry tickets into another person's name
- extend the validity of unused tickets
- change booking date/time/destination
- add/deactivate user accounts
- change user role/permissions
- update the ferry service status/ferry schedule/vessel names/special events, promos, cancel trips, etc., on the website
- generate and print the various reports in detail

III. The ability of travellers to use the Ferry Booking website facilities to:

- make bookings/purchase ferry tickets
- subscribe to updates, offers, and promos

- view up-to-date ferry schedules and ferry service status
- contact the Access Division with any queries/concerns
- be linked directly over to the Montserrat Tourism Division website

24. **Fixed Ferry Ticket Price**. The cost of the ferry tickets are fixed and cannot be changed by Access Division. Adjustments to the fares can only be approved and executed, by Cabinet.

25. **Change in Purchase Policy.** Access Division had to introduce a cut-off point for ferry tickets being purchased online. Some passengers, especially those from overseas, waited until the very last minute to purchase their ticket just before they boarded. This caused delays in the boarding process and disruption of the ferry schedule. Passengers can only now purchase their tickets one hour before departure.

26. **Additional Reporting Categories.** The following extra reports were added, by the request of the Access Coordinator:

- Refunds – by agents or admin
- Sales by Passengers – for online bookings
- Passengers – i.e. the number of people who travel on the ferry. This report was included specifically for DFID.

27. **Amendment of Refund and Ticketing Policies.** The current Access Coordinator amended the policies concerning Refunds and Tickets. Passengers are now able to receive refunds; unused ferry tickets will be validated for one year; and ferry tickets can also be transferred from one passenger to another.

CHAPTER 3 OUTSOURCING

Outsourcing Policy

28. An outsourcing policy would define what IT functions can be outsourced and what should remain in-house. The GoM does not have a formal document that outlines or highlights the services that could be outsourced, nor do they have any clear approval process for the outsourcing of a function or service.

Solicitation

29. In May 2013, the decision was made by the former Access Coordinator to hire Lavabits, to develop the Montserrat Ferry Booking application. The services of the software company, was verbally solicited and there was no tendering process.

Service Level Agreement

30. In the initial stages of the software development project, a Service Level Agreement (SLA) was not put forward by either Access Division or Lavabits. The SLA would have detailed all the requirements during the developmental stages and after software was implemented; technical and list of services to be performed; baselines for the services that will be measured, measurement period, duration, location and reporting timelines (e.g. help desk hours response times, etc.)

31. However, Lavabits took the initiative and devised a proposal with the specifications for the ferry booking application, which they submitted and it was approved by the MCW, Access Division in May, 2013. Lavabits developed the Ferry Booking application as per their proposal, which was approved by the stakeholders. Not many changes were made to the proposed ferry booking application, during the development phase.

Contract

32. As of 2016, Lavabits began submitting an annual Maintenance Agreement to the OotP, Access Division. The contract is valid for a period of one (1) year; during which Lavabits would perform maintenance duties to the Ferry Booking application as follows:

a) Maintain software (bug fixes, security updates, an software upgrades
b) Provide technical support to the Access Division and Ferry Agents (Jemmotte Shipping and Jenny Tours)
c) Upload ferry schedule to Access Division's online booking system
d) Maintain the Access Division's server
e) Process on behalf of the Access Division credit card verifications and refunds.

33. The OotP is to pay Lavabits an annual fixed sum with a single, fixed, upfront payment for each request during the one year period. The contract states that Lavabits is not an employee, agent, servant, partner, or joint venture associate, of the GoM.

Vendor or Contractor Monitoring

34. Lavabits was monitored by the stakeholders during the developmental stages via meetings and demos. There were also trial runs before the official launch of the Ferry Booking application in November 2016.

Retaining Business Knowledge and Ownership of Business Process

35. There was, and still is no, formal document between OotP, Access Division that clearly states who retains the business knowledge or who owns the business process, for the Montserrat Ferry Booking. Therefore, because there was/is no formal SLA or contract that states the ownership of, protection of, and access rights to, the data inputted/stored in Montserrat Ferry Booking application, there is an inherent risk of loss of data which resides with the developers of the Montserrat Ferry Booking application.

36. Secondly, seeing that the OotP and Access Division do not retain ownership of the software, and although the Montserrat Ferry Online Booking application is in current operational use, the software's source code is still held and owned by the developers. This can pose a number of high risks associated with the developer maintaining control over the software as follows:

(i) Delays in processing the online ferry booking application when difficulties with the functionality of the software, are encountered.

(ii) Continued availability of support or supplier failure, which could lead to the loss of software use.

37. These risks would negatively impact the online booking facility and other important ferry related procedures and tasks.

CHAPTER 4 BUSINESS CONTINUITY AND DISASTER RECOVERY

Business Continuity Plan

38. Neither Lavabits nor Access Division has any published Business Continuity Plan (BCP) concerning the contingency operation of Montserrat Ferry Booking application.

39. Access Division's informal Disaster Recovery backup plan, is to revert to the manual process of making bookings, checking-in passengers, recording cargo and ferry manifest, etc., until Internet access is restored by the local service provider, and if it is the case, the replacement of damaged or destroyed computer equipment.

Back-Up and Disaster Recovery for Outsourced Services

40. Lavabits does not have a physical office space with hardwired network comprised of computers and server equipment, to maintain and monitor. The Ferry Online Booking software is run and maintained on Cloud platforms servers provided by US-based companies Heroku and Amazon. Heroku and AWS are responsible for backing up the system and for securing their servers; backups are created daily and the current storage plan being used by Lavabits, allows twenty-five 25 backups to be retained for any duration. Heroku/ASW only stores the amount of data that is inputted into the booking system, on a given day.

41. There are no backup sites for any of the entities. Back-up premises are not necessary as the Montserrat Ferry Online Booking application can be accessed at any time from any device that enables web browsing, and there is internet access.

Observations

42. **Cloud Hosting Business Continuity obligations**. Heroku/Amazon Web Services (AWS) Cloud platforms are responsible for the security monitoring and maintenance of their own servers, and for backing-up the Ferry Booking application.

CHAPTER 5 INFORMATION SECURITY

Physical Security & Environmental Controls

43. A walkthrough of Access Division and both the Ferry Terminals premises was conducted and the following control parameters in terms of building structure, UPS, fire protection, humidity, temperature, and voltage, flood protection, etc., were examined:

(A) Access Division - 3rd floor of the Hubert Buffonge Building, Brades

44. The Access Division is housed in a large concrete, air conditioned office space with several lightly tinted, large and medium-sized, impact resistant windows against inclement weather, with curtains and window blinds to control direct rays of sunlight. The main entrance/front doors are large, glass double doors that are also impact resistant and lightly tinted.

45. The flow of traffic through the front doors is monitored at all times during working hours, by Access Division and Montserrat Tourism Division, staff.

46. There is no backup generator in case of power cuts; each personal computer is plugged into a UPS, most of which do not work. The printer is not plugged into a UPS or surge protector. There are breaker panel switches in case of an emergency shut down of the power.

47. Although there was a reported incident of slight flooding at the back of the office during inclement weather in 2018, at the time of the inspection, there were no signs of dampness or water damage; water bubbles in paint or peeling paint; mildew; water stains on wooden ceiling, walls, floorboard skirting, or window ledges; or moisture oozing out of the walls.

48. Notably, there is no fire detection, suppression, protection warning system, or equipment, in the office space.

(B) Jenny Tours - Ferry Terminal, Heritage Quay, Antigua

49. Jenny Tours is housed in a small, air-conditioned, elevated, wooden office space. There is only one door leading into the office for staff use only, and two small double hung, impact resistant, windows at the front through which all transactions with travellers are conducted.

50. There were no signs of water damage, dampness, or mould on the walls or wooden roof despite the recent passage of severe weather a few months prior. There was also no fire detection, suppression, protection/warning system or equipment, in the office space or around the ferry terminal.

51. All of Jenny Tours' computers and office equipment (laptops, Personal Computer, All-in-one Printer, passport and/or card readers, and receipt printers) were not plugged into UPSs or surge protectors. They were all plugged directly into the wall sockets. In addition, there was no backup generator in the event of power cuts at the ferry terminal to provide an uninterrupted source of power in the event of a power outage to Jenny Tours, and the Customs and Immigration Depts.

52. There were no CCTV cameras, but there is purportedly 24-hour security guard service, although we only observed on-duty guards during the daytime. However, it was pointed out that there are night security guards that patrol the Heritage Quay wharf area.

(C) Jemmotte Shipping & Tours - Ferry Terminal, Port Little Bay

53. The Montserrat Ferry Terminal building is a solid concrete structure that is not air-conditioned; it is equipped with only ceiling fans. As a result, the building tends to get very hot at certain times of the day and year, making it uncomfortable for the passengers and booking agents, alike. In addition, long-term exposure to the intense heat at the ferry terminal can cause all of the computers and other electrical equipment, to overheat and to eventually malfunction.

54. The outer area of the ferry terminal is not prone to flooding and there were no signs of water damage, dampness, or mould anywhere on or inside the building.

55. The Access Division's laptop, Personal Computer, Printer, passport and/or credit card readers, and receipt printers, are not plugged into a UPS. Half of the computer equipment is plugged into a standard power strip, which is in turn plugged into an industrial power strip that has a surge protector. The other half of the computer equipment is also plugged into this industrial power strip, which is also plugged directly into a wall socket. The Montserrat Port Authority (MPA) has a backup generator and the ferry terminal, which falls under the jurisdiction of the MPA, benefits from this generator during power cuts.

56. There are no smoke/heat detectors or fire alarm. However, the ferry terminal is well equipped with five (5) chemical fire extinguishers that are to be inspected and tested by fire dept. every three (3) months. At the time of the audit, the last inspection date was 1 May, 2018; the MPA will prompt the Fire Dept. to conduct the testing, if they are delinquent in adhering to their quarterly schedule.

57. The ferry terminal is not equipped with water sprinklers; however fire hoses are available nearby and around the MPA compound. There is a fire hydrant at the MPA's main gate; in addition, seawater would be pumped from the ocean using a saltwater pump, to extinguish fires.

58. Access in and out of the ferry terminal premises, from boardwalk area, is restricted and monitored by high fencing, locked gates, and security personnel. From the MPA side, access is controlled by security guards at the main gate where persons are manually logged in and out and issued with visitor's badges to be worn in plain sight at all times once inside MPA's compound. There are also CCTV cameras in and around the ferry terminal building. In addition, there is 24-hour security guard patrol of the Port Authority compound, jetty and ferry terminal areas.

Access Controls

59. There is no formal access control policy documentation pertaining to the Montserrat Ferry Booking software, but there are certain procedures in place that ensures access to the application, is authorised:

- Access is commensurate with job function/role and segregation of duties only. There are clearly defined roles and/or privileges that are mapped to the job functions of the users; that is, 'Administrator' or 'Agent'.
- Authorisation to use the software to perform certain tasks in the Ferry Booking application has to be assigned/approved by the Access Coordinator, who is also one the chief administrators. He would send an email to Lavabits, authorising the addition/deactivation/change of privileges, of user(s).
- There is an RBAC (role-based access) list of authorised users who can to sign-in using a unique user ID and password.
- Passwords have to be 8 characters long
- Passwords do not have to be forcibly changed although this feature is built-in the software

Data Security

60. The Montserrat Ferry Booking application's data is secured appropriately as it is stored and run from Heroku/AWS cloud platform servers. To date, there has not been any reported case of breach of security on the cloud platform servers.

61. Access control logs are automatically generated as soon as anyone logs into the ferry booking application, with their unique user id and password. These user logs are built-in security audit trails that capture all of the authorised users' activities i.e. user unique id, dates, times, and what tasks were performed, etc.

62. The unusual activity of a lower level GoM employee, who was granted authorised access to the ferry booking application for work purposes only (reporting), was recently uncovered. The Access Division was able to trace this employee's activities utilising the Ferry Booking application's built-in audit logs, associated with this employee's user account.

63. Based on the requirements and usage of the Ferry Booking system, i.e. the amount of data being created, the basic package for storing/running (hosting) the software on Heroku/AWS, was chosen by Lavabits. This package is sufficient to run the ferry booking application from and to keep maintenance costs down. Heroku/AWS only stores the amount of data that is input into the booking system, on a given day. Back-up of the Ferry Booking software is performed on a daily basis on the Heroku/AWS cloud platform servers. The current back-up plan being used by Lavabits, allows twenty-five (25) backups to be retained for any duration.

Observations

64. **Power Outages and Internet Access issues.** The following issues arise whenever there is a power outage or the internet access is interrupted, at the ferry terminals:

- passengers can only be checked in manually
- the agents will be unable to generate and issue any tickets or boarding passes
- only one-way manual bookings can be made as the agents at the other end will not have a record of the bookings.

- If the ferry agents were in the middle of a booking, they would have to resort to manually re-inserting passenger's details when they regain access to the booking software.
- The Antiguan Customs and Immigration personnel would have to process passengers manually, which is very time-consuming.

65. All of these issues can leave room for human error; result in delays of the ferry service; and indicate overall poor customer service.

66. **Cloud Hosting.** Lavabits utilises the services of Heroku/AWS Cloud for the hosting and storage of booking application. Therefore, there is no physical data centre as the Montserrat Ferry Booking application can be accessed at any time from any device that enables web browsing. The web page address for persons wanting to book and purchase ferry tickets online, is: *http://ferry.mniaccess.com*

67. **Health & Safety Risk due to poor environmental control issue.** On a normal basis, the solid concrete Montserrat Ferry Terminal is very hot, which tends to intensify at certain times of the day and especially in summertime. A very hot environment like this one can cause any one of the health related conditions, listed below, for both the ferry passengers (arriving and departing) and the ferry agents alike:

- heat exhaustion
- dehydration
- heat cramps
- heat strokes; and
- may cause or worsen existing health conditions (for e.g. heart problems, high or low blood pressure, respiratory conditions, and kidney disease)[1]

68. It would be beneficial to all stakeholders, in the long run, if the OotP and Access Division, and the Montserrat Port Authority jointly consider devising some measure(s) to alleviate or eliminate the heat problem. One way of accomplishing this, can be to localize the solution in the departure lounge area.

[1] *https://www.ccohs.ca/oshanswers/phys_agents/heat_health.html*

CHAPTER 6 APPLICATION CONTROLS

Input Controls

Online Travellers

69. It was noted that if errors are made during the online booking process, i.e. travel date and time, and destination, the traveller cannot go back and make changes once the ticket has been purchased; they will have to contact the Access Division.

70. The same applies to agents; if an error is made by an agent whilst making a booking on the spot, (for example, selecting the credit card payment option instead of cash) the agent cannot go back and change the mistake. The agent would have to cancel the booking and start anew. This cancellation would create a double booking for that passenger, which Lavabits has to retrieve and delete.

Authorised Users

71. There are proper user-specific access privileges and segregation of duties; the Access Division manages the levels of authorisation for the users, who input information into the Montserrat Ferry Booking application.

Booking Agents

72. The Online Booking Application is a relatively error-free application, for the most part, as it was designed with adequate input validation controls. Information is entered into the ferry booking software using Passport/Credit Card readers, and by clicking the mouse on:

- Drop down menus
- Text fields
- Contained buttons/Text buttons

73. There is not very much manual insertion of data, only when the agents (and sometimes the administrators) are conducting a search; or typing in a passenger's name, a booking confirmation number, and driver's license or social security card details, because the card readers cannot scan them.

Document Reader Scanners

74. For the electronic input of passenger information into the Ferry Booking system, 3M CR100 Document Passport Reader Scanners are used to scan/read passport, and credit card details.

Processing Controls

75. For high value transactions, credit card payments are conducted across Secure Socket Layer (SSL) standard security protocol. The Ferry Booking system uses the SSL technology to ensure all credit card payment data input by the document reader scanner:

(i) is encrypted and

(ii) is securely transmitted between the user's browser and the financial institution's web server.

Output Controls

76. The Montserrat Ferry Booking information output can only be modified or processed by authorised personnel from Lavabits, Access Division and the ferry agents. For example, posting of ferry schedules, status updates and messages, printing and issuing boarding passes, generating and printing of the various summary and detailed reports, etc.

Application Security

77. Access logs are created whenever an authorised user (i) logs in and (ii) do bookings (ii) check in passengers, print reports. Only Lavabits have access, and the authorisation, to disable or delete audit trails and this is simply not done.

78. The system is designed to send alert messages, via email, to the main developer at Lavabits of any security related issues. The users of the system are locked out until Lavabits resolves the issue. For example, recently the Lavabits' annual hosting licence expired and no one was able to log-in, until the developer renewed it.

Observations

79. **Privacy Policy**. There is a privacy policy on the Montserrat Ferry booking website, which stipulates the confidentiality of the data inputted by the traveller, how it is managed and handled by the Access Division.

80. **Card Readers issues.** A manager of one of the tour companies, indicated that if the passports are not swiped through the card readers with due diligence, the passport data entered would be fragmented and not legible. The agents would have to resort to performing manual searches via the passengers' confirmation number, which at times, slows down the checking-in process.

81. **Antigua Immigration mobile passport scanner issues.** An Antiguan Immigration Officer drew our attention to a problematic formatting issue that they encounter. The date on Montserrat driver's licences is in the American format where the month comes first, instead of the British way where the date is first and then the month. This causes confusion and inaccurate information to be documented if they had to scrutinize Montserrat passengers who use their driver's licence to travel on the ferry.

82. **Loss of Ferry Online Booking Information.** Once there is a power cut or loss of internet access, only the information that the agent was processing at the time, will be lost. Booking/checking-in transactions that were already completed would be stored in the database and be accessible once a refresh of the website page is done.

83. In the case of personal online bookings, it all depends on the customer's web browser and on which step of the booking process that the traveler lost internet connectivity. Some web browsers retain the user's history; therefore, if they lost the internet connection before the payment was successfully made they can simply refresh the browser and continue from the page where they lost the connection. They can also restart the booking process without being concerned of making double bookings. In addition, if a customer loses their internet connection after payment was successful, even if the browser does not retain the history, the application would have already sent them an email with their receipt and itinerary.

84. **Slow Immigration Processing issue at Antigua Ferry Terminal**. Over the years, there have been numerous complaints pertaining to the long delays caused by the very slow Immigration process at the ferry terminal in Antigua. Most of the complaints lodged, underscored the issues of long queues of disgruntled passengers and disruption to the ferry service. Reason for this is that the Immigration Department use mobile scanners to process ferry customers, which are very slow and are not geared towards processing large numbers of people. Secondly, these portable scanners require a reliable, high-speed, internet connection; the bandwidth of the communal Wi-Fi at the ferry terminal is very inadequate as the speed drops intermittently. Consequently, it can take quite a long time to process one passport depending on the internet speed.

85. As a result, the Immigration terminal checking system is not conducive for the smooth and expeditious processing of ferry passengers, in Antigua.

CHAPTER 7 IT OPERATIONS

Change Management

86. Any changes to the Montserrat Ferry Booking application will be documented via email and the change management software utilised by Lavabits. The Access Coordinator makes change requests, and gives the authorisation to fulfil the change requests, via email to Lavabits. There is usually no need for training after changes; however, if a new feature is introduced to the online booking software, Lavabits personnel would train the relevant users, how to use the feature.

87. There have been no emergency changes, to date, only modification of certain features, and the addition of new ones.

Problem & Incident Management

88. Lavabits have a very skilled incident person(s) with proper tools, resources, and to handle incidents. Their helpdesk hours are very flexible and they will respond to any requests or resolve any issues in a timely manner and according to the urgency of the issue or request.

Observations

89. **Continuous updates to Ferry Online Booking application**. Upgrades and maintenance of the Montserrat Ferry Booking application by Lavabits, is an ongoing process. It was also noted that since the current Access Coordinator took over the post, the following have been requested and executed:

- Upgrade of the user interface to speed up passenger booking and checking-in process, print boarding passes, etc., by reducing boarding process to fewer clicks of the mouse. There is very little need for manual input
- Update of the aesthetics look of the Montserrat Ferry Booking's Home page
- Abolishing the 'No Refund' policy.
- Resolution of booking and ticketing issues such as:
  - Ticket expiration time - if passengers should miss a booked trip, tickets are now valid for 12 months
  - Group tickets - if person or persons from a group are unable to travel on the booked day as the rest of the group, tickets will still be valid for a later travel date
  - Booking online times - passengers can no longer purchase ferry tickets online at the last minute, especially during the peak periods. They now have to book their tickets at least 1 hour before departure time
- Introduction of the Subscribe facility, for travellers to sign-up and receive special updates, offers, and promotions.
- Addition of the following reports:

  - Sales by Passengers (online bookings)
  - Refund
  - Passengers (number of people - specifically designed for DfID)
- At the commencement of this audit, Lavabits was in the process of updating the ferry booking application with the following features:
  - Ability of the agents to track cargo and the payments
  - Conduct Surveys after online booking/reservations
  - Allow an agent or travellers making online bookings, to change the date of a reservation or to cancel a ticket
  - Enable agents to scan boarding passes during the boarding process

90. **Frequent Review of User Account activity.** User activity information is not reviewed by Lavabits unless requested by Access Division. However, the Access Coordinator, who can access and review all user account information and generate reports for himself, attempts to perform this task twice a week, depending on the time of year.

CHAPTER 8 FINDINGS & RECOMMENDATIONS

91. Overall, the Montserrat Ferry Booking application has met the objectives that were initially outlined in Lavabits' May 2013 proposal document. The ferry booking application is web-based, user-friendly, and accessible from any electronic device that has access to the Internet, and/or from any data-enabled device. Lavabits continues to maintain the Montserrat Ferry Booking application; it constantly performs seamless updates and upgrades to the software, and proficiently performs any requested and approved amendments to the application, with very minimal downtime.

92. Access to, and the use of the Montserrat Ferry Booking Application, is determined on each user's job function or role (segregation of duties). All users, and user account privileges, must be approved by the Access Coordinator who also has the authority to terminate/disable user accounts. Audit trails/logs capture all of the authorised users' activities as soon as they login to the system using their unique user ID and password. All of the transactions or activities performed by the users, under their user accounts, are documented and traceable. These records span from the time the software was launched.

93. The majority of the application controls incorporated into the software, ensures and protects the accuracy, integrity, reliability, and confidentiality of the information that is inserted, processed, and outputted/produced by the booking application. They make sure that the initiation of the ferry passenger checking-in process and payment transactions are properly authorised, valid input data is processed, completely recorded, and accurately reported, etc.

94. There is no physical network to be monitored by Lavabits as the Montserrat Ferry Booking application's data is secured appropriately as it is stored and run from Heroku/AWS cloud platform servers. These overseas companies perform their own security monitoring and maintenance; to date, there have not been any internal or external IT-related security breaches or problems, associated with the Montserrat Ferry Booking application. Frequent and cumulative back-ups are performed by the Heroku/AWS Cloud computing platforms, on which Lavabits elected to have the Montserrat Ferry Booking application run and stored. If needs be, these backups are intended for business recovery purposes.

95. Although there were several findings noted by the OAG, we have pinpointed a few noteworthy concerns that we propose the OotP and Access Division, address as follows:

OUTSOURCING

96. **Establishing Standardised Service Level Agreements (SLA) or Contracts.** There was no SLA or formal contract in the initial developmental phases of the Montserrat Ferry Booking software project; the expert services of Lavabits was solicited by (the then) Access Coordinator, via a verbal agreement. To date is there no formal agreement that clearly states:

(a) Ownership of the Ferry Booking software

(b) Protection of, and access rights to, the data inputted and stored on the Montserrat Ferry Booking application and overseas servers.

97. There is only the recent Maintenance Agreement that Lavabits submits to OotP on an annual basis. OotP and Access Division therefore run the risk of abdicating or losing the

ownership of the software, which may be claimed by the service provider as their intellectual property. In addition, there is the inherent risk of loss of the Ferry Booking data, which resides with the developers of the application.

98. SLAs and Contracts are very important documents to have, especially when considering acquiring bespoke software from local or overseas software vendors or contractors. They are documented agreements between the organisation and the vendor to whom the services are outsourced and key tools to managing vendors. We therefore recommend that the GoM develop a standardised SLA and contract format that defines the services a vendor or contractor will be expected to accomplish, and the technical parameters for those services. Whatever items are critical to the GoM must be included in the SLA.

99. Typical areas would include, but not necessarily restricted to the:

- Types of services that will be performed by the vendor
- Allocation of responsibilities between the organisation and the vendor
- Services that will be measured, the measurement period, duration, location, and reporting timelines (defect rates, response time, help desk staffing hours, etc.)
- Time taken to implement new functionality, or re-work levels
- Intellectual property rights for the ownership of the software and the data rights
- Type of documentation required for applications developed by the vendor
- Location where services are to be performed
- Frequency of back-up, data recovery parameters
- Termination and data delivery methods and formats
- Incentive and penalty clauses

100. Secondly, the OotP and Access Division should strongly consider the creation of a Contract, or (if possible) the negotiation and re-drafting of the Maintenance Agreement, to affirm:

a) which of the involved parties have sole ownership of the ferry booking software.

b) that OotP and Access Division owns, and have access rights, to the Montserrat Ferry Booking data that was inputted and is being stored on the Heroku/AWS host servers.

c) the non-disclosure to, or the non-use by, third parties of any Montserrat Ferry Booking related material or the data that is being stored on the Heroku/AWS host servers.

101. **Acquisition of the Montserrat Ferry Booking application.** The OotP and Access Division is dependent on the services of Lavabits to maintain the ferry booking software. This is a high risk situation, as OotP and Access Division will be placed in a difficult position if Lavabits should fold, withdraws its services, or fails to provide the services outlined in this Maintenance Agreement. Consequently, it would be beneficial for OotP and Access Division to strongly consider the feasibility of purchasing the software, and maintaining it in-house, at the Department of Information Technology & e-Services (DITES).

102. Should this option not be accepted by Lavabits, then OotP and Access Division should ask for the software to be lodged in an escrow agreement where the source code is stored with

an independent third party or reputable escrow agent. Therefore, if Lavabits goes out of business, suspends, or withdraws its services (for whatever reason) then OotP and Access Division would have access to the source code enabling it to continue using the Montserrat Ferry Booking application.

103. **Institution of a Steering Committee.** For future GoM IT projects, we suggest that a Steering Committee be established with representation from DITES, Legal Dept., OotP, and other relevant stakeholders, to develop IT Outsourcing or Acquisition Policies and/or Standards. The document should identify and define, but is not limited to, the following:

- The functions that can be outsourced and what remains in-house (DITES)
- The roles and responsibilities between GoM and future vendors/contractors such as:
  - Development and acquisition of bespoke software
  - Draft and review SLA agreements between GoM and vendors/contractors
  - Monitor the initial and progressive stages of IT projects outline and goals
  - Address any issue in the SLA or contract between all involved parties.

BUSINESS CONTINUITY (BC) & DISASTER RECOVERY (DR)

104. **Need for Business Continuity (BC) and/or Disaster Recovery (DR) plans.** In terms of contingency, neither Lavabits nor OotP, Access Division, have a documented Business Continuity (BC) or Disaster Recovery (DR) plan.

105. A feasible reason why Lavabits do not have such documentation is that the online ferry booking application is web-based and it is stored and run from Heroku/AWS cloud platforms. These hosting companies ensure the security of the data, and have their own provisions in place for business continuity and disaster recovery.

106. However, we are still recommending that the Access Division and the OotP develop and implement their own BC and/or DR plan(s), in regards to the Montserrat Ferry Online Booking application. These contingency documentation should include provisions that facilitate the smooth transition of the online ferry services in the event:

- of extended power outage or loss of internet connectivity, in the aftermath of a natural disaster;
- if Lavabits folds or decides to suspend or withdraw its services

107. We also propose that the Access Division consider the feasibility of setting up an auxiliary server at the GoM's Department of Information Technology and e-Services (DITES), for the backup storage of the Montserrat Ferry Booking application's data.

INFORMATION SECURITY

108. **Poor Environmental Controls.** Some of the environmental controls at the Access Division and both ferry terminals are nonexistent, lacking, or substandard at best. There is a huge issue with heat at the Montserrat ferry Terminal; on the Antigua side, Jenny Tours office space is not equipped with any fire suppression implements or back-up generator. Both ferry

terminals require proper protection of their computer equipment against power outages and surges.

109. Consequently, we recommend that:

a. The Access Division, Montserrat's ferry terminal, and Jenny Tours office space, be equipped with surge protectors and heavy-duty UPS's for backup in order to protect the computer equipment in the event of electrical outages and surges.

b. Jenny Tours office requires a Carbon Dioxide (CO_2) or dry powder fire extinguisher. Their office is a minuscule wooden structure that houses a lot of paper and several pieces of electrical equipment.

c. Computers have to be kept in a specific environment to function efficiently. Conditions such as intense heat can damage and lessen the performance of a computer. Therefore, there is the risk of the hot computer equipment (laptop, PC, scanner readers, and printer), running slower, and prolonged exposure to the extreme temperatures at the Montserrat ferry terminal will eventually damage and shorten the lifespan of the hardware. The damage caused would be irreparable.[2]

[2] *https://smallbusiness.chron.com/temperature-affect-performance-computer-components-28197.html*

CHAPTER 9 CONCLUSION

110. From this Information Security (IS) study, we the Office of the Auditor General concluded that the Montserrat Ferry Booking application is very secure and robust with adequate policies and procedures and application, logical, and physical access controls in place to ensure the accuracy, integrity, and security of the ferry booking software and the data inputted and stored on it.

111. However, we surmised that there is much room for improvement in a number of areas that were highlighted in Chapter 8.

CHAPTER 10 MANAGEMENT RESPONSE

112. The findings and recommendations in Chapter 8 are duly noted and management will seek to secure resources to progress implementation in a phased manner, as considered in the matrix below:

No	Timeline	Recommendation No and Short Description
1	**Immediate** (0-3 months)	112a - Equipping PC equipment in Agency Offices with surge protection devices.
2		112b - Equipping Antigua Agency Office with fire extinguisher
3	**Short Term** (3-12 months)	102 - Sign-off Service Level Agreement with Contractor
4		103 - Create a Contract or re-draft Maintenance Agreement
5		109 - Develop Business Continuity and Disaster Recovery Plan
6		110 - Setup auxiliary server at DITES for back-up storage
7		112c - Cooler environment at Montserrat Ferry Service Agency terminal
8	**Medium Term** (1-2 years)	104 - Acquisition of Ferry Booking software application

113. Management extends appreciation to the Office of the Auditor General for the conduct of this Special Audit, Information Security Audit of the Montserrat Ferry Online Booking Application.