REPORT

ON

PERFORMANCE STUDY OF
GOVERNMENT INFORMATION SYSTEMS UNIT – BUSINESS CONTINUITY PLANNING

FOR THE PERIOD JANUARY 2006- DECEMBER 2006

Prepared by

OFFICE OF THE AUDITOR GENERAL
BRADES, MONTSERRAT
MAY 2007

PERFORMANCE STUDY
OF THE
GOVERNMENT INFORMATION SYSTEMS UNIT:

BUSINESS CONTINUITY PLANNING

This is the report of a performance audit we conducted under section 8(f) of the Audit Act 2001.

May 2007

FOREWORD

The Government Information Systems Unit (GISU) is the main arm which manages Information Systems. It procures and services IT equipment to all central government agencies as well as providing technical support for several critical services. Given the dependence on the IT infrastructure for effective service delivery, I undertook a performance study to assess and report on Business Continuity Planning.

Overall, minimal attention has been paid to designing a comprehensive Business Continuity Plan.

I have recommended improvements in two broad areas: obtaining managerial support in the area of business continuity planning, and conducting business impact analysis to inform development of plan.

This audit involved discussions with and the provision of information by many staff at the Government Information Systems Unit. I wish to thank them for their co-operation and the assistance given.

Florence A Lee
Auditor General

31 July 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Government Information System Unit (GISU) is responsible for the procurement, implementation, support and maintenance of all information and communication technologies infrastructure, equipment and applications within the Public Sector. Over the years the GISU has been enhancing its operations further to ensure that the entire sector provides quality to the people of Montserrat. The performance of this unit is therefore critical to ensure the efficient and effective delivery of services.

In 2005, the Office of the Auditor General decided to expand its audit services to include other audits such as IT audits and value for money/performance audits. We also decided to examine business continuity plans (BCPs) for core IT systems. Business continuity planning is fundamental to the well being of an organization and is intended to ensure continuity in the face of unforeseen or difficult circumstances.

This study covered the period January 2006 to December 2006 and was conducted by Miss Marsha V. E. Meade, Deputy Auditor General. This study sought to assess and report on the existence of disaster recovery or business continuity procedures within the GISU. The three main objectives of this performance study were to validate the business continuity plan at GISU; scrutinize and verify preventive and facilitating measures for ensuring continuity; and examine evidence about the performance activities that can assure continuity and recovery.

Our Findings

The GISU has a disaster plan in place but there are key elements that are not included. These include outlined roles and responsibilities and a documented crisis management process.

Our Recommendations

We recommend the appointment of a disaster recovery board with responsibilities for developing a clear policy statement on BCP. Additionally, we recommend that Business Impact Analysis be conducted and a BCP be developed.

CHAPTER 1

1.0 INTRODUCTION

1.1 Background and Rationale for this study

In 2005, the Office of the Auditor General decided to expand its audit services. Instead of focusing on financial audits we decided to include other audits such as IT audits, value for money/performance audits, health and safety audits and forensic auditing as part of our Annual Audit Programme. It was also decided to examine business continuity plans (BCPs) for core IT systems. The purpose of a business continuity plan is to ensure that following a disaster and/or unexpected event, prompt action is taken, in a coordinated manner, so as to limit negative impacts on the public service, the economy, and to re-establish systems and ultimately full service-delivery.

This decision to conduct IT audits was speeded up because of the government server crash of May 2006. The server which stores the data for most of the departments on the headquarters compound crashed unexpectedly. This server is configured with a robust hard drive redundancy system (Raid 5); and for reasons yet to be determined, four of the nine hard drives in the Raid Array failed simultaneously. This meant that some data which were normally accessible on drives H: and G: was lost. For these reasons, the Office of the Auditor General took the initiative to undertake this performance study.

1.2 Objectives of this study

Our study sought to assess and report on the existence, adequacy, completeness and appropriateness of disaster recovery and business continuity procedures at the GISU. The three main objectives of this performance study were to:

- validate the business continuity plan[1];
- scrutinize and verify preventive and facilitating measures for ensuring continuity; and
- examine evidence about the performance activities that can assure continuity and recovery.

1.3 Scope of this study

The study will cover the period January 2006 to December 2006 and will focus on the examination of GISU's business continuity plans (BCP) and or areas. The auditor monitored the audit closely and has amended some areas so as to maximize the efficiency of the audit.

1.4 How this study was conducted

A benchmarking strategy was adopted to facilitate this audit. Benchmarking is a complex process. However, it provides best practice information that can be tailored to meet an organization's unique circumstances. The OAG have examined a number of different ways of benchmarking. Since GISU does not have comprehensive internal BCP we have decided to use external benchmarking.

[1] For example, the auditor has knowledge of the unit, the systems in use and the extent of the business dependence on IT. The focus therefore is on validating the plan against this knowledge.

There is a large body of literature about disaster recovery and business continuity planning; including journal articles[2] and texts. Our external benchmarking focused on comparing the GISU's business continuity procedures with good practice and other BCPs.

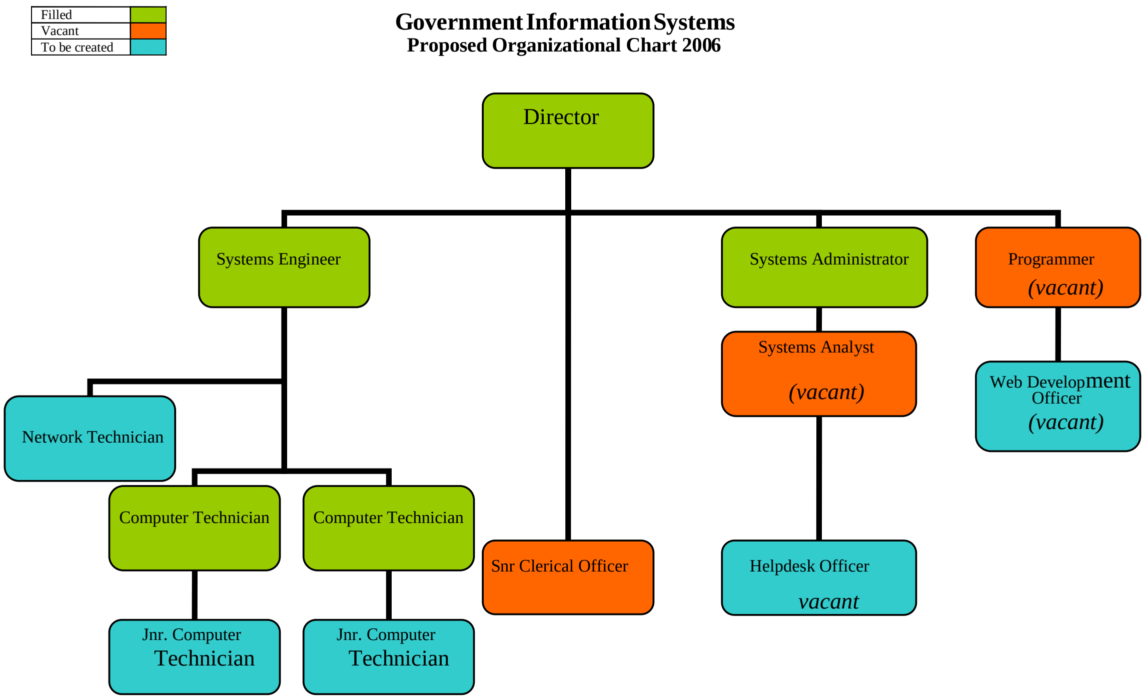
The auditor has also conducted an interview with the Director of the GISU about the unit's procedures and a questionnaire was administered to capture more detailed information. The auditor also visited the GISU on a number of occasions to verify the existence of any information on disaster recovery or business continuity posted around the main office. The OAG also examined the existing Disaster Plan for GISU.

1.5 Overview of GISU

The GISU is responsible for the smooth functioning and maintenance of the Government of Montserrat network infrastructure. The department is ultimately responsible for all the network and computer equipment in all government offices. It has a server room which houses several pieces of very expensive and mission critical equipment. It maintains file storage systems and databases for most government offices as well as Email and Internet access. It also maintains a wireless network that provides connectivity between the offices at Government Headquarters in Brades and all other government offices located at various locations on Montserrat.

[2] A useful article was written by S. Anantha Sayana, "Auditing Business Continuity" Information Systems Control Journal, Volume 1, 2005

The GISU as a whole is overseen by a Director who reports to the Financial Secretary within the Ministry of Finance. The diagram below shows the proposed organizational structure for the GISU.


Government Information Systems
Proposed Organizational Chart 2006

1.6 Reasons for Business Continuity Plans

There are many different risks that can negatively impact the normal operations of the unit. A risk assessment should be performed to figure out what constitutes a disaster and which risks the unit is susceptible to. These may include:

- natural disasters i.e. volcano, hurricane, flood;
- fire;
- power failure;

- organized or deliberate disruptions;
- system and/or equipment failures;
- human error;
- computer viruses;
- legal issues
- worker strikes and so on.

There are reasons why an organization would want to undertake a BCP. Over the years there has been increased dependency on computerized information systems within the public service. This includes the dependence on IT systems for processing of transactions, facilitation of payment to vendors and provision of financial and statistical information. Given the heavy reliance on IT systems for efficient and effective delivery of services there is a need to establish a formal process to be followed when disaster occurs.

CHAPTER 2

2.0 MAIN FINDINGS

2.1 GISU's Disaster Plan

The GISU has a disaster plan in place that is geared towards a hurricane warning announcement. The unit has the following procedures or practices in place:

- BCP plan is communicated to staff but only to the extent that it exist;
- The unit has identified alternative site for storing hardware and other peripherals;
- It has established an expected recovery time of 24 hours for critical business functions;
- "Business as usual" servicing capability is in place and is designed to address 51-75% recovery;
- The current plan has established critical computer applications, operating systems and data files with recovery priorities;
- Alternate (secondary) site for data center recovery purposes is located 1.5 miles from production (primary) site.
- The Ministries/Departments are often reminded and/or advised by GISU to conduct internal back up of their drives for safe keeping.

From our interview with the Director and from our own observation, we have determined that a number of things such as back ups sent off site weekly, surge protectors, fire preventions, antivirus software, and uninterruptible power supply are in existence although not noted on the plan.

2.2 Shortcomings of GISU Disaster Plan

There are a number of factors that the current plan does not take into consideration and these are outlined below. GISU does not

- have an approved BCP that identifies roles and responsibilities within the unit;
- have a documented crisis management process;
- have a clear process for notification, activation and escalation of a BCP;
- engage in testing or practice drills periodically and no test dates are scheduled over the next 12-18 months;
- have the same capacity back up facility to that of the primary facility. Additionally, it is not feasible to run the back up facility for an extended period of at least six weeks and copies of the plan are not kept at the off site facility;
- have a dedicated team focused on business continuity and or IT disaster recovery.

With the rise in information technology and the reliance on business-critical data, the landscape has changed in recent years in favor of protecting IT equipment and irreplaceable data. Even though there is a disaster plan for GISU, we are not satisfied with the contents and will now make recommendations to assist the unit with improving its procedures and systems.

CHAPTER 3

3.0 RECOMMENDATIONS & CONCLUSION

3.1 Appoint Disaster Recovery Board

The unit needs to appoint individuals responsible for designing and implementing a plan. Members of the board must have knowledge of the business and a clear understanding and ability to perform the needed procedures. This board should issue a clear policy statement on business continuity planning. At a minimum, this statement should contain the following instructions:

- the unit should develop a comprehensive BCP;
- a formal risk assessment should be undertaken in order to determine the requirement for the BCP;
- the BCP should cover all essential and critical business activities;
- the BCP should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed;
- a disaster recovery test should be done annually with the IT team to recover key information systems on separate hardware at a recovery site.
- all staff must be made aware of the BCP and their own respective roles and responsibilities;
- the BCP is to be kept up to date to take into account changing circumstances.

This policy statement should be communicated to all management and staff as part of its information security policy and management process.[3]

3.2 Business Impact Analysis

The Disaster Recovery Board should then conduct a business impact analysis to assess the impacts of disruptions on the GISU and all other government departments/ministries and to identify and prioritize critical services and associated assets. This analysis involves the following steps:

a. Determine the nature of the GISU's business (e.g. role, mandate) and the services it must deliver according to its constituent or other legislation, government policy, obligations to other departments, and service sharing arrangements, treaties, contracts, memoranda of understanding or other agreements. Internal and external functions on which services depend must also be identified.

b. Determine the direct and indirect impacts of disruptions on the unit, including the quantitative and qualitative effects.

c. Assess services to determine which are likely to cause high degree of injury to employees and the government, if disrupted. It is vital to achieve immediate recovery or maintain minimum levels of service until full service is restored.

[3] http://www.yourwindow.to/business%2Dcontinuity/ - Business Continuity Planning and Disaster Recovery Planning – An Online Guide

d. Identify and prioritize critical services and list the resources (personnel, contractors, suppliers, information, systems and other assets) that support them directly or indirectly, within or outside the unit. Priority should be assigned based on the maximum allowable downtime and the minimum service level required.

e. Obtain top management approval of the results of the business impact analysis before proceeding with the development of continuity plans.

3.3 Preparation of the Plan

For a plan to be effective it must be in writing, must be understandable and must be accessible to those who need it. Because of constant changes that occur in the modern business environment, a plan should be updated frequently to deal with new and existing threats as they become known. A good plan takes into account many different factors. The most important to note are:

a. Telephone Tree

This should be in place to notify all key personnel of a problem and assign them tasks focused toward the recovery plan. There should be a visible emergency telephone numbers list in the office so that staff can be easily notified.

b. Ability to Recover Data and Systems

The continual backing up of data and systems can help minimize the severity of threats. The plan should also include information on how best to recover any data that has not been copied. Controls and protections should be in place to ensure that data is not damaged, altered, or destroyed during this process. Information technology experts and procedures need to be identified that can accomplish this endeavor. Vendor manuals can also assist in determining how best to proceed.

c. Tests and Drills of Disaster Procedures

Practice drills should be conducted periodically to determine how effective the plan is and to determine what changes may be necessary. A lesson learned report should be prepared after testing activities or actual events (validation can range from a questionnaire through table top exercises). The report should include aspects of the exercise that went as planned, problems uncovered during these drills and procedures designed to deal with these and other potential deficiencies.

Two tests should be done on an annual basis. GISU must conduct a table top BCP test that results in guidance for what information systems would be required in the event of a disaster. The second test to be performed is the disaster recovery test which would confirm that processes and procedures are in place to restore those information systems.

d. Procedures Allowing Effective Communication

Management and the recovery team should have procedures which allow for effective communication. This can be accomplished by making sure contact information is easily accessible and drills conducted test communication abilities. Procedures should include non-technological as well as technological methodologies in case of power or system failures. Communications between the unit and outside individuals and organizations also need to be taken into account when designing the plan.

e. Documentation

Adequate records need to be retained by the unit and the Director should ensure that after a more detailed plan is implemented each member of staff and other members of the recovery team receive a copy.

f. Emergency Procedures

Capabilities of administering CPR/first aid, and dealing with family emergencies should be clearly written and tested. This can generally be accomplished by the unit through good training programs and a clear definition of job responsibilities.

g. Backup of Key Personnel Positions

Clearly written policies and specific communication with employees should be used to substantiate this. There also must be confirmation that the personnel backups can actually do the duties assigned to them in an event of an emergency. Periodic training can also help alleviate this. This training should include updates to existing job positions and testing to confirm proficiency.

CHAPTER 4

4.0 CONCLUSION & MANAGEMENT RESPONSE

4.1 Conclusion

BCP captures how an organization prepares for future incidents that could jeopardize an organization's core mission and its long term health. With the hurricane season fast approaching and living with an active volcano, the bottom line is for GISU to ensure that achievable procedures exist, essentially, a framework, to ensure that sound continuity practices are adopted and maintained in the event of a disaster.

4.2 Management Response

A draft copy of the report was submitted to the Director, Government Information System Unit who made the following comments:

> "The GIS Department welcomes the Office of the Auditor General's comprehensive look into our preparedness to handle Natural disasters and other unforeseen impacts on our services, and interruptions to the Network and Computer systems which we are responsible for maintaining.
>
> The findings of the report are accurate in the main and we accept the recommendation that we need to develop a more comprehensive plan in the near future.

One of the critical elements for improving our plan lies in the recruitment of the additional staff as outlined in our Business Plan and proposed new organizational structure. We would further welcome the Office of the Auditor General's assistance in getting this point across to the persons responsible for approving our plans and getting the additional staff on board and functioning within the GIS Department.

The GIS Department looks forward to the continued assistance of the Office of the Auditor General as we seek to develop and fine tune a more comprehensive Business Continuity Plan."