REPORT

ON

GOM E-Governance Initiatives -

MONTERRAT ONLINE VISA APPLICATION (MOVA)

Prepared by

OFFICE OF THE AUDITOR GENERAL
BRADES, MONTSERRAT
OCTOBER 2015

OUR MISSION

“The OAG 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”.

GoM E-GOVERANCE INITIATIVES - MONTSERRAT ONLINE VISA APPLICATTION (MOVA)

REPORT

This report has been prepared under Section 103(1) of the Montserrat Constitution Order 2010 for presentation to the Legislative Assembly in accordance with Section 103(2) of said Constitution.

Florence Lee
Auditor General
Office of the Auditor General
October 2015

TABLE OF CONTENTS

ABBREVIATIONS USED

API	-	Application Programming Interface
AWS	-	Amazon Web Services
BCP	-	Business Continuity Plan
CGI	-	Common Gateway Interface
CSS	-	Cascading Style Sheets
DRP	-	Disaster Recovery Plan
DfID	-	Department for International Development
DITES	-	Department of Information Technology and E-Government Services
EC$/XCD	-	Eastern Caribbean Dollars
GL	-	General Ledger
GoM	-	Government of Montserrat
HTML	-	Hyper Text Manual Language
IDI	-	INTOSAI Development Initiative
IRD	-	Inland Revenue Department
IT	-	Information Technology
ISSAI	-	International Standards for Supreme Audit Institutions
MySQL	-	My Structured Query Language
MTB	-	Montserrat Tourist Board
PFMAA	-	Public Finance Management and Accountability Act
PFMAR	-	Public Finance Management and Accountability Regulations
MOU	-	Memorandum of Understanding
MOVA	-	Montserrat Online Visa Application
OAG	-	Office of the Auditor General
RBC	-	Royal Bank of Canada
RMPS	-	Royal Montserrat Police Service
SAI	-	Supreme Audit Institutions
SLA	-	Service Level Agreement
SSL	-	Secure Service Layer
TCF	-	Treasury Consolidated Fund
TDP	-	Tourism Development Plan

AUDITOR GENERAL'S OVERVIEW

The Government of Montserrat in seeking to build a strong successful economy has introduced a number of public sector reform initiatives which emphasises the need for a more efficient and effective public service. Some of these initiatives focused on the use of providing e-government services by using information and communication technology systems to facilitate easier and timely accessibility of service.

One of the services introduced was an online visa application server where eligible persons could obtain an e-visa to enter Montserrat. In keeping with my constitutional mandate, I authorised a review of the MOVA service. The purpose of the review was to determine whether appropriate systems, policies, procedures, and controls were in place to mitigate all associated risks of operating the online system.

The review revealed weaknesses in the MOVA control environment as policy documents to guide outsourcing of IT services, business continuity planning and disaster recovery are non-existent. Moreover, the management of the MOVA services is being provided without a signed contractual arrangement which is contrary to existing procurement regulations and there is no documented service management agreement. We have provided several suggestions for addressing these matters.

Our report is intended to assist GoM in strengthening its IT systems. It is therefore critical that management carefully review the recommendations in this report with a view toward adopting the measures outlined and thereby strengthening its overall control systems.

Finally, I wish to thank all the persons who provided information and/or extended courtesies to my staff during the course of this audit.

Florence A Lee, CPA, BSc, MSc
Auditor General

EXECUTIVE SUMMARY

The Government of Montserrat (GoM) is seeking to improve the services it offers to its customers. It seeks to do this by making the provision of public services more efficient and thus is placing more focus on the use of technology to aid in making some services more readily accessible to the public. It therefore embarked on reducing the turnaround time for persons seeking visas to enter Montserrat and payment of resident permits by expats, by using available technology to implement an online visa application service – the Montserrat Online Visa Application (MOVA).

This pilot study covered the period 2010 - 2014. It sought to assess what Outsourcing, BCP/DRP, IT Security, Application Controls, and IT Operations measures that: **(i)** the Department of Information Technology and e-Services (DITES), has implemented for contracting an outside entity/company to provide services for GoM **(ii)** the contractor and/or DITES have implemented to ensure that MOVA is able to operate at some defined capacity after a natural disaster or man-made disruption **(iii)** DITES and/or contractor have protected MOVA and the computing hardware it runs on, from unauthorised modification, theft, accidental or intentional damage and/or destruction **(iv)** ensure that all users of the MOVA system are properly identified and are authorised to access the software to either carry out their assigned duties or the information being inputted/outputted, is correct **(v)** contractor and/or DITES is effectively delivering the service parameters and performance indicators and requirements laid out in a Service Level Agreement (SLA) or a contract, pertaining to MOVA.

MAIN FINDINGS

We observed the following findings in areas such as:

I. Outsourcing

The GoM does not have any outsourcing policy that defines what functions are to be outsourced and what must remain in-house. Nor do they have Service Level Agreements (SLA) and/or contracts.

The GoM did not prepare/create either document outlining the services parameters, performance indicators, and requirements, it expected from Lavabits. Only the contractor drafted a combined SLA/contract, in which the entity retained all rights pertaining to and ownership of the MOVA software, source code and background technology. The drafted document was never signed by the GoM. This unsigned cum SLA/contract, does not include a data rights clause to stipulate ownership, access to, or protection of, the data inputted into MOVA and is currently being stored on Lavabits' overseas servers.

This is a very high risk issue as should the contractor fail to maintain the software, goes out of business, or folds, GoM does not retain business knowledge or ownership of the business process(es), or the data.

II. BCP/DRP and IT Policies

GoM has no published/approved Business Continuity Policy (BCP) or Disaster Recovery Policy (DRP) in place, with clearly defined training requirements and testing schedules. Nor does it have any IT policy documentation concerning the contingency operation of MOVA. The contractor Lavabits, themselves, does not have any either.

In addition, there is no back-up site with the appropriate environmental and physical control mechanisms devised and put into place for MOVA, in the event that the Immigration Department has to evacuate its current office space.

III. Information Security

The environmental and physical controls in place, at the Social Security building that houses the Immigration Department's office space, are adequate. There have been no reports either of any incidents/security breaches to MOVA from the contractor's side, since its initial debut in 2012.

IV. Application Controls

There are adequate input/output validation controls in place, which ensures that the data being input/output is accurate, reliable and complete when accepted by MOVA, in a timely manner.

MOVA's information is properly protected and secured against misuse via segregation of duties, different user roles, and access rights, available for each user profile.

V. IT Operations

Although the contractual agreement between the two parties is unsigned, the operation of MOVA is in full effect. The SLA/contract that Lavabits drafted was geared mainly towards the development and implementation of MOVA, not post-MOVA functionality.

Service reports, maintenance, and user/application response time is adequately maintained by Lavabits.

OUR RECOMMENDATIONS

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

- ❖ DITES and/or GoM should develop a clear outsourcing policy that documents the IT functions that are to be outsourced and what remains in-house. It/they should identify and define all the roles and responsibilities between GoM and future vendors/contractors. This includes an SLA that defines the services the vendor/contractor will be expected to accomplish, and the technical parameters for those services, i.e., whatever items critical to the GoM must be included in the SLA.

- An updated/new SLA and/or contract between DITES and Lavabits must be drafted and signed, which gives DITES sole ownership of the data collected and stored on MOVA overseas servers.
- DITES should assess the feasibility of purchasing the software and maintaining it, in-house (within central government agencies). Should this option not be accepted by the supplier, then DITES should request that the software be lodged in an escrow agreement where the source code is stored with an independent third party. If the supplier goes out of business or withdraws its services and/or source code, then DITES would have access to the source code enabling it to continue using this software.
- GoM and/or DITES, does not have BCP/DRP or IT Security Policy documents relating to MOVA. It is recommended that management develop and test various working practices, procedures, policies and controls necessary for the security of MOVA's data and the smooth operation of the Immigration Department in the event of a natural disaster or other disruption.

CONCLUSION

The Office of the Auditor General found areas that were deficient. From the findings of the review, the most pressing concerns were the unsigned cum SLA/contract, the lack of IT Outsourcing Policies and/or Standards, and the non-existence of Business Continuity or Disaster Recovery Policies. We made recommendations to address these issues thereby making the systems and controls more robust.

We note that the main users of the IT system are the RMPS and IBSU units. Thus, some of the recommendations were highlighted to them for their consideration of the best course of action.

CHAPTER 1 INTRODUCTION

1.1 Background

The Government of Montserrat (GoM) is seeking to improve the services it offers to its customers. It seeks to do this by making the provision of public services more efficient and thus is placing more focus on the use of technology to aid in making some services more readily accessible to the public. It therefore embarked on reducing the turnaround time for persons seeking visas to enter Montserrat by using available technology to implement an online visa application service – the Montserrat Online Visa Application (MOVA).

1.2 Management Responsibility

Management is responsible for ensuring that appropriate policies and effective controls exist to guide the facilitation of MOVA services. More specifically, management must ensure that policies exist to facilitate IT governance and to guide development and acquisition of IT products, IT operations, outsourcing of IT services, information security, business continuity planning and disaster recovery planning. Management is also responsible for establishing appropriate IT controls and for ensuring that they function effectively.

1.3 Auditor's Responsibility

Our responsibility is to independently express a conclusion on the operations of the MOVA system based on our audit. Our work was conducted in accordance with ISSAI 100 and 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.

1.4 Audit Mandate

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) 2008 and the Public Finance Management and Accountability Regulations (PFMAR) 2009.

1.5 Audit Standards & Guidelines

The standards and guidelines used to assess the MOVA system included the use of ISSAI 1, 100, 3100, 4100, together with the IDI Handbook for IT Audits.

1.6 Audit Objectives

GoM has implemented several internet based or related technologies with the intention of improving the performance within the public sector. As with any project, there will be a number of risks involved. The risks associated with this pilot IT audit encompass concerns such as:

- given that this is a bespoke IT package, there is a risk that the service would be discontinued should person(s) and/or entities in charge, cease to operate or services are terminated
- a virus infection resulting in the corruption of the data and hence no reliance on the data
- loss of personal data leading to non-reliance on the data, possible legal liabilities and reputational risks
- hacking of systems, misuse of data and possible contingent liabilities

Therefore, bearing in mind the above risks, the purpose of this pilot IT audit is to provide assurance that GoM has a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) process that ensures that MOVA is able to continue providing services and that adequate security measures are in place to protect data.

Consequently, the main aim of this pilot IT audit is to determine what impacts does the chosen application, have on the government services. That is, to assess and determine if:

(i) adequate controls exist to ensure security of sensitive/personal information and

(ii) provisions were made by the GoM to ensure continuance of these services if person(s) and/or entity maintaining the application and system should leave or if their services were terminated.

1.7 Audit Scope and Methodology

The pilot audit is focused on assessing the policies, procedures, and controls that guide outsourcing, operations, business continuity, and security of e-government services provided by Department of Information Technology and e-Services (DITES). Emphasis will be placed on assessing the programme implemented by the Tourism & Immigration Departments and the Cabinet Secretariat over the period 2010 - 2014.

The audit will include a review of relevant policy documents; enquiries of management regarding operational tenets, defined benefits, performance indicators or milestones set at onset of the programmes; discussions held with stakeholders to seek feedback on the programmes; and analysis of the information collected.

CHAPTER 2 E-GOVERNANCE IN MONTSERRAT

2.1 Objective of the Audited Entity

The Government of Montserrat (GoM) embarked on an E-Government program with a mission to modernise the public service. This was based on a premise of creating a connected government, improving operational and decision making processes, achieving efficiencies, and building a good governance structure[1]. It was felt that there was need for, among other things:

- increased efficiency and effectiveness of the public service
- modernised and integrated business systems of GoM and
- Improvement in the delivery of services to citizens and other stakeholders.

GoM focused on the use of Information Technology to drive its modernisation plan across the public service. For purposes of this assignment, the audited entity is being regarded as central government agencies - Ministries and Departments.

2.2 Organisational Arrangements

Montserrat is a British Overseas Territory, with a Governor and a locally elected government led by the Premier. There is a Cabinet and a Legislative Assembly with nine elected members including four ministers of government. The Attorney General and the Financial Secretary sits in both bodies to provide technical guidance and support.

GoM is comprised of 4 main portfolios, each of which consists of numerous departments (*see appendices for last updated organisational chart - Appendix 1)*:

- Ministry of Finance, Economic Development, Tourism & Culture
- Ministry of Communications, Works, & Labour
- Ministry of Education, Health, Community Services, Sports & Youth
- Ministry of Agriculture, Lands, Housing, Environment & Ecclesiastical Affairs

2.3 Budget and Nature of Information Technology (IT) Activities

An annual budget is provided to all government departments. In order to formulate ICT strategies and engage in the delivery and support of world class IT and e-Government services across GoM, the Department of Information Technology & e-Services (DITES), received the following approved estimated/revised budgets over a 4-year period, spanning from 2010 - 2014. Among other things, this includes purchasing of IT equipment (hardware and software), professional services and fees (consultation), and maintenance services (licences). The budgets are quoted in Eastern Caribbean dollars (EC$).

[1] *"A Model of Good Governance", e-Government Strategy, Volume 1, Ramesh Gupta, 2010*

2010/2011	-	1,569,500.00
2011/2012	-	2,315,200.00
2012/2013	-	2,697,000.00
2013/2014	-	1,252,200.00

2.4 Significant IT Activities in the Last 3 - 4 Years

Investment in IT facilities, systems and processes is essential for achieving GoM's goal of providing effective and efficient E-Government services. To that end, Government has upgraded and/or replaced several pieces of hardware across the public service. Several desk and laptop computers were replaced making it relatively easier to complete work. Networking equipment was replaced and aging servers and data storage devices were upgraded. Moreover, government has embarked on a project to replace and or expand its fibre optic infrastructure island wide. This was damaged by volcanic activity which destroyed two-thirds of the island in the mid to late 1990's.

2.5 Name of Application Used

Some entities procured hardware and/or upgraded software to enable faster and more efficient services. This includes, but is not limited to, geographical information systems, audit management software, revenue collection and administration software, visa management, management of Cabinet documents, and performance development and review software. As can be clearly seen, the GoM has undertaken a range of activities to modernise its services and to create value-added services. For purposes of this study however, we will focus only on the Montserrat Online Visa Application (MOVA) introduced by the GoM to improve visa services being delivered to visitors and tourists.

2.6 Functions Performed by the MOVA Application

The Montserrat Online Visa Application (MOVA)[2] was part of a governmental initiative. It was part of their strategic growth plan in conjunction with the Department for International Development (DFID). In the Memorandum of Understanding (MOU)[3] between GoM and DFID, MOVA was the 11th milestone[4] that fell under the Immigration Policy and Tourism sector. Initially, the online visa feature was the sole option of the application; the resident permit feature was an addendum months after MOVA was launched.

MOVA (which later included the Resident Permit Extension), has been operational since September 2012 where potential visitors/tourists to the island of Montserrat, and expatriate property owners, can apply and pay for their visas and resident permits online.

[2] https://www.immigration.ms/

[3] http://www.gov.ms/wp-content/uploads/2012/05/MOU-Reforms.pdf

[4] http://www.gov.ms/wp-content/uploads/2012/05/STRATEGIC-GROWTH-AND-DEVELOPMENT-REFORMSCOMMITMENTS.pdf

The previous system entailed applicants from certain African, Asian, European, Middle Eastern and South American countries who required a visa to enter Montserrat, to apply at the nearest British Consulate. If the application was approved, the visa was stamped in their passport for a maximum period of three (3) months. This process was a lengthy one and more than likely an expensive one, for those who had to travel from their home country to the nearest British Consulate.

Consequently, the purpose of MOVA was to:

a. eliminate and replace the old system of going to a British Consulate to submit a visa application to obtain a visa to visit Montserrat
b. speed up the process of issuing visas and resident permits
c. make the application process more convenient and less costly to applicants
d. Provide a means to attract and increase the number of tourists/visitors to the island, as per the MOU.

A **Montserrat eVisa** is equivalent to a conventional visa, but no paper is inserted into the applicant's passport. Applications for eVisas are submitted online, verified online, and in most cases, they are approved and issued online within 24 hours. Anyone with a valid passport who wishes to enter Montserrat, as a visitor or on business is eligible to apply. In certain cases, where an invitation letter or other supporting documents are necessary to obtain an eVisa, applicants will be informed via the email address they provide in the online application form.

A **Resident Permit** is a permit which is granted to non-nationals, who are owners of property in Montserrat. Applicant(s):

- must be the owner of property in Montserrat
- is not a national of Montserrat
- must have documentation of property ownership

Payment options for eVisa and resident permits include via credit card and/or walk-ins at the Immigration Department - this form of payment applies only to resident permits. The application fee for both the online visa and online resident permit is USD$50.00. Once either type of application has been submitted, it is processed and issued within 24 hours. Both the eVisa and the resident permit are valid for one (1) year. Once granted, they are delivered electronically as attachments to the email address the applicants have provided.

Walk-ins pay EC$100 for their Resident Permits at the Department of Immigration, where the Immigration Officer issues the permits straight away. They are given a handwritten receipt and the transaction is also written up in a log book. Applicants are given a year extension for the permits. They have to return on the same date the following year to renew their resident permit.

Property owners that live abroad are not required to pay for a resident permit if they stay on the island for less than 12 months, i.e. a few weeks to a few months, or come and go several times a year. When they arrive at the airport, once they can prove a short length of stay, they will be given up to the maximum time of 6 months by the Immigration Officers.

The service of a local software company, Lavabits, was solicited by the GoM, to develop and implement the MOVA application. They were formally contracted and given a $20,000.00 Eastern Caribbean (EC) dollar budget to complete the project within 7 – 9 week time frame. The Resident Permit feature was added shortly after, via a verbal contract between the GoM and Lavabits, with an EC$8,000.00 budget. Lavabits charges annual fees of EC$720.00 to host MOVA on their server and EC$530.00 for Secure Socket Layer (SSL) certificates.

CHAPTER 3 DEVELOPMENT AND MANAGEMENT OF ONLINE VISA PROCESS

3.1 GoM and the Department for International Development (DfID)

The online visa concept was the 11th strategic major reform milestone and partly the brainchild of a representative from DFID. He contended that the online visa system would help, *"...meet the Strategic Growth Programme plans of increasing tourism development and facilitating easier access for travellers..."*.[5]

The online visa project was spearheaded mainly by the DfID representative, along with the Director of Department of Information Technology & e-Government Services (DITES). Other government officials who were part of the planning process included the head of the Montserrat Royal Police Service (RMPS) & Immigration Departments., the (former) Premier of Montserrat, and the (former) Cabinet Secretary.

The main requirements for the online visa application[6] were to:

- ❖ enable anyone who needs to travel to Montserrat, from one of the countries identified as requiring a visa to be able to apply online (*see Appendix 5 for list of countries*)
- ❖ receive a response within 24 - 48 hrs via email
- ❖ permit applicants to make one-time credit card payment online

The GoM's Reform Growth Matrix Action Plan timeline scheduled the implementation of a pilot online visa system by 1st September, 2012, under the Immigration Policy (*see Appendix 2 for the actual progressive target dates that were scheduled*). Amendments were made to the Immigration Act[7]to facilitate the processing online visa applications.

3.1.1 Operational Statistics

In MOVA's first year of operation, the following table below represents the application's report card status for the period 1 September, 2012 - 30 April, 2013:

Total Number of Visa Applications	46	Average Application Processing Time	26.3 hrs
Number of Approved Visa Applications	45	Longest Processing Time	265.25 hrs
Number of Declined Visa Applications	1	Shortest Processing Time	0.02 hrs

[5] http://www.gov.ms/2013/05/14/montserrat-online-visa-service-making-it-easier-for-travellers/
[6] https://www.immigration.ms/tourists/guide
[7] http://agc.gov.ms/wp-content/uploads/2011/10/Immigration-Act1.pdf

Further operational statistics for MOVA from 2012 to present (as at April 2015) indicate that the highest number of applications, by nationality, was from the Syrian Arabic Republic. The shortest processing time is still 0.02hrs. The overall audience review from November 2014 - April 2015. USA & UK rank in the top two (*refer to Appendix III & IV for operational statistics*)

3.2 Department of Information Technology & e-Government Services (DITES)

At the inception stage of the project, DITES was devoid of capable in-house software programmers. Therefore, the decision was made to outsource to a fledgling local software development company, Lavabits, in July 2011.

The initial plan was for the online visa application to be installed and run from a DITES server. Consequently, the Director of DITES managed and coordinated the project by maintaining constant consultation and disseminating information with the outsourced software development company, the Commissioner of Police, and other relevant personnel via phone calls, emails and internal meetings. DITES did the groundwork for the setting-up of the e-commerce bank account at the local branch of the Royal Bank of Canada (RBC), where all credit card payments would be deposited. They submitted to Lavabits the requisite information received from the bank for the facilitation of secure online credit card payment on the MOVA website. This included a link to their Plug n Play Application Programming Interfaces (APIs), login ID, password, and ecommerce presentation, checklist and Common Gateway Interface (CGI) options. However, subsequent conflict between Lavabits and the Director of DITES resulted in MOVA being launched and maintained by Lavabits, instead, on an independent server. Either party has refrained from commenting on what the issue(s) was/were, between them.

The Director of DITES has administrative rights to MOVA and receives email notifications of visa and resident permits applications and credit card payments. However, he does not have the authority to approve or decline visas or resident permits. He is the main person responsible for adding/deleting users and assigning access rights to them.

The Director revealed that there have been a few allegations of credit card fraud from applicants, which have gone uncontested and the monies refunded because no visa or permits were granted in these instances.

3.3 Treasury Department

The payments made for visa applications are deposited into a credit card/merchant account at RBC. There are five signatories on the bank account and two signatures are required for transactions. The bank account is not exclusive to MOVA and payments made to the account are not listed individually. Treasury Consolidated Fund (TCF) deposits and payments made to MOVA are lump summed. Payments are reconciled monthly, the process is as follows:

- ❖ Extract MOVA transactions from the TCF account.

- Reconcile balance of General Ledger (GL) to TCF bank statement.
- If amounts reconcile, create journal entry.
- Debit bank & credit income account.

Monies collected from MOVA online payments remain on the TCF account at RBC, no withdrawals are made. Money in the account is posted as revenue to Treasury's GL and cash book via journal voucher. Postings made can be viewed in SmartStream.

There were previous issues with online payments where payments were made in XCD (Eastern Caribbean Dollars) instead of USD. This glitch continued for approximately 12 months but has since been corrected.

3.4 Montserrat Tourist Board (MTB)

The online visa project was funded by the Tourism Development Programme 2 (TDP2)[8] that set out to improve the marketing and promotion of Montserrat, the development of an on-island infrastructure and product, visitor facilitation and improvement of its tourism industry standards. The MTB paid Lavabits from their marketing and advertising account:

- For the development of MOVA the total amount of EC$20,000 in four equal installments of EC$5,000.
- A total amount of EC$5,250 was paid for the installation of a wired network for MOVA, at the new Immigration Department office location
- The total amount of EC$8,000 was paid in two equal instalments for the insertion/addition of the alien Residents Permit feature extension to the MOVA website
- An additional payment of EC$530 was paid to Lavabits for a SSL certificate for the MOVA website

3.5 Immigration Department/Integrated Border Security Unit (IBSU)

The Immigration Department[9] (or the IBSU) falls under the umbrella of the Royal Montserrat Police Service (RMPS). It is responsible for the regulation and monitoring of all ports of entry/exit in Montserrat, which includes processing of online visa applications.

Initially, ten (10) Immigration/Police Officers were handpicked by the Commissioner of Police (CoP) to be trained by Lavabits to use and manage the MOVA application; that is to be approvers and/or back end users of the system. Twenty-four (24) Police/Immigration Officers in total (including the Commissioner and Deputy Commissioner of Police) were trained and given the roles as Administrator/Immigration Officer.

[8] http://www.gov.ms/2012/02/28/design-of-phase-3-of-the-montserrat-tourism-development-plan-2012-2015/
[9] http://police.gov.ms/departments-beat-7-patrol/core-policing/immigration/

The specified time frame for processing of visa is stipulated at 24 - 48 hrs, excluding weekends. Although the Immigration Officer can review the applications from home or anywhere once there is access to the Internet, visa applications are not processed on weekends except in very urgent/pressing instances.

3.6 Lavabits

3.6.1 Online Visa Application Proposed Specifications

When the GoM contracted Lavabits, the company drafted a proposal for an application called Online Visa Application System (OVAS), which was subsequently, renamed MOVA. The proposed functionalities for this system were:

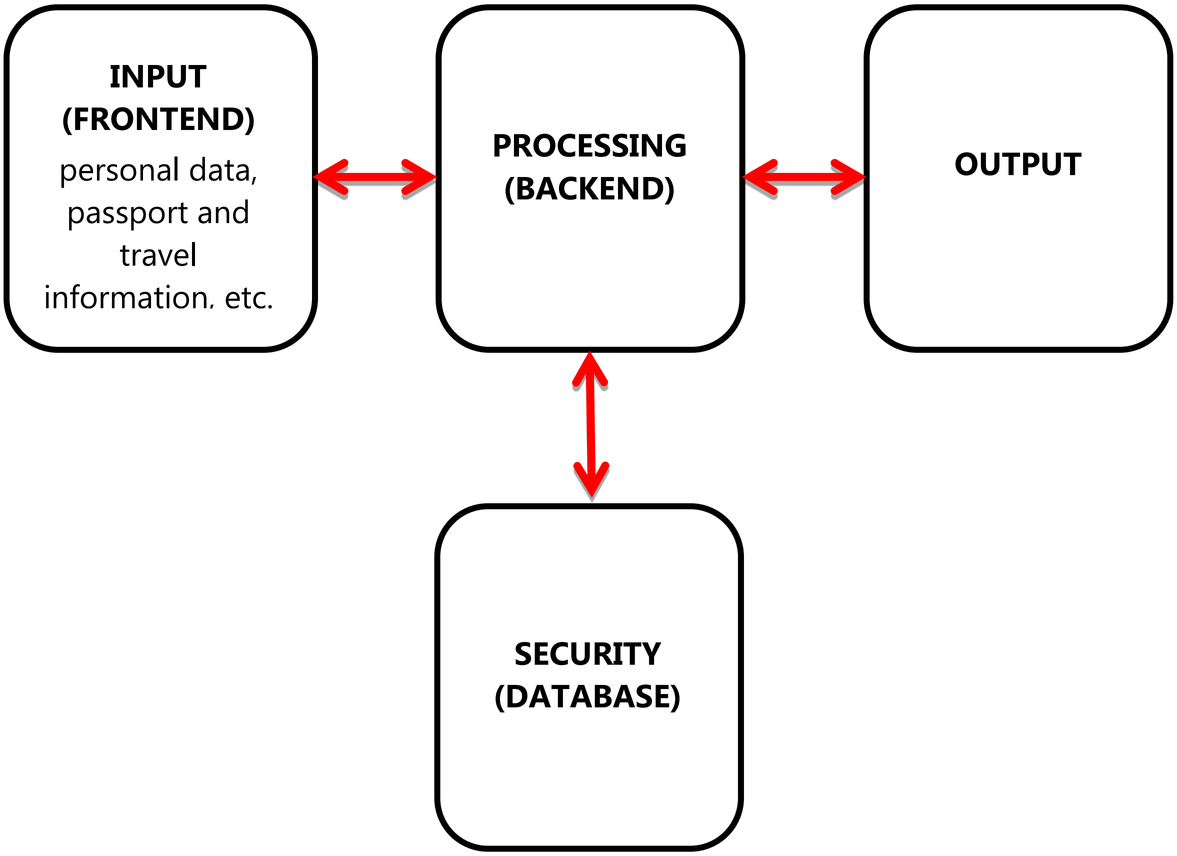
- online application for visas
- facilitation for online payment
- facilitating storage and retrieval of applications
- a back end for the administration of visa applications

The online visa application consists of three main components, that is, a front end that is seen and used by the applicant in the form of a digital application form; a back end that is seen and used by the Immigration officer processing the visa applications; and a database.

1. **Front End** - that will be seen by the applicant. The front end would consist of pages as follows:
   - Preliminary Visa Requirement
   - Check Terms and conditions
   - Application number
   - Personal information
   - Passport information
   - Contact information
   - Travel information
   - Payment Review
   - Thank you.
2. **Back End** - seen and utilised by the Immigration Officer/Administrators processing the online visas, as follows:
   - Log in
   - Urgent applications
   - Applications
   - Applicant
   - Issue Visa

3. **Database** - This stores and retrieves the visa application data.

COMPONENTS OF MOVA SYSTEM



3.6.2 Implemented Specifications for MOVA

The chronological specifications/requirements for the MOVA software that Lavabits implemented are as follows:

- Website with instructions and application forms and other information
- Applicant visits website and reads instructions and other relevant information
- Applicant fills in the online form
  - Form can be saved before final submission for up to 14 days
- Applicant hits the submit button
- Applicant is taken to the payment page
- Applicant enters Credit Card details
- If Credit Card rejected
- Application is saved in the Visa Application database and tagged as 'Not-Paid'
- Visa Application notification sent by email to the Applicant's email address
- Online form shows 'Application not Forwarded.....Please resubmit CC payment'

- If Credit Card accepted
- Online form shows 'Application Forwarded'
- Application is saved in the Visa Application database and tagged as 'Paid'
- Visa Application notification sent by email to visa processing department
- Application Confirmation email is sent to Applicant's email address
- Visa Application acknowledged by visa processing department
- Visa application status is set to; 'processing'
- Visa Application is processed by visa processing department
- Visa Application is Accepted or Rejected by visa processing department
- Visa application status is set to; 'Accepted', 'Pending' or 'Rejected'
- If 'Accepted', Notification is emailed to the Applicant with an attached confirmed visa for travel to Montserrat
- Visa can also be downloaded online
- If 'Pending', Notification is emailed to the Applicant informing them that further information is required and specifying what additional information should be sent
- If 'Rejected', Notification is emailed to the Applicant informing them that the application was not successful
- Successful Visa Applications are valid for 1 year after acceptance

3.6.3 Maintenance

A 4-week testing week period after the system was launched was required to resolve any technical issues (free of charge), after which Lavabits contractual obligations would be fulfilled and completed. An extended maintenance package would be offered after the contract expires.

If the GoM wanted Lavabits to commence with the MOVA project straightaway, they were required to:

a. sign the contract/Software Development Agreement Lavabits submitted

b. provide Lavabits with 25% of the EC$20,000 fee being charged.

3.7 Proposed Resident Permit Extension System

Processing of Resident Permits[10]was an extension made to MOVA. This extension was requested by the GoM and Lavabits submitted a proposal on 10th May 2013 to have it completed and the MOVA system updated, no later than in 5 weeks.

The purpose of the module would be to enable expats who own property on, and/or live on Montserrat, an easy way to pay for their Resident Permits. Applicants populate the required fields with their personal, passport, contact, travel, and property/parcel number information. The issuing process is similar to that of the online visa. Once the application

[10] http://www.gov.ms/2013/10/25/montserrat-resident-permits-available-online-as-of-november-1st/

is submitted and paid for via online credit card payment, the applicant will receive an email from the Immigration Department within a 24 - 48 hour time frame.

The resident permit will either be granted or declined:

- ❖ If **granted** - the resident permit will be attached in an email.
- ❖ If **declined** - no reason is given in the email.

The charge/fee for the online resident permit application like the online visa is a one-time payment of US$50, which under normal circumstances, is usually non-refundable.

3.7.1 Proposed Resident Permit Extension Specifications

The Resident Permit extension was to be added to the MOVA system as a module with three main components:

1. **Front End** - that will be seen by the applicant. The front end would consist of pages as follows:
   - Preliminary Visa Requirement
   - Check Terms and conditions
   - Application number
   - Personal information
   - Passport information
   - Contact information
   - Travel information
   - Payment Review
   - Thank you.
2. **Back End** - that the administrator(s) uses
   - Log in
   - Urgent applications
   - process Applications
   - Issue Visas
3. **Database** - This stores and retrieves the visa application data.

3.7.2 Development Schedule

The development schedule Lavabits proposed for the Resident Permit extension was for 6 weeks. There was a 6-week gratuitous testing period after the system was launched, in order to iron out any technical issues. After which, Lavabits were no longer obligated to the terms of the contract.

The development progress of the MOVA software was reported in stages in the form of presentations and hands on demonstrations. These presentations were conducted three times to representatives from DfID, DITES, Police and Immigration departments.

If the GoM wanted Lavabits to commence the extension project immediately, they were required to:

a. sign the contract/Software Development Agreement Lavabits submitted

b. provide Lavabits with 50% of the EC$8,000 fee being charged.

3.7.3 Maintenance

Maintenance of the extension was offered for only after the contract was fulfilled and the new module would be hosted along with the existing MOVA system.

3.8 Banking/Online Payment

The GoM has an e-Commerce merchant bank account at the local branch the Royal Bank of Canada (RBC), where all the online payments for the online visas and resident permits, are deposited.

RBC is responsible for the processing and storage of the customers' credit card information; it does this via third party plug and play.

When the applicant pays for either service via his/her credit or debit card:

- their details are sent to the plug and play
- plug and play charges the card
- plug and play informs MOVA if payment is successful or not. Applications will be declined if there is no money on the applicant's credit/debit card.

The bank provides the Treasury Department with monthly bank statements, of all MOVA online transactions.

3.9 MOVA Website Technical Implementation

The MOVA website is run off a server, with a ruby framework that automatically generates the web pages. Ruby, separates the pieces of the website (e.g. navigation and content), combines 'on the fly' and dynamic content (e.g. database access), and integrates with the static component of the website. Cascading Style Sheets (CSS) are utilised to allow for more flexibility within the design of the website. CSS makes it easy to conduct any future updates or changes while preserving the Hyper Text Manual Language (HTML) content.

3.10 Database

MYSQL database is used for storage and retrieval of the visa application data.

3.11 Network Infrastructure

A. Lavabits

MOVA is not run from a physical server. Lavabits opted to store MOVA on rented servers with cloud platforms from USA-based companies Amazon Web Services (AWS) and Heroku. Therefore, Lavabits does not have a physical office building/space or physical computer equipment with hardwiring.

B. GoM

MOVA is accessed by the processing Immigration officer(s), from a tower desktop PC linked to a switch infrastructure.

The network at the Social Security building serves the Immigration Department and other GoM departments housed there. It is comprised of only one switch. This switch is connected to the main network at DITES via a fibre optic, which runs from the Social Security Building in Little Bay to the DITES server room at the Government Headquarters in Brades.

3.12 Mova User Manual

3.12.1 Back End User Procedures

Lavabits provided a user manual that outlined the back end user procedures for the person(s) processing online visa applications. The approved duties that the back end users of the MOVA system can perform, falls under the following headings:

- Users
- Applications
- Visas
- Payment
- Countries
- Settings
- Access Permissions

3.13 Observations

1. Some of the trained officers no longer work in the department or with the GoM.

2. In November 2014, when the main Immigration Officer went on vacation, the replacement officer could only see the applications but could not approve them. Consequently, the stand-in had to ask the Deputy Commissioner of Police to process and grant the visas.

3. If a technical issue arises (for example, if an applicant cannot see the visa as approved or is unable to print the visa from their end), the main Immigration Officer would call Lavabits to get the issue resolved. The problem is usually resolved in a few hours.
4. The Commissioner and Deputy Commissioner of Police have administrative rights to MOVA, they can approve, reject, and override approved visas and resident permits.
5. The Acting Director of Customs & Revenue Service, also has administrative rights to MOVA

CHAPTER 4 OUTSOURCING

4.1 Outsourcing Policy

An outsourcing policy would define what IT functions can be outsourced and what should remain in-house. At the inception stage of the MOVA project, DITES was devoid of any capable in-house software programmers; consequently, the outsourcing option allowed GoM a level of flexibility in dealing with its core IT services in-house whilst soliciting external assistance to develop and introduce the online visa service.

The GoM has no formal and/or documented outsourcing policy, or any list highlighting the services that could be outsourced or any clear approval process for the outsourcing of a function/service. There are no documents to record that GoM has identified the risks associated with different modes of outsourcing or to verify that the organisation is aware of the risks associated with the possibility of takeover, closure or withdrawal of Lavabits' services.

4.2 Solicitation

The decision was made by the committee that spearheaded the MOVA project, to outsource a fledgling local software development company, Lavabits, in July 2011. They were approached directly with the project by the DfID representative.

4.3 Service Level Agreement (SLA)

The Software Development Agreement drafted by Lavabits, is a combined SLA and contract. However, to date, this agreement is unsigned by the GoM.

4.4 Vendor or Contractor Monitoring

Lavabits' Software Development Agreement, adequately outlined provisions and parameters in the clauses, which the GoM could have utilised to monitor/manage Lavabits and taken appropriate action if their performance or quality of work was not acceptable.

The provisions and parameters included:

- the plan and schedules it would implement pre- and post- MOVA development project plan
- payment terms and conditions and penalty for services rendered and for the development of MOVA
- terms and conditions and penalty for changes in project scope, testing of software and training
- payment terms and conditions and penalties for the maintenance and support post-MOVA
- ownership of software, background technology, and source code for MOVA

- other clauses that include: warranties, relationship of the parties, limitation of developer's liability, non-solicitation of developer's employees, confidentiality, term/termination of agreement, meditation and arbitration, attorney fees, complete agreement, governing law, assignment and signatures.

4.5 Retaining Business Knowledge/Ownership of Business Process

There is no clause in SLA/contract that states ownership of business process. It only states the terms and conditions for use of the source code, only if/when one or more incident(s) arises to render Lavabits incapable of providing support and maintenance services to MOVA.

Use of the source code is restricted, as outlined in the agreement.

4.6 Observations

1. The contract has not been officially signed by the GoM, simply because Lavabits does not know which entity and/or person, to submit their Software Development Agreement to. Due to the non-execution of the SLA/contract, it is an "inferred" contract, where although it is not signed, it is operable for a given time frame. The ramifications of an unsigned contract could present litigation risks with non-adherence to procurement regulations.
2. As per clauses 17 - 19 of the Software Development agreement, Lavabits retains all rights pertaining to and ownership of the MOVA software, source code and background technology. GoM has to seek written consent from Lavabits to use, the background technology for any other commercial use. Overall, this could pose as a high risk issue for the GoM, as it has plans to commercially share MOVA with other British Overseas Territories.
3. GoM does not retain ownership of the business process(es). The SLA/contract states that they will receive a contingent licence from Lavabits to use the source code in machine readable form only, to support the use of MOVA software. The issuance of the licence is contingent on if Lavabits:
   - goes out of business
   - fails to maintain the software
   - becomes insolvent /admits insolvency or is unable to pay off their debt
   - files for bankruptcy or
   - is controlled by a rival customer
4. Although MOVA is in current operational use, the software's source code is still held and owned by the developers. The staff of DITES and the Immigration Department cannot make any changes to it. Although this may appear on the surface as a good

control mechanism, it poses several high risks associated with the developer maintaining control over the software.

- ❖ Firstly, there is the risk of delays in processing applications when difficulties with the functionality of the software are encountered.
- ❖ Secondly, continuous upgrades may prove costly, as this is bespoke software, that is, it is not a software package where regular updates can be purchased off the shelf.
- ❖ Thirdly, there is a risk of continued availability of support or supplier failure that would lead to loss of software use and negatively impact the processing of visas.

5. There is an inherent risk of loss of data which resides with the developers of MOVA.
6. The SLA/contract drafted by Lavabits is geared more towards their own advantage. Hardly any provisions were made for the benefit of GoM.
7. There is no clause in SLA/contract that states ownership of, protection of, and access rights to, the data inputted/stored in MOVA. It only sets out the terms and conditions for ownership of the background technology and the ownership of the software and source code only.

4.7 Recommendations

1. DITES, with guidance from the policy directorate, should consider developing a clear outsourcing policy that documents the functions that can be outsourced and what remains in-house. They should identify and define all the roles and responsibilities between GoM and future vendors/contractors.
2. We suggest that DITES develops an SLA that defines the services the vendor/contractor will be expected to accomplish, and the technical parameters for those services; whatever items critical to the GoM must be included in the SLA. Typical areas would include:
   - 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 to implement new functionality, rework levels
   - 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

3. An updated/new SLA and/or contract between DITES and Lavabits needs to be drafted and signed by DITES/Cabinet Secretariat. The document(s) must give DITES sole ownership of the data collected and stored on the MOVA oversea servers.
4. With respect to risk of supplier failure, we recommend that DITES should assess the feasibility of purchasing the software and maintaining it, in-house (within central government agencies). 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. If the supplier goes out of business or withdraws its services and/or source code, then DITES would have access to the source code enabling it to continue using this software.

4.8 Management Response

Have not received a response to date.

CHAPTER 5 BCP AND DRP

5.1 Business Continuity Policy/Disaster Recovery Policy

GoM has no published/approved Business Continuity Policy (BCP) or Disaster Recovery Policy (DRP) and IT policy documentation in place, with clearly defined training requirements and testing schedules.

5.2 Testing the BCP/DRP

No tests/drills or mock-ups have been conducted.

5.3 Back-Up and Disaster Recovery for Outsourced Services

Lavabits, themselves, do not have any published/approved Business Continuity Plan (BCP) or Disaster Recovery Policy (DRP) in place or IT policy documentation, concerning the contingency operation of MOVA. The main reason being that DITES does not have such documentation for them to adhere to.

Secondly, Lavabits does not have a physical office space; neither do they have any physical computer equipment with data on it to maintain. MOVA is run and maintained on cloud platforms servers provided by US-based companies Heroku and Amazon. Heroku and Amazon are responsible for any security breaches into their servers. No breach has occurred to date. However, logs are kept for 7 days of all requests made to MOVA, for e.g., hackers making unauthorised requests to MOVA.

5.4 Environmental and Physical Controls

There is no back up site with the appropriate environmental and physical control mechanisms devised and put in place for MOVA if the Immigration department had to evacuate their current office space.

5.5 Recommendations

1. DITES needs to formulate, establish and test BCPs/DRPs, and/or an IT Policy, in regards to MOVA.

2. The Integrated Border and Security Unit needs to conduct a Business Impact Assessment and put in place backup plans to facilitate smooth transition of services in the event that Lavabits folds, or decides to withdraw its services for whatever reason.

5.6 Management Response

Have not received a response to date.

CHAPTER 6 INFORMATION SECURITY

6.1 Physical & Environmental Security

6.1.1 Social Security Building

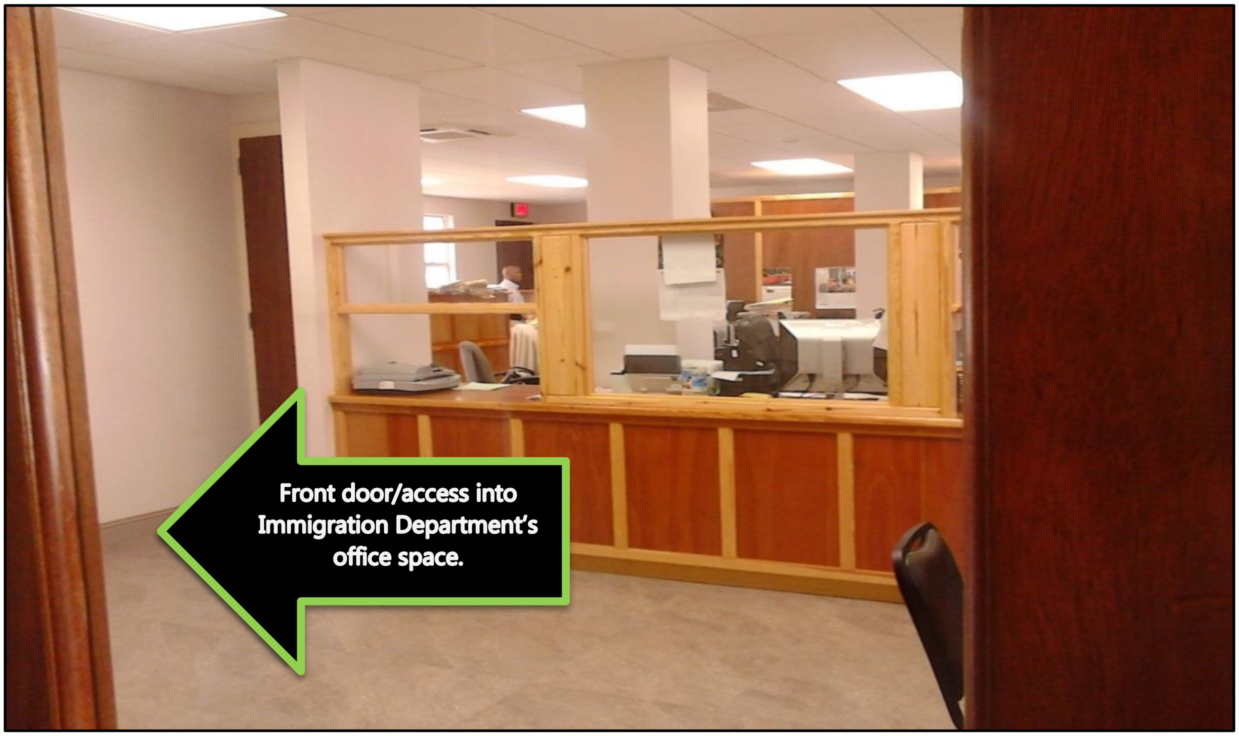
A walkthrough of the Social Security premises that houses the Immigration Department office space was conducted and the following control parameters in terms of building structure, UPS, fire protection, humidity, temperature and voltage, flood protection, etc., were observed and assessed:

- The Social Security building that houses the Immigration Department office space is a new building that was completed in January 2013. This building was constructed using Montserrat Building Code and Guidelines[11], (which is only a draft code since early 1990s and has yet to be passed by Montserrat's Legislative Assembly). It is a combination of American, British, Caribbean Uniform Building Code (CUBIC) and other ad hoc building standards and codes.
- Building is steel reinforced with a structural steel roof
- Roof is covered with 22" gage galvalum and is sloped in order to promote adequate run off
- Has 8" drainage guttering that runs around the circumference of the roof that drains rain water into catch pits to duct covered drains
- The entire parking lot (to the sides and back) for the building, is a drainage system for the rain water that falls on it or runs down from a solid stone embankment on the east side. The water is lead through duct covered drains, into rectangular trench drains, to the northern side of the building.
- Above the stone embankment (to the east) is an earth drain that traps water that soaks into earth/ground and would potentially drain/run down the face of the solid stone embankment onto the parking lot. The water instead, drains down into a stepped open drain and runs under a culvert beneath the road, down to the sea.
- Under the galvalum, is thermal insulation which prevents direct external heat from sun, to be transmitted into the rooms/spaces below.
- Building is properly grounded via multiple earthing points that are covered with protective earth mats, all around its perimeter.

[11] http://cidbimena.desastres.hn/pdf/eng/doc5536/doc5536-introduccion.pdf

6.1.2 Immigration Department Office Space

Access into the Immigration Department, is through/via the IRD office space. The Inland Revenue Department (IRD) and the Immigration Department are located on the ground floor.


Front door/access into Immigration Department's office space.

Front Area of Inland Revenue Department (IRD) Office

6.1.3 Environmental Controls

1. Water Damage and Dust

a. Building Structure

Inside the Immigration Dept. office space there are no signs of leakage outside or inside of building:

- no water bubbles in paint or peeling paint
- no mildew
- no water stains on ceiling paneling, walls, floorboard skirting, or window ledges
- no cracks in the walls
- no oozing moisture out of the walls

b. Windows

The windows are dust and impact resistant, double hung, replacement windows that are quarter inch (¼") thick. Consequently, no outer hurricane shutters are required

2. Temperature

a. Ventilation

Ventilation is mechanical (a/c units). The entire building has an air conditioning system that each office space can control the climate to their comfort level. A small vent is installed in the office space ceiling and the temperature is controlled via an a/c thermostat on the rear wall.

b. Direct sunlight

The windows are usually kept closed during working hours due to the climate controlled air conditioning. However, there are no curtains or protective shades/blinds against the direct rays of sunlight. Consequently, the Immigration Officer has taped large white sheets of paper to the windows (on the inside), as a means to stave off the direct rays of sunlight on her person and the computer equipment. The windows had been measured for blinds (over a year ago), but they have not been delivered or installed to date.

3. Fire Prevention

a. Smoke Detectors

The entire building interior is outfitted with smoke detectors and fire alarms. However, within the Immigration Department there is only a single smoke detector installed in the ceiling; there no fire alarm in the office space.

b. Fire Extinguishers

Furthermore, there is no sign of any class of fire extinguishers (A, B, C or D) in either the IRD, or Immigration Department. These Government departments rent their office spaces from Social Security and it is government's policy that each department or office is responsible for outfitting their own spaces with fire extinguishers.

c. Sprinkler System and Fire Hose

The building has no sprinkler system or fire hoses

d. Fire Drills

No fire drills have ever been conducted.

4. Backup Power Source

The building has a communal standby 3-phase current diesel generator, which is a more stable supply of current for when there is a power outage.

There is no Uninterruptible Power Supply (UPS) in case the generator does not start. The computer that Immigration officer uses to access MOVA is only plugged into a standard power surge strip.

6.1.4 Physical Access Controls

a. Entry/Exit

The Immigration Department's office is a narrow space, 780 sq. ft. in size, with two heavy wooden paneled doors (possible) fire doors with narrow, rectangular, glass vision panels. One leads into the room from main IRD outer reception area, the other into the IRD inner office space. The main office/reception area entrance door is a fire exit that leads into the Social Security building lobby area and so is the back door inside the IRD internal office space that leads out into the rear parking lot area. The two doors of entry/exit into the Immigration dept. office space, the front door (public access) and the back door (staff access) are locked with keys only; so are the all of the doors in the IRD.

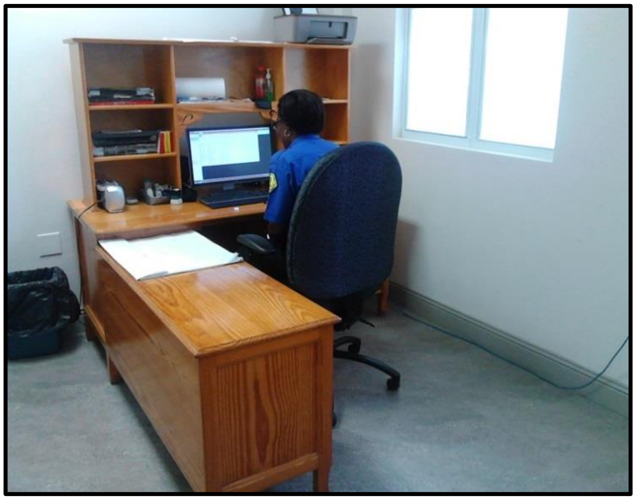
b. Roof/Ceiling

There is no crawl space between the floor above and the office space ceiling area for intruders to access and/or hide.

The ceilings are comprised of acoustical paneling that are suspended by wires to reduce sound being transmitted from the upper office spaces, floors. The spaces between the floors above and ceilings are not big, or sturdy, enough to accommodate or bear the weight of an adult. Each space would be less than 1 foot high. The office ceilings are not interconnected either, so there can be no freedom of movement between the office spaces laterally or perpendicularly.

c. Windows

The windows are usually kept closed during (and after) working hours, due to the climate controlled air conditioning. They are not armed with an alarm system.



Back door leading into IRD office space

Immigration Office Space where Online Visas and Resident Permits are Processed

6.2 Software Access Controls

Access Control policy

There is no access control policy pertaining to the MOVA software, but there are certain procedures in place that ensures access to government offices and access to MOVA, is authorised:

- ❖ There is an access control list of authorised users who are required to sign-in to MOVA, using a unique user ID and password.
- ❖ Access requested is commensurate with job function/role and segregation of duties. There are also clearly defined requested roles and/or privileges that are mapped to the job functions of the users (Administrator or Immigration Officer).
- ❖ Access to, and authorisation to, perform certain tasks in MOVA is assigned by the Director of DITES, who is the Chief Administrator.
- ❖ Physical access into IRD and Immigration Dept., are through front and back doors, locked with keys.

6.3 Data Security

Although there are no BCP/DRP to ensure security of data, MOVA, hardware and Immigration Dept., office space/Social Security building, MOVA and its data are secured appropriately. MOVA is stored and run from Amazon and Heroku cloud platform servers. To date, there has not been any known case of breach of security on the cloud platform servers. Access control logs are automatically generated as soon as anyone logs into MOVA, with their unique user id and password.

Backups are done on a weekly basis by Heroku and Amazon. However, there are no local back-ups done of the MOVA information/data and application by DITES.

6.4 Risk Assessment

The perceived internal and external threats pertaining to the overall security of MOVA and its information/data, were identified, analysed, and evaluated, which resulted in the following assessments:

- ❖ There is an inherent risk of loss of business knowledge which resides with the developers of MOVA. The drafted contract clearly defines the terms and conditions of the business arrangement in Lavabits favour. This is a high risk issue.
- ❖ There no local back-up servers of the web application by the developers as it hosted on two overseas servers (Amazon &Heroku) which is medium-low risk area.
- ❖ The physical and environmental security of the building is adequate; the risks are very low.

- ❖ Access control to MOVA is a low to medium risk. OAG was not able to assess/analyse any status reports, as Lavabits did not provide the department with requested documents. However, according to Lavabits and DITES, to date there has never been any security breaches.

6.5 Observations

1. Current control system regarding door keys, require that keys for all of the government departments are kept at the police station and only a few authorised members of staff from each dept., can sign for, and will receive, the keys outside of normal working hours.

2. There are no security guards on the premises during the day or at nights. Neither the interior, nor exterior, of the entire building is being monitored by CCTV.

3. The Immigration Officer does not have a set of keys for IRD's front doors and the officer is not sure if she is one of the authorised signatories. The officer indicated that should she need to access the office after normal working hours, she would contact one of IRD's authorised signatories to sign for and collect the keys on her behalf.

4. MOVA is efficient and reliable within the parameters of its purpose. There have been no reports of any incidents/security breaches to MOVA since its initial debut in 2012.

5. User logs that capture user id, date & time, etc., for security audit trails are created

6. Upgrades and maintenance to MOVA application is automatic;

7. Back-up is constant on the Amazon &Heroku cloud platform servers.

6.6 Recommendations

1) Physical access by staff in both IRD and Immigration Dept. should be controlled via swipe or key cards.

2) There should be a local backup server for the data stored on MOVA, in the event that Lavabits folds or withdraw their services, or if Heroku or Amazon servers go offline or breach of security.

3) The physical and environmental securities of the building are adequate; however we recommend that the Immigration Office space be equipped with:

- ❖ a proper surge protector and UPS back-up in case of electrical outage and the standby generator does not start-up.
- ❖ at least one Carbon Dioxide (CO_2) fire extinguisher

6.7 Management Response

Have not received a response to date.

CHAPTER 7 APPLICATION CONTROLS

7.1 Input Controls

A. Online Applicant

In the first phase of the online visa application, it has to be determined whether or not a visa is required to enter into Montserrat. As per the input conditions, specific criteria are required for applicants that need a visa for online processing checks:

- If visa is required, the inputted data is stored on the database server.
- If none is needed, applicants are not required to fill out the form nor will their information be stored on the database server.

Once the applicant's credit/debit card information and number are accurate:

- the payment transaction will be instantaneous and
- applicant's credit card information will be secure

B. Immigration Officer/Authorised Personnel

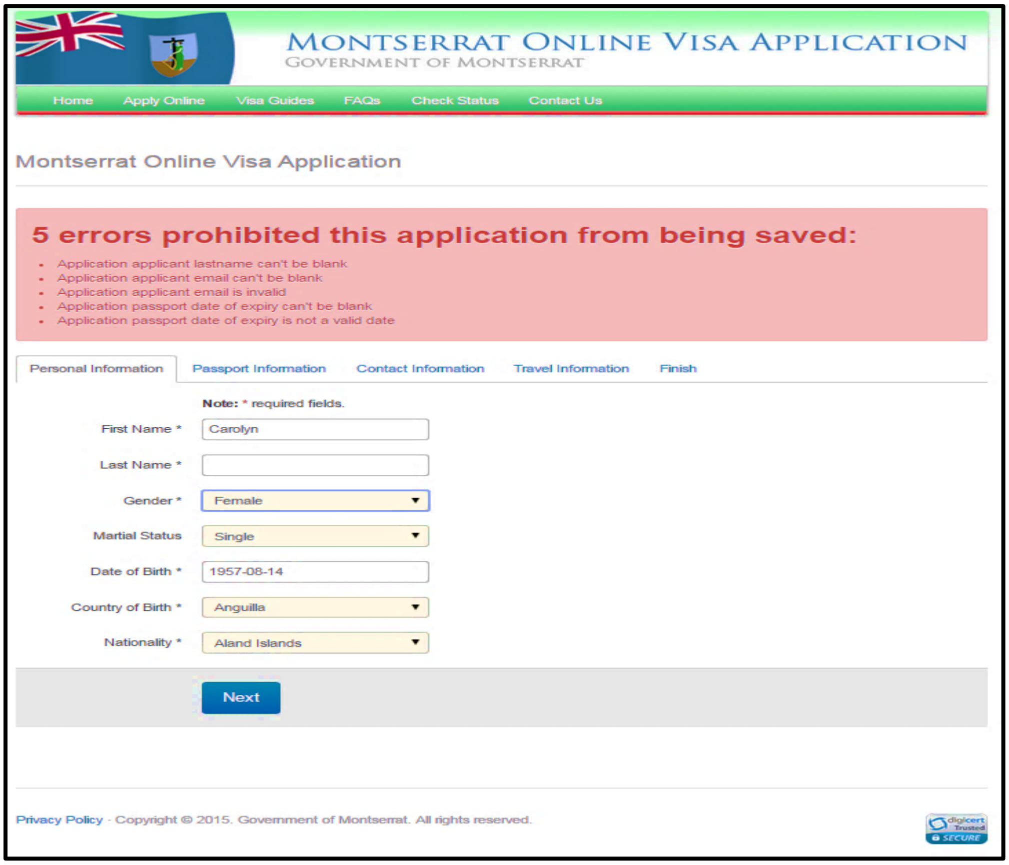
In order to review, authorise approval, or denial of online visas/resident permits, the processing Immigration officer or authorised person has to access the MOVA database via the online access point *www.immigration.ms*.

Login requires a unique user id and password.

7.2 Error Handling

A. Online Applicant

If specific criteria is not inputted into the required fields, when the online forms/applications are submitted a red message text box field will show the specific error(s) that need addressing.



Montserrat Online Visa Application

5 errors prohibited this application from being saved:

- Application applicant lastname can't be blank
- Application applicant email can't be blank
- Application applicant email is invalid
- Application passport date of expiry can't be blank
- Application passport date of expiry is not a valid date

Note: * required fields.

First Name *	Carolyn
Last Name *	
Gender *	Female ▾
Martial Status	Single ▾
Date of Birth *	1957-08-14
Country of Birth *	Anguilla ▾
Nationality *	Aland Islands ▾

Privacy Policy - Copyright © 2015. Government of Montserrat. All rights reserved.

B. Database Server

Errors are non-existent, as the MOVA database is constantly being updated on the Heroku & Amazon cloud platform servers. These servers are maintained on a regular basis.

C. Data Entry

DITES is the entity that manages/controls the authorisation levels for transactions within MOVA. There are proper user-specific access privileges and segregation of duties as there only two user roles of duties (Administrator and Immigration Officer). Not all Immigration Officer user roles have user permissions to issue visas/resident permits and to reject applications.

The applicants' data and information inputted are properly protected. There is a privacy policy (*refer to Appendix V*), which stipulates the confidentiality of data inputted by the applicant and how it is managed and handled by the Immigration Department.

7.3 Processing

Generally, there is data integrity, validity, reliability and completeness throughout the transaction processing cycle, except for when an unexpected interruption occurs. The applicant(s) would need to re-enter all of their information.

If necessary, the Immigration Officer can access the MOVA database when away from the office via the internet using a desktop, laptop, or handheld device.

7.4 Output

Information is in the form of messages, emails and issued visas with unique identifiers. They can only be viewed and accessed by either the applicant or Immigration Officer.

There is a privacy policy which stipulates the confidentiality of data inputted by the applicant and how it is managed and handled by the Immigration Department.

7.5 Application Security

Access logs are created whenever an authorised person or Immigration Officer (i) logins in and (ii) process application forms. Only Lavabits have access, and the authorisation, to disable or delete audit trails.

Storage of the data input by applicants' in the online application form is on the cloud platform servers. DITES receive notification every time someone submits an online application form. When successful applications are submitted they are given a unique ID number which is sent to both applicant, and Immigration officer who will process the online applications.

For high value transactions, the credit card payments are processed by e-commerce plug & play application from Royal Bank of Canada (RBC), which is on their secure servers. These servers are based off-shore in Barbados, and only RBC can promptly review these payments in detail.

7.6 Observations

1. There are adequate input validation controls for data being keyed into the MOVA software, by both the applicant and authorised personnel. The controls in place ensure that the data being inputted is accurate, reliable and complete when accepted by MOVA in a timely manner.
2. MOVA has adequate procedures for error handling
3. MOVA operations run according to the parameters in the design flow.
4. Information output by MOVA is complete and accurate before further use.
5. The applicants' data and information are properly protected.
6. MOVA's information is properly secured against misuse as there are audit trails of all of the application's processes and user activity. These series of records capture login activity, any modifications/edits, overrides, unauthorised access, etc.

CHAPTER 8 IT OPERATIONS

8.1 Service Management

DITES does not monitor the IT operations of MOVA neither do the responsibility for the Quality of Service (QoS) of MOVA (helpdesk, application level support and troubleshooting, and maintenance). These all fall under Lavabits, as MOVA is not run on DITES' servers.

The GoM has no BCP standards for data back-up and recovery practices. However, Lavabits performs a weekly backup of the database.

There is no formal Software Development Agreement between Lavabits and GoM. The draft provided by the contractor is outdated and unsigned to date.

8.2 Compliance

The SLA/contract that Lavabits drafted was geared mainly towards the development and implementation of MOVA. There are no operational parameters aside from maintenance of software clauses 12, 13, 14 and 15, where Lavabits is to:

- provide a minimum of 3 years' support and error-correction service after the 6 months warranty expired
- timely payment of annual maintenance fee of $2,000 in quarterly instalments
- prompt error reporting by Immigration Department, in writing.

8.3 Capacity Management

In terms of Capacity Management, support and error-correction services for MOVA are handled by Lavabits. Lavabits ensures that sufficient resources and appropriate tools are utilised to handle network monitoring and help desk functions, and the personnel involved are proactively engaged in addressing bottlenecks while remaining responsive to business needs.

DITES only provides the Immigration Department with access to the GoM's network.

8.4 Observations

1. Although the contractual agreement between the two parties is unsigned, the operation of MOVA is in full effect. Service reports, maintenance and user/application response time is adequately maintained by Lavabits.

2. The SLA/contract that Lavabits drafted was geared mainly towards the development and implementation of MOVA, not post-MOVA functionality

3. Error reporting is made mainly through phone calls to the developers.

8.5 Recommendations

1) DITES should request that quarterly status/service and/or incidents reports, on functionality of the MOVA application, are provided from Lavabits

8.6 Management Response

Have not received a response to date.

CHAPTER 9 CONCLUSION

The Office of the Auditor General found areas that were deficient. We made recommendations for DITES, RMPS and IBSU, to consider and to take the best course of action. From the findings of the investigation, the most pressing concerns were no Outsourcing Policies and/or Standards in place and the unsigned cum SLA/contract.

DITES do not have any Outsourcing standards and/or policies for the development and acquisition of IT products or IT services from outside entities or vendors, or for the management of these entities or vendors. Organisations need to have some form of policy that outlines functions that are to be outsourced and functions that must remain in-house.

SLAs contain the specific requirements and operational parameters of the entity that solicits the services of external service providers, and can be a key tool to managing these vendors. It defines the day-to-day technical parameters that the vendor/contractor is to adhere to, or the services it expected to provide, at that level. The contract defines the overall requirements for the effort and any associated security or other requirements to be followed. Both are legally binding agreements between the outsourced entity and the soliciting organisation. Consequently, the vendor/contractor can be managed and held accountable to the terms of service agreed upon in the signed contract and/or service level agreement. However, there is no signed SLA, or formal contractual documentation, between GoM, and the outsourced contractor Lavabits.

DITES should take the initiative to have this issue resolved as soon as possible to avoid the possible loss of ownership of the MOVA business process(es) as the software’s source code is still being held and owned by the developers, Lavabits.

We noted the absence of Business Continuity, Disaster Recovery and IT Security polices and guidelines. The lack of these policy documents weakens the governance and management of the IT systems.

REFERENCES

Documents

A Model of Good Governance, e-Government Strategy, Volume 1, Ramesh Gupta, (2010)

WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions 2014

Websites

http://agc.gov.ms/wp-content/uploads/2011/10/Immigration-Act1.pdf

http://cidbimena.desastres.hn/pdf/eng/doc5536/doc5536-introduccion.pdf

http://www.gov.ms/2012/02/28/design-of-phase-3-of-the-montserrat-tourism-development-plan-2012-2015/

http://www.gov.ms/2012/03/23/budget-statement-201213-securing-a-sustainable-future-for-montserrat/

http://www.gov.ms/wp-content/uploads/2012/05/MOU-Reforms.pdf

http://www.gov.ms/wp-content/uploads/2012/05/STRATEGIC-GROWTH-AND-DEVELOPMENT-REFORMSCOMMITMENTS.pdf

http://www.gov.ms/wp-content/uploads/2012/06/Draft-Final-Report-6-July-2012.pdf

http://www.gov.ms/publications/SDP_MONTSERRAT.pdf

http://www.gov.ms/2013/05/14/montserrat-online-visa-service-making-it-easier-for-travellers/

http://www.gov.ms/2013/10/25/montserrat-resident-permits-available-online-as-of-november-1st/

http://www.immigration.ms

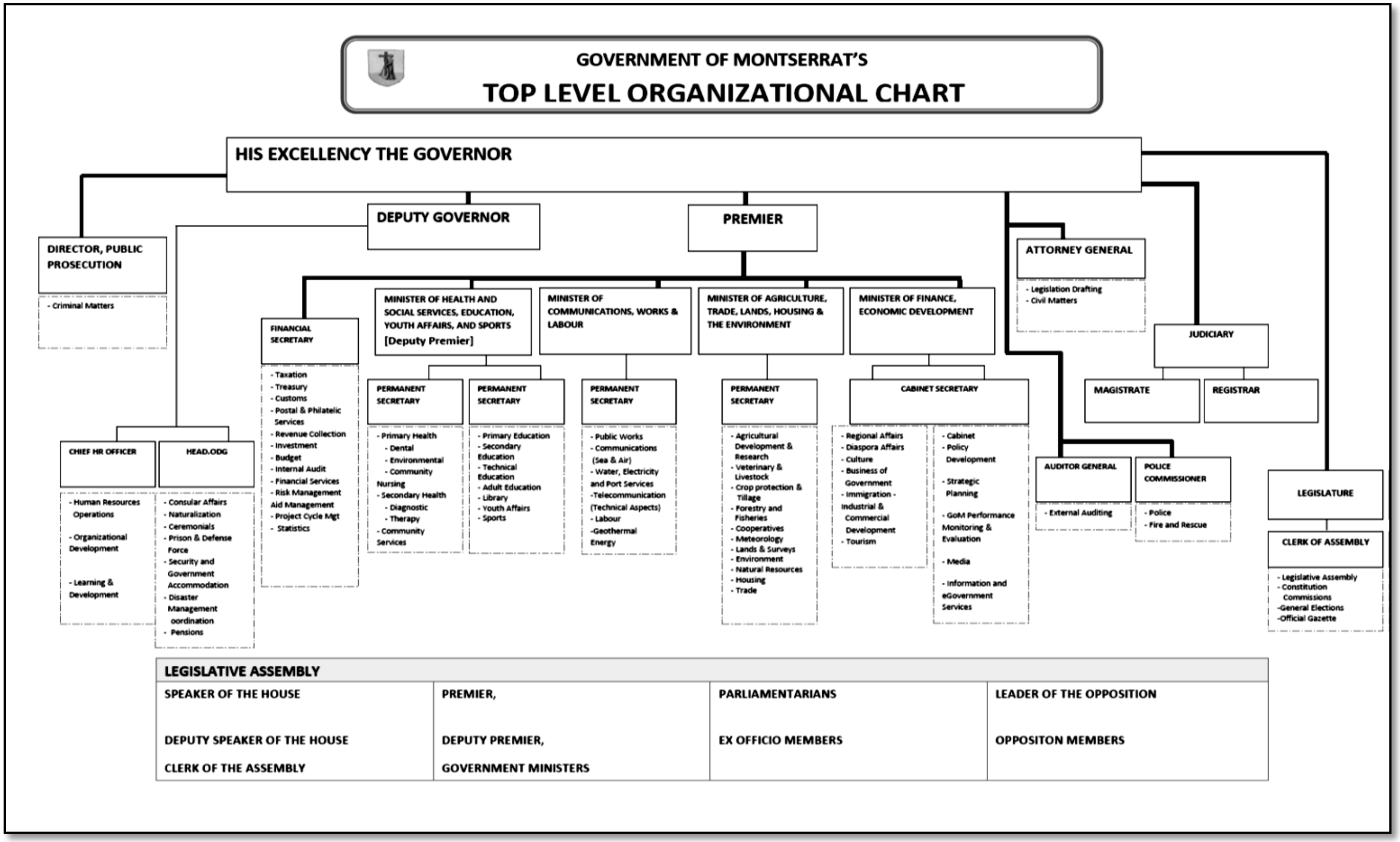
https://www.immigration.ms/tourists/guide

http://www.lavabits.com

http://police.gov.ms/departments-beat-7-patrol/core-policing/immigration/

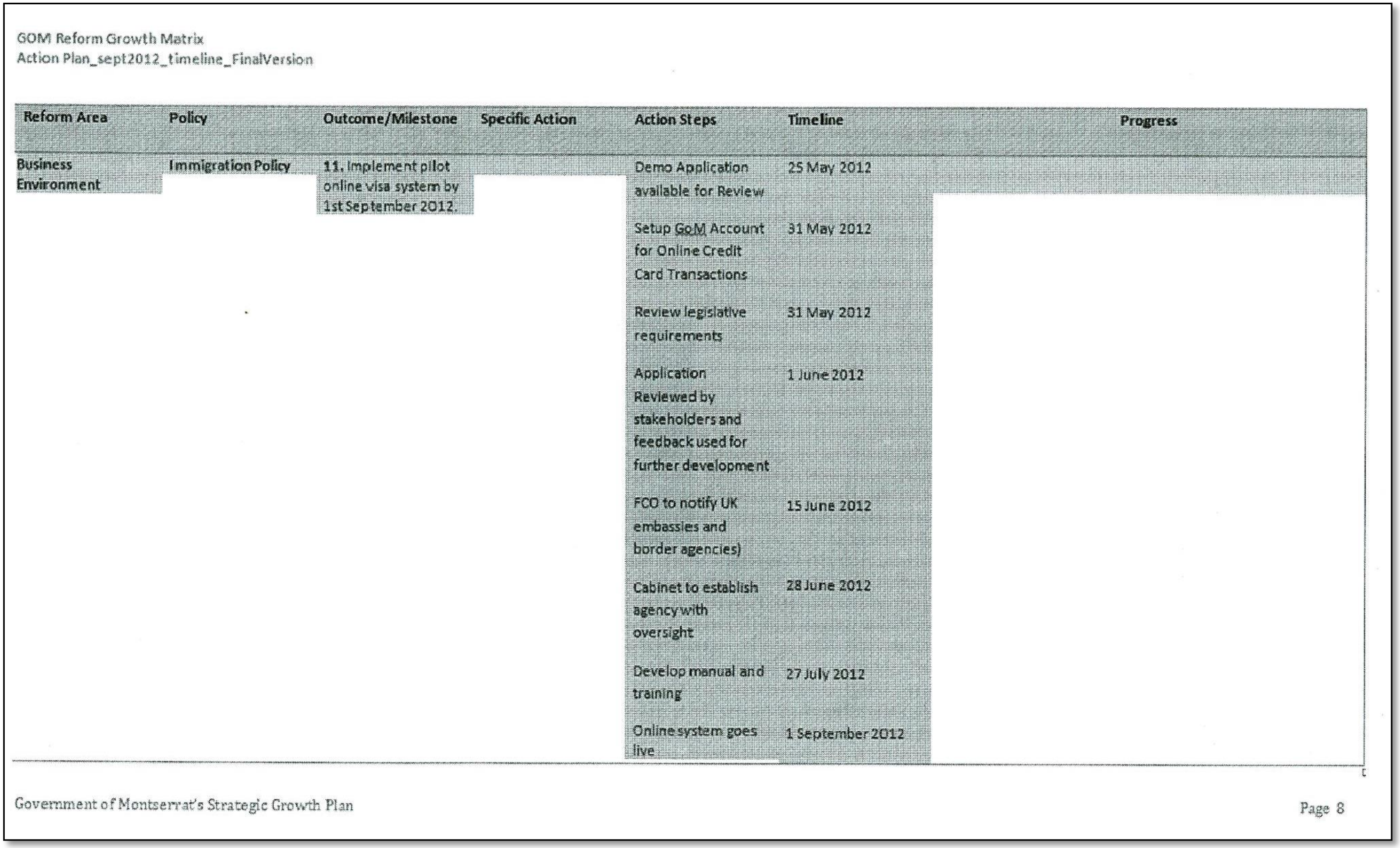
APPENDICES

Appendix 1 – GoM Organisational Chart



LEGISLATIVE ASSEMBLY			
SPEAKER OF THE HOUSE	PREMIER,	PARLIAMENTARIANS	LEADER OF THE OPPOSITION
DEPUTY SPEAKER OF THE HOUSE	DEPUTY PREMIER,	EX OFFICIO MEMBERS	OPPOSITON MEMBERS
CLERK OF THE ASSEMBLY	GOVERNMENT MINISTERS		

Appendix 2 - GoM Reform Growth Matrix



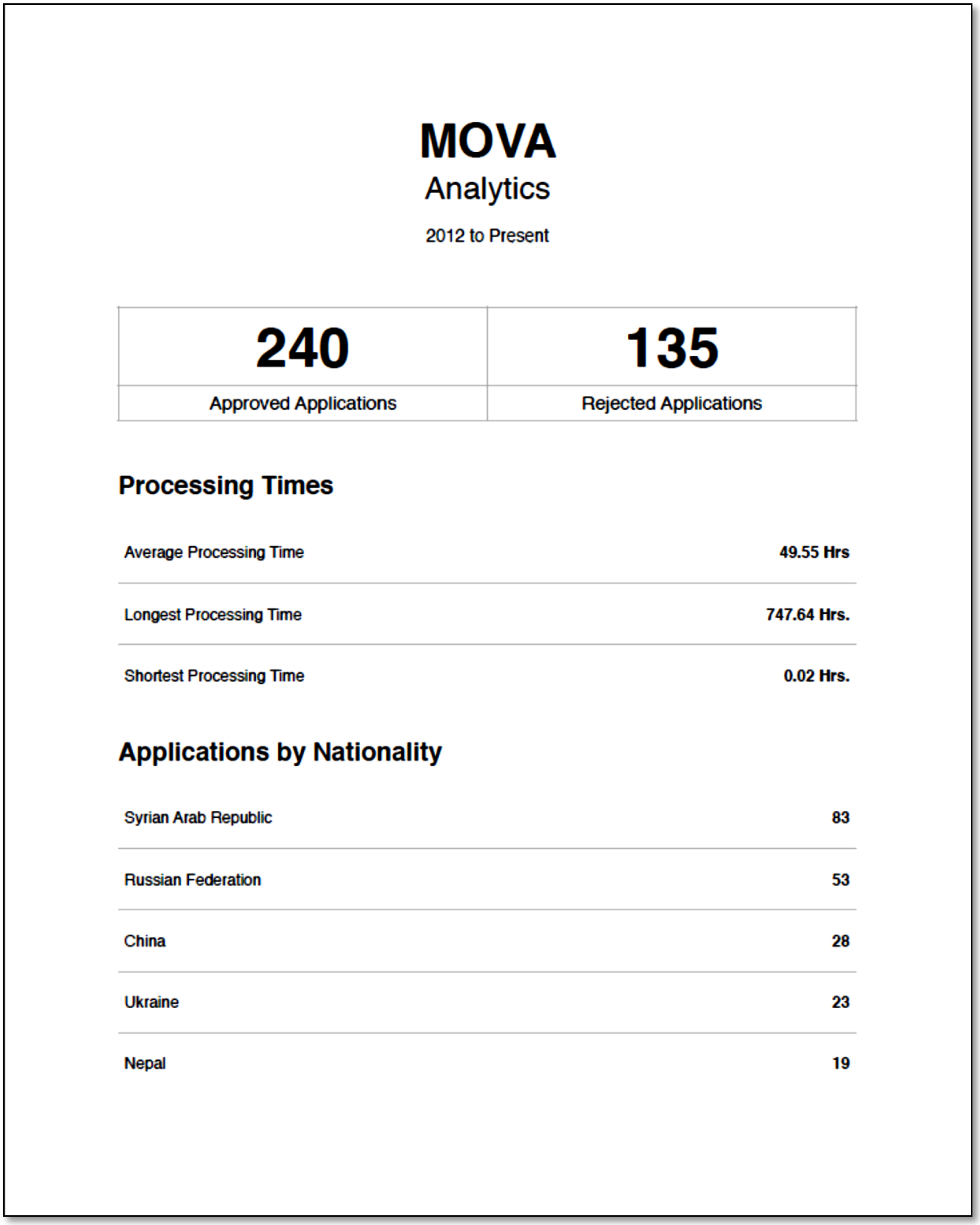
GOM Reform Growth Matrix
Action Plan_sept2012_timeline_FinalVersion

Reform Area	Policy	Outcome/Milestone	Specific Action	Action Steps	Timeline	Progress
Business Environment	Immigration Policy	11. Implement pilot online visa system by 1st September 2012.		Demo Application available for Review	25 May 2012	
				Setup GoM Account for Online Credit Card Transactions	31 May 2012	
				Review legislative requirements	31 May 2012	
				Application Reviewed by stakeholders and feedback used for further development	1 June 2012	
				FCO to notify UK embassies and border agencies)	15 June 2012	
				Cabinet to establish agency with oversight	28 June 2012	
				Develop manual and training	27 July 2012	
				Online system goes live	1 September 2012	

Government of Montserrat's Strategic Growth Plan

Page 8

Appendix 3 - MOVA Operational Statistics I



MOVA

Analytics

2012 to Present

240	135
Approved Applications	Rejected Applications

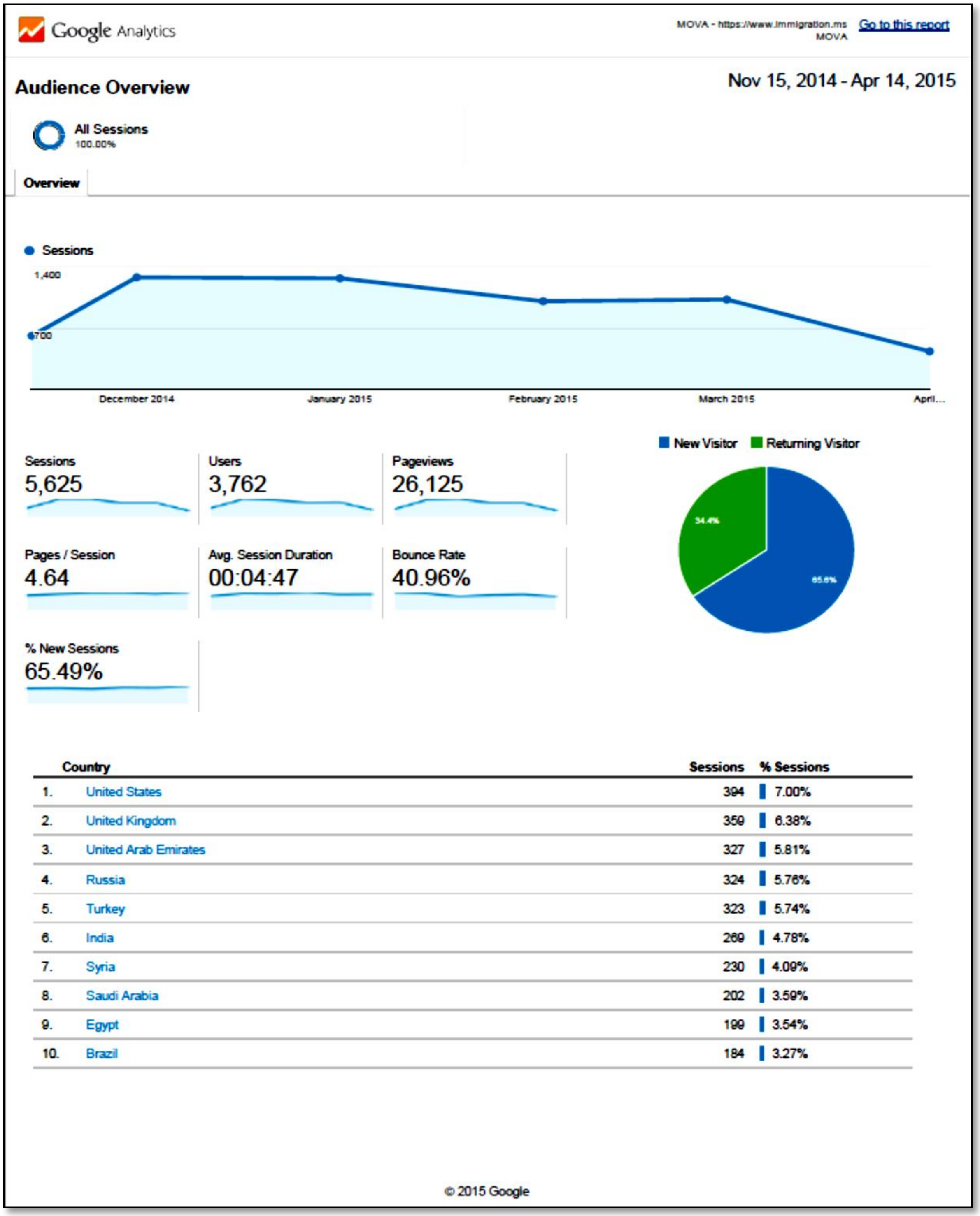
Processing Times

Average Processing Time	49.55 Hrs
Longest Processing Time	747.64 Hrs.
Shortest Processing Time	0.02 Hrs.

Applications by Nationality

Syrian Arab Republic	83
Russian Federation	53
China	28
Ukraine	23
Nepal	19

Appendix 4 - MOVA Operational Statistics II



Audience Overview

Nov 15, 2014 - Apr 14, 2015

All Sessions
100.00%

Sessions
5,625

Users
3,762

Pageviews
26,125

Pages / Session
4.64

Avg. Session Duration
00:04:47

Bounce Rate
40.96%

% New Sessions
65.49%

	Country	Sessions	% Sessions
1.	United States	394	7.00%
2.	United Kingdom	359	6.38%
3.	United Arab Emirates	327	5.81%
4.	Russia	324	5.76%
5.	Turkey	323	5.74%
6.	India	269	4.78%
7.	Syria	230	4.09%
8.	Saudi Arabia	202	3.59%
9.	Egypt	199	3.54%
10.	Brazil	184	3.27%

© 2015 Google

Appendix 5 - Countries Requiring a Visa

Afghanistan	Lao People's Democratic Republic
Aland Islands	Lebanon
Albania	Liberia
Algeria	Libya
Angola	Macedonia, The Former Yugoslav Republic of
Armenia	Madagascar
Azerbaijan	Mali
Bahrain	Mauritania
Belarus	Mayotte
Benin	Moldova, Republic of
Bhutan	Mongolia
Bolivia, Plurinational State of	Montenegro
Bosnia and Herzegovina	Morocco
Burkina Faso	Mozambique
Burundi	Nepal
Cambodia	Niger
Cape Verde	Oman
Central African Republic	Palestinian Territory, Occupied
Chad	Peru
China	Philippines
Colombia	Qatar
Comoros	Reunion
Congo	Russian Federation
Congo, The Democratic Republic of The	Sao Tome and Principe
Cote D'ivoire	Saudi Arabia
Croatia	Senegal
Cuba	Serbia
Djibouti	Somalia
Ecuador	South Sudan
Egypt	Sudan
El Salvador	Svalbard and Jan Mayen
Equatorial Guinea	Syrian Arab Republic
Eritrea	Tajikistan
Ethiopia	Thailand
Gabon	Togo
Georgia	Tunisia
Guinea	Turkey
Guinea-Bissau	Turkmenistan
Indonesia	Ukraine
Iran, Islamic Republic of	United Arab Emirates
Iraq	Uzbekistan
Ivory Coast	Venezuela, Bolivarian Republic of
Jordan	Viet Nam
Kazakhstan	Yemen
Korea, Democratic People's Republic of	
Kuwait	
Kyrgyzstan	