
# BUSINESS CONTINUITY PLANNING
# FOLLOW-UP AUDIT

**REPORT**

**ON**

**PERFORMANCE STUDY OF THE**
**DEPARTMENT OF INFORMATION TECHNOLOGY**
**& E-SERVICES (DITES)**

**FOR THE PERIOD AUGUST 2007 - JULY 2016**

**Prepared by**

**OFFICE OF THE AUDITOR GENERAL**
**BRADES, MONTSERRAT**
**MAY 2017**

THIS PAGE WAS INTENTIONALLY LEFT BLANK

# BUSINESS CONTINUITY PLANNING
# FOLLOW-UP AUDIT

## PERFORMANCE STUDY OF THE
## DEPARTMENT OF INFORMATION TECHNOLOGY
## & E-SERVICES (DITES)

# BUSINESS CONTINUITY PLANNING

## FOLLOW-UP AUDIT PERFORMANCE STUDY OF THE DEPARTMENT OF INFORMATION TECHNOLOGY & E-SERVICES (DITES)

This is the report of a Business Continuity (BC)/Disaster Recovery (DR) Planning audit we conducted under the Montserrat Constitution 2010.

May 2017

## TABLE OF CONTENTS

THIS PAGE WAS INTENTIONALLY LEFT BLANK

## EXECUTIVE SUMMARY

The Department of Information Technology & e-Services (DITES) is responsible for the procurement, implementation, support, and maintenance of all information and communication technologies infrastructure, equipment, and applications within the Government of Montserrat's enterprise network infrastructure.

In May 2006, there was an unexpected system failure of the government server where the data for most of the Government departments, on both the H: and G: drives, was lost. As a result, the Office of the Auditor General (OAG) conducted a pilot performance IT audit in July 2007, to investigate the incident.

This follow-up review is to determine if DITES have been compliant and implemented any of the recommendations outlined in the initial performance audit.

## FINDINGS

DITES has been non-compliant with the recommendations outlined in the initial performance study conducted in 2007. They do not have a BCP or DRP, which has been tested, updated, and disseminated to the staff.

## RECOMMENDATIONS

The same recommendations from the initial performance study stands, as follows:

**1)** Appoint Disaster Recovery Board

**2)** Conduct Risk Assessment and Business Impact Analysis

**3)** Preparation of the BC/DR Plan

a. Telephone Tree
b. Ability to Recover Data and Systems
c. Tests and Drills of Disaster Procedures
d. Procedures Allowing Effective Communication
e. Documentation
f. Emergency Procedures
g. Backup of Key Personnel Positions

## AUDIT OPINION

The Office of the Auditor General has determined that DITES have been non-compliant and they need to adopt, and/or put into effect, the recommendations outlined above.

THIS PAGE WAS INTENTIONALLY LEFT BLANK

# CHAPTER 1 INTRODUCTION

## 1.0 OVERVIEW

In July 2007, the Office of the Auditor General (OAG) conducted a pilot performance IT audit to investigate the unexpected system failure of the government server. As a result, data for most of the Government departments on both the H: and G: drives, was lost.

This follow-up review is to determine if DITES have been compliant and implemented any of the recommendations outlined in the initial performance audit. The recommendations were agreed by DITES management.

The Department of Information Technology & e-Services (DITES) is responsible for the procurement, implementation, support, and maintenance of all information and communication technologies infrastructure, equipment, and applications within the Government of Montserrat's enterprise network infrastructure. Their server room houses several pieces of very expensive and mission critical equipment on which they maintain a file storage system, databases, e-mail, and Internet access for all of the government offices. It also maintains a wireless network that provides connectivity between the offices at Government Headquarters in Brades and other government offices located at various sites on the island.

## 1.2 MANAGEMENT RESPONSIBILITY

Management is responsible for ensuring that appropriate continuity and recovery policies and effective controls exist. More specifically, management must ensure that policies exist to facilitate IT governance and to guide the development of business continuity planning, disaster recovery planning, and business impact analysis. 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 an opinion on the continuity and recovery operations, and the risk and impact assessments, for DITES, based on our audit. Our work was conducted in accordance with ISSAI 100 and 5300. These principles require that we comply with ethical requirements and plan and perform the audit in order to obtain reasonable assurance whether tried and true policies, plans, procedures, and internal controls exist and are functioning effectively, proper records have been and are being kept, and all the necessary information and explanations for the purpose of our audit, has been obtained.

## 1.4 AUDIT MANDATE

The Office of the Auditor General 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 BCP/DRP operations and BIA and Risk assessments included the use of ISSAI 100, 200, 300, 400, 3100, 4100, and 5300, Control Objectives for Information and Related Technologies (COBIT) 4.1, and National Institute of Standards and Technology (NIST) SP 800-34, together with the INTOSAI Development Initiative (IDI) Handbook for IT Audits.

## 1.6 AUDIT OBJECTIVES

Considering the capital invested in the mission critical computer equipment housed in DITES, and because of their importance to the continued, smooth, operation of the Government of Montserrat (GoM), they must be effectively protected against all hazards whether accidental, deliberate, or act of God.

Consequently, the main purpose of this follow-up performance IT audit review is to confirm if any of the recommendations made by Office of the Auditor General in the 2007 report, have been effected and/or instituted by DITES.

We want to establish mainly the following:

1. If DITES has implemented a comprehensive, effective, and approved Business Continuity (BC)/Disaster Recovery (DR) Plans and/or Policies.
2. Is there a dedicated Business Continuity or IT Disaster Recovery team in place?
3. Does the organisation's BC/DR plans include backup and recovery procedures for hardware, data, application software, and data centre (recovery) and have they been suitably implemented?
4. Is the BCP/DRP adequately documented to conduct effective interim business activities and recovery procedures after a business interruption?
5. Confirm if any of these plans and/or policies effectiveness have been tested, the frequency of these run-throughs, and if any of the results have been recorded and reviewed.
6. Is DITES's staff aware of these business continuity and disaster recovery documents, their roles and responsibilities, and the different crisis management processes, outlined in the plans?
7. If DITES has conducted any Business Impact or Risk Assessments and if there is a Risk Management system in place.

## 1.7 SCOPE OF THIS STUDY

The study will cover the period August 2007 to July 2016 and will focus on the examination of DITES's Business Continuity (BC) & Disaster Recovery (DR) plans, Risk Assessment and Business Impact Assessment (BIA).

## 1.8 METHODOLOGY

A combination of two techniques were utilised to gather information and assess whether relevant controls existed, were implemented, and if they were effective in

ensuring that expensive mission-critical equipment were protected. These were interviewing of management and other members of staff, and inspection of documents and assets.

A questionnaire was issued to the Director of DITES in order to gather in-depth information about the department's BC, DR, and BIA plans, policies, procedures, operations and assessments.

The findings of this report were discussed with the Director of DITES and his view(s) was taken into consideration when finalising the report.

# CHAPTER 2 BUSINESS CONTINUITY (BC) & DISASTER RECOVERY (DR) PLANNING

## 2.0 CONTINGENCY PLANNING AND CONTINUITY

With the increased dependency on computerised information systems within the public service (for example, processing of transactions, facilitation of payment to vendors, provision of financial and statistical information) for efficient and effective delivery of services, there is a need to establish a formal process to be followed when disaster occurs.

A business continuity plan contains everything that is necessary to provide an organisation with the ability to fulfil its corporate mission during the period of disruption and then to return to normal in a controlled manner. This way the organisation would not lose the capability to process, retrieve, and protect the information it stores and maintains should there be an interruption or disaster that leads to temporary or permanent loss of computer facilities.

## 2.1 CONTINGENCY PLANNING

Contingency planning is a component of business continuity, disaster recovery and risk management and usually falls under the domain of the IT Department. A contingency plan focuses on specifics, such as the actions that are necessary to transfer a business system to a standby site. This plan is a course of action designed to help an organisation respond effectively to a significant future event or situation that may or may not happen. It is sometimes referred to as "Plan B," because it can be also used as an alternative for action if expected results fail to materialize.[1]

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Given these severe implications, it is critical that an entity have in place (1) procedures for protecting information resources and minimising the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centres and telecommunications facilities, as well as those performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises.[2]

The seven-steps outlined for an IT contingency plan in the *NIST 800-34 Rev. 1* publication are:

[1] http://whatis.techtarget.com/definition/contingency-plan
[2] http://gao.gov/assets/80/77142.pdf

1. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
2. Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business functions.
3. Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
4. Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
6. Ensure plan testing, training and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.
7. Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes. [3]

## 2.2 BUSINESS CONTINUITY

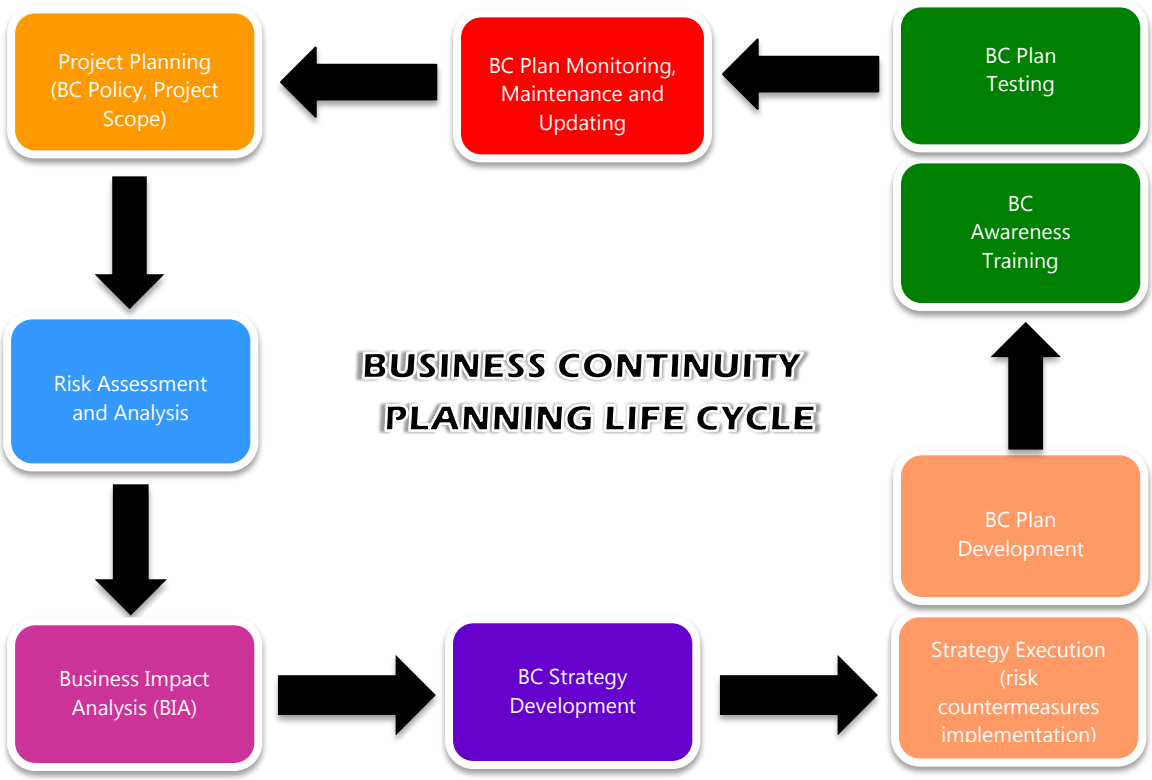
Effective business continuity planning requires a range of skills, together with the understanding of the:

- business environment and its objectives and strategies
- full range of risks that the business would face and the most cost effective options for managing them
- people, communications, and other support services on which the business systems rely

The development of a workable continuity plan requires a wide range of skills that may include consultancy support, significant resources, and the co-operation of many personnel in different areas of the organisation. The developed plan will also require an annual budget to cover the cost of awareness training, testing, and maintenance. Consequently, any worthwhile progress on continuity planning will not be possible without the strong commitment from the organisation's top management.[4]

[5]The wide range of skills required to draft up comprehensive plans, is due to the numerous questions that will have to be resolved during the planning process; a methodical approach to the task will help to ensure that nothing important is omitted. The developmental process is usually initiated and managed as a 'project' that will involve:

[3] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
[4] https://www.scribd.com/document/145639293/2007-BCP-Student-Notes
[5] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/business-impact-analysis.aspx




***Flowchart I – BCP Life Cycle***[6]

a. defining that project objectives and deliverables

b. agreeing a project budget and deadline

c. allocating sufficient skills and resources

d. appointing a Project Board/Steering Committee to 'own' the project, monitor progress and make any major decisions that are necessary

It is the responsibility of an institution's board and senior management to ensure that the institution identifies, assesses, prioritises, manages, and controls risks as part of the business continuity planning process. The board and senior management should establish policies that define how the institution will manage and control the risks identified. Once policy is established, it is also important for the board and senior management to understand the consequences of these identified risks and support continuity planning on a continuous basis.

## 2.3 OBSERVATIONS

**1.** No BCP was conducted or related documentation exists.

**2.** No DRP was conducted or related documentation exists.

[6] http://slideplayer.info/slide/2777317/

## 2.4 MANAGEMENT RESPONSE

We have been seeking to obtain Management Responses since February 2017. Despite repeated requests and reminders, we have not received any.

# CHAPTER 3 BUSINESS IMPACT ASSESSMENT (BIA) AND RISK ASSESSMENT

## 3.1 BUSINESS IMPACT ASSESSMENT (BIA)

[7]Recovering from a business interruption requires planning ahead to keep focus during the aftermath of an outage. Companies can prepare for the possibility of adverse events that interrupt their operations by developing a business impact analysis (BIA) and conducting a risk assessment (RA).

[8]A Business Impact Analysis (BIA) is the first step in the business continuity and disaster recovery planning process and should include the:

**A.** Assessment and prioritisation of all business functions and processes, including their interdependencies, as part of a work flow analysis

**B.** Identification of the potential impact of business disruptions resulting from uncontrolled, non-specific events on the institution's business functions and processes

**C.** Identification of the legal and regulatory requirements for the institution's business functions and processes

**D.** Estimation of maximum allowable downtime, as well as the acceptable level of losses, associated with the institution's business functions and processes

**E.** Estimation of recovery time objectives (RTOs), recovery point objectives (RPOs), and recovery of the critical path.

**F.** Where third party service provider(s) have been outsourced, a BCP should also be considered for the service provider(s).

Often the BIA uncovers some less visible, but vital component that supports the critical business process. When documenting the mission critical functions performed, the following questions should be considered:

- What critical interdependencies exist between internal systems, applications, business processes, and departments?
- What specialised equipment is required and how is it used?
- How would the department function if the mainframe, network, and/or Internet access were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- What are the required responsibilities of the institution and the third-party service provider as defined by the service level agreement?
- What critical operational or security controls require implementation prior to recovery?

[7] http://www.wolfpacsolutions.com/articles/using-business-impact-analysis-prepare-emergency
[8] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/business-impact-analysis.aspx

- What is the minimum number of staff and amount of space that would be required at a recovery site?
- What special forms or supplies would be needed at a recovery site?
- What equipment would be needed at a recovery site to communicate with employees, vendors, and customers?
- What is the potential impact if common recovery sites serve multiple financial institutions?
- Have employees received cross training, and has the department defined back-up functions/roles that employees should perform if key personnel are not available?
- Are the personal needs of employees adequately considered?

Once the BIA is complete, it should be evaluated during the risk assessment process and incorporated into and tested as part of, the BCP. The BIA should be reviewed by the steering board and senior management periodically and updated to reflect significant changes in business operations, audit recommendations, and lessons learned during the testing process. In addition, a copy of the BIA should be maintained at an offsite location so it is easily accessible when needed.

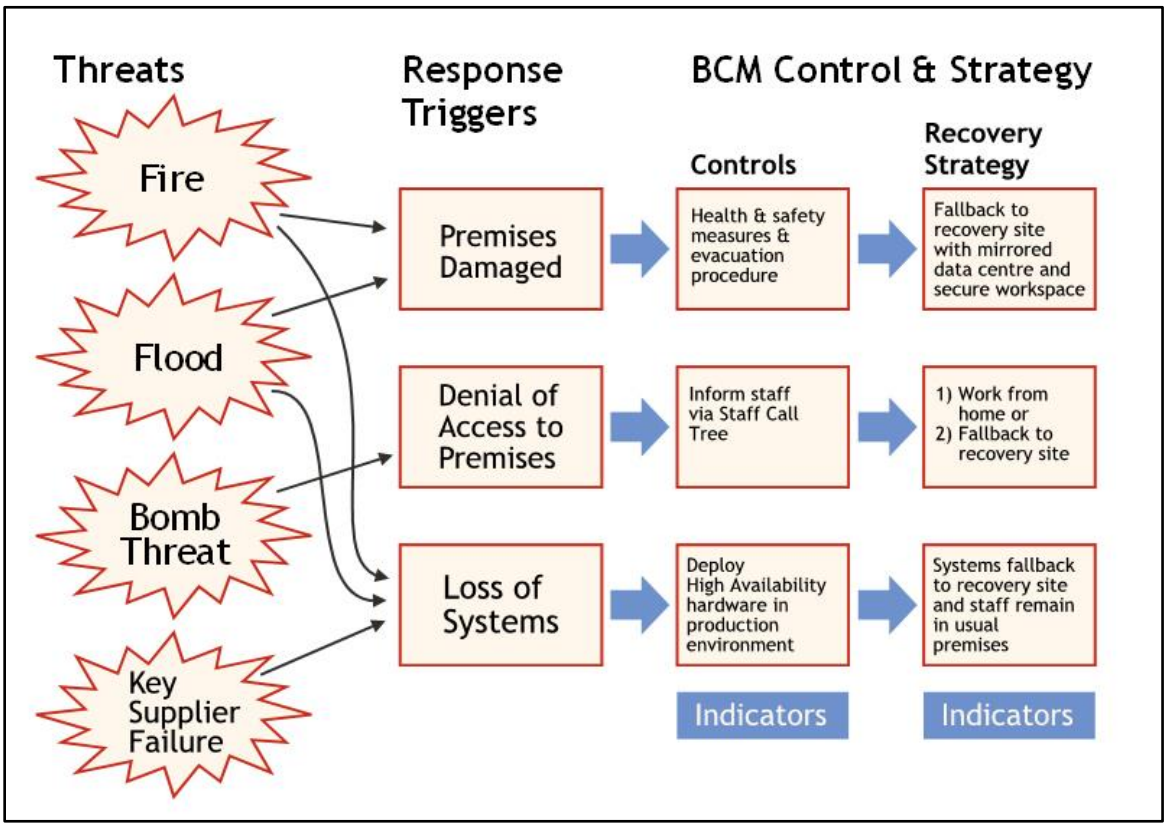
### 3.2 RISK ASSESSMENT

[9]Risk assessment is the second step in the business continuity planning process. It should include:

- Evaluating the BIA assumptions using various threat scenarios
- Analyzing threats based upon the impact to the institution, its customers, and the financial market it serves
- Prioritizing potential business disruptions based upon their severity, which is determined by their impact on operations and the probability of occurrence;
- Performing a "gap analysis" that compares the existing BCP to the policies and procedures that should be implemented based on prioritized disruptions identified and their resulting impact on the institution.

[10]In any organisation, the continuity of certain operations is more important than other operations, and it is not cost effective to provide the same level of continuity for all operations. For this reason, it is important that the organisation determines which are the most critical and what resources are needed to recover and support them. This is carried out by performing a risk assessment, identifying probable threats and their impacts on the organisation's information and related resources including data and application software, and operations. The risk and impact assessment should cover all functional areas. A decision on residual risk should accordingly be taken where the impact of a possible threat is minimal or control systems are adequate to highlight such instances in time.

[9] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/business-impact-analysis.aspx
[10] WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions




***Flowchart II - Example of a typical set of threats, response triggers and corresponding controls***[11]

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

❖ **Natural Hazards**

- Meteorological - Flooding, Severe Thunderstorm (Wind, Rain, Lightning), Windstorm, Hurricanes and Tropical Storms, etc.,
- Geological - Earthquake, Tsunami, Landslide, Subsidence/Sinkhole, Volcano
- Biological - Pandemic Disease, Foodborne Illnesses

❖ **Human-Caused Hazards**

- Accidents - Workplace accidents, Entrapment/Rescue (Machinery, Water, Confined Space, High Angle), Transportation Accidents (Motor Vehicle, Water, Air), Structural Failure/Collapse, Mechanical Breakdown
- Intentional Acts - labour strike, demonstrations, civil disturbance (riot), bomb threat, workplace violence, pilfering, terrorism (chemical, biological, radiological,

[11] http://www.chasecooper.com/pub-art-sub/98-business-continuity-management-3-threat-and-risk-assessment.html

nuclear, explosives), arson, cyber/information technology (malware attack, hacking, fraud, denial of service, etc.)

- Fire/Explosion - Fire (Structure, Wildland), Explosion (Chemical, Gas, or Process failure)
- Hazardous Materials - Hazardous Material spill/release, Transportation Accidents, Natural Gas Leak Supply
- Chain Interruption - Supplier Failure, Transportation Interruption

❖ **Technical Hazards**

- Utility Outage - Communications, Electrical Power, Water, Gas, Steam, Heating/Ventilation/Air Conditioning, Pollution Control System, Sewage System
- Information Technology - Loss of Connectivity, Hardware Failure, Lost/Corrupted Data, Application Failure

[12]The criticality and sensitivity of various data and operations should be determined and prioritised based on security categorisations and an overall risk assessment of the organisation's operations. Such a risk assessment should serve as the foundation of an organisation's IT security plan. Factors to be considered include the importance and sensitivity of the data and other organisational assets, and the cost of not restoring data or operations promptly. For example, a one-day interruption of a fee-collection systems or a loss of related data could significantly slow or halt receipt of revenues, diminish controls over a significant amount of revenue in receipts, and reduce public trust. Likewise, a system that monitors employee training could be out of service for perhaps as much as several months without serious consequences.

Once critical data and operations have been determined, the minimum resources needed to support them should be identified and their roles analysed. The resources to be considered include computer resources, such as hardware, software, and data files, networks including components such as routers and firewalls, supplies including paper stock and pre-printed forms, telecommunications services, and any other resources that are necessary to the operation, such as people, office facilities and supplies, and non-computerised records. Because essential resources are likely to be held or managed by a variety of groups within an organisation, it is important that program and information security support staff work together to identify the resources needed for critical operations.

In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed. A carefully developed processing restoration plan can help employees immediately begin the restoration process and make the most efficient use of limited computer resources during an

[12] *http://www.gao.gov/new.items/d09232g.pdf*

emergency. Both system users and information security support staff should be involved in determining emergency processing priorities.

### 3.3 OBSERVATIONS

**1.** No BIA was conducted, or related documentation exists.

**2.** No risk assessment was conducted or related documentation exists.

### 3.4 MANAGEMENT RESPONSE

We have been seeking to obtain Management Responses since February 2017. Despite repeated requests and reminders, we have not received any.

# CHAPTER 4 FINDINGS & RECOMMENDATIONS

## 4.1 FINDINGS

Nine years after the initial BCP study was carried out, it was found that DITES did not take into consideration, or implemented, any of our initial recommendations.

However, it is noteworthy to mention that we have already verified from prior and recent audits, and interviews with the Director of DITES and other members of staff, that the following do/do not exist:

1. DITES have system backups, surge protectors, fire preventions, antivirus software, and uninterruptible power supply are already in place
2. The department has a very basic disaster recovery plan in place that is geared towards a hurricane-warning announcement. The department has the following procedures or practices in place:
    - The basic disaster recovery plan is communicated to staff but only to the extent that it exist
    - There have not been any drills or testing done to date
    - The organisation has not identified an alternative site for storing hardware and other peripherals, they store them at the DITES main office space
    - Recovery time for critical business depends on how damaged the enterprise network equipment is and what, or if any, spares are on hand
    - "Business as usual" servicing capability is in place and is designed to address 51% to 75% recovery – again this is dependent on the amount of damage incurred by the enterprise equipment and if spares are available on site
    - The plan, although not current, has established critical computer applications, operating systems and data files with recovery priorities
    - An alternate site or hot site, for data centre recovery purposes, has not yet been found. Recent attempts have been made to secure this hot site at the new Communication and Works building in Brades. However, financial and other limiting constraints are major hindrances. For e.g. the capacity to house, and the capability to cool, all of the server room equipment.

## 4.2 RECOMMENDATIONS

Due to non-compliance of DITES to apply the recommendations outlined in the initial performance study conducted, we will reiterate the same recommendations as follows:

### 1) Appoint Disaster Recovery Board

The organisation 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 organisation 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

**2) Business Impact Analysis**

The Disaster Recovery Board should then conduct a business impact analysis to assess the impacts of disruptions on the DITES 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 DITES'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, and 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 organisation, 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

**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 organisation. 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) Preparation of the BC/DR 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 endeavour. 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. DITES 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 organisation and outside individuals and DITESs also need to be taken into account when designing the plan.

**e. Documentation**

Adequate records need to be retained by the organisation 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 organisation 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.

**4) Locate an alternate disaster recovery site**

[13]A disaster recovery site, for data centre purposes, is an important asset because it keeps an organization running, albeit in a lesser state. This alternate recovery site is often located in an entirely different location, city, province, state, or even another country. This ensures a higher probability of safety when a primary facility fails due to a localized disaster.

## 4.3 MANAGEMENT RESPONSE

We have been seeking to obtain Management Responses since February 2017. Despite repeated requests and reminders, we have not received any.

[13] https://www.techopedia.com/definition/29757/disaster-recovery-site-dr-site

## CHAPTER 5 AUDIT OPINION

The Office of the Auditor General has determined that DITES have been non-compliant and they need to adopt, and/or put into effect, any of the recommendations we outlined for them in 2007.

In the event that there is a major disaster, the continued operations of the department and the Government of Montserrat (GoM) will depend on DITES's ability to replicate the IT systems and data. Therefore, DITES need to devise and put into operation both a BC and DR plan, as they are integral parts of the overall risk management for any organisation.

[14]Therefore, overall, for the BC and DR plans to be well written the department needs to be cognisant of, appreciate, and consider the following factors:

**A.** The effectiveness of the BC process depends upon the involvement of a Project Board/Steering Committee and senior management

**B.** The BC process involves a continuous, process-oriented approach that includes a BIA, a risk assessment, risk management, and risk monitoring and testing.

**C.** A thorough BIA and risk assessment should form the foundation of the comprehensive BCP.

**D.** The BCP and testing program should be developed on an enterprise-wide basis.

**E.** The effectiveness of the BCP should be validated through annual, or more frequent, testing.

**F.** The BCP and test program should be thoroughly documented, evaluated by DITES management, independently reviewed by an internal and/or external audit function, and reported to the steering committee.

**G.** The BCP and test program should be updated to reflect and respond to changes in the institution and gaps identified during continuity testing.

**H.** In addition to the BCP, other IT and security related policies, standards, and processes should be integrated into the business continuity planning process.

[14] http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/summary.aspx

## ACKNOWLEDGEMENT

The Auditor General wishes to express her gratitude for the assistance and courtesies extended to the auditor during the course of this audit.

**Florence A Lee**
**Auditor General**

## REFERENCES

### Websites


https://www.bia.ca/risk-management-the-what-why-and-how/

http://www.csoonline.com/article/2118605/disaster-recovery/pandemic-preparedness-business-continuity-and-disaster-recovery-planning-the-basics.html?upd=1476819972676

http://www.disasterrecovery.org/it_network_dr.html

http://www.disasterrecovery.org/plan_steps.html

https://www.fema.gov/media-library-data/1392217307183-56ed30008abd809cac1a3027488a4c24/2014_business_user_guide.pdf

http://gao.gov/assets/80/77142.pdf

http://www.idealintegrations.net/disaster-recovery-and-business-continuity/

http://www.infoentrepreneurs.org/en/guides/crisis-management-and-business-continuity-planning/

http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf

https://www.interstaterestoration.com/blog/why-business-impact-analysis-bia-important

http://www.mir3.com/30-five-phases-of-bc-planning/

https://oig.justice.gov/reports/USMS/a0429/app5.htm

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

https://www.sans.org/reading-room/whitepapers/recovery/computer-security-considerations-disaster-recovery-planning-1512

https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164

https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-survivability-security-1274

https://www.sans.org/reading-room/whitepapers/recovery/oversight-physical-security-contingency-planning-557

https://www.sans.org/reading-room/whitepapers/recovery/preparing-disaster-determining-essential-functions-first-1658

https://www.sans.org/reading-room/whitepapers/recovery/requirements-design-secure-data-center-561

http://searchdisasterrecovery.techtarget.com/essentialguide/Essential-guide-to-business-continuity-and-disaster-recovery-plans

http://searchstorage.techtarget.co.uk/tip/Business-impact-analysis-BIA-process-basics

http://searchdisasterrecovery.techtarget.com/tip/How-to-establish-a-recovery-time-objective-RTO

http://searchdisasterrecovery.techtarget.com/tip/Strategies-for-locating-a-recovery-site

http://slideplayer.info/slide/2777317/

http://www.slideshare.net/ATBHATTI/audit-checklist-for-information-systems-14849697

http://whatis.techtarget.com/definition/contingency-plan

https://www.wolfandco.com/insight/using-business-impact-analysis-and-risk-assessment-prepare-business-disruptions

http://www.wolfpacsolutions.com/articles/using-business-impact-analysis-prepare-emergency

## Electronic Documents

Federal Financial Institutions Examination Council (FFIEC). February 2015. Business Continuity Planning (BCP) IT Examination Handbook. Retrieved from http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/business-impact-analysis.aspx

United States Government Accountability Office (GAO), February 2009, Federal Information System Controls Audit Manual (FISCAM). Retrieved from http://www.gao.gov/new.items/d09232g.pdf

Marianne Swanson et al, May 2010 NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

## Documents

Office of the Auditor General, July 2007. Report on Performance Study of Government Information Systems Organisation - Business Continuity Planning for the period January 2006 – December 2006

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

# APPENDICES

## APPENDIX I – BCP Matrix Planning Grid

| Category | Number of risks | Audit Objectives |
|---|---|---|
| **IT Governance** | **0** | |
| IT Strategy and Planning | | |
| Organisational structures, Standards, Policies and Procedures | | |
| Internal Control | | |
| Investment Decisions | | |
| IT Operations | | |
| People and Resources | | |
| **IT Operations** | **0** | |
| IT Service Continuity management | | |
| Service Level Agreement | | |
| Information Security Management | | |
| Capacity Management | | |
| Problem and Incident Management | | |
| Change Management | | |
| **Development & Acquisition** | **0** | |
| Requirements Development & Management | | |
| Project Management & Control | | |
| Quality Assurance & Testing | | |
| Solicitation | | |
| Configuration Management | | |
| **Outsourcing** | **0** | |
| Outsourcing Policy | | |
| Solicitation | | |
| Vendor / contract Management | | |
| Service Level Agreement (SLA) | | |
| Benefit Realisation | | |
| Security | | |
| **Information Security** | **0** | |
| Risk Assessment | | |
| Security Policy | | |
| Organisation of IT Security | | |
| Communications & Operations Management | | |
| Asset Management | | |
| Human Resources IT Security | | |
| Physical and Environmental Security | | |
| Access Control | | |
| IT Systems Acquisition, Development and Maintenance | | |
| IT Security Incident Management | | |
| Compliance | | |
| **Business Continuity and Disaster Recovery** | **7** | |
| Business Continuity Policy, Plan and Organisation | 1 | To assess whether DITES has developed and instituted an effective business continuity policy |
| Establishment of Business Continuity Function | 1 | To assess whether DITES has an adequate business continuity team in place |
| Business Impact Assessment and Risk Management | 1 | To assess whether DITES has performed and completed a business impact assessment and/or risk assessment and has a risk management system in place. |
| Preventive and environmental controls | 1 | To determine whether the DITES has suitable environment control at back-up sites. |
| Disaster Recovery Plan | 1 | To assess whether the Business Continuity Plan includes back-up and recovery plans for hardware, data, application software and data centre (recovery) and has been suitably implemented? |
| Testing | 1 | To assess whether the business continuity disaster recovery procedures have been tested |
| Security | 1 | To assess whether business continuity plan and disaster recovery plan ensure security of data, application software, hardware and data center. |
| **Application Controls** | **0** | |
| Input Controls | | |
| Processing Controls | | |
| Output Controls | | |
| Application security controls | | |
| **TOTAL** | **7** | |

## APPENDIX II – Business Continuity Planning Matrices

| Business Continuity Policy | |
|---|---|
| **Audit objective:** To assess whether the DITES has developed and instituted an effective business continuity policy | |
| **Audit Issue: Policy**<br>Does the DITES have a contingency plan and/or policy for business continuity and/or disaster recovery? | |
| **Criteria:**<br>DITES has a published/approved and adopted contingency plan and has a policy in place that comprehensively covers all areas of contingency operations and clearly identifies training requirements and testing schedules. | |
| **Information Required:**<br>▪ Business Continuity Policy Document<br>▪ Disaster Recovery Policy Document<br>▪ IT Policy Document<br>▪ Approval process for adoption of business policy objectives<br>▪ Correspondence and minutes of meetings related to business continuity/disaster recovery | **Analysis Method(s):**<br>▪ Document review for assessing that the policy is consistent with the DITES overall IT policies.<br>▪ Document review to assess that the policy addresses requirements of business continuity by defining DITES contingency objectives, DITES framework and responsibilities for contingency planning.<br>▪ Review or interview personnel to determine how often the policy is updated if conditions change.<br>▪ Review policy to determine who approved it and when was it last distributed /interview a sample of business users to assess if the policy has been sufficiently communicated within DITES. |
| **Audit Conclusion:** | |

| Organisation of Business Continuity Function | |
|---|---|
| **Audit objective:** To assess whether an adequate business continuity team is in place. | |
| **Audit Issue 2**: **Business Continuity Function**<br>Is there a business continuity team or equivalent function in place? | |
| **Criteria:**<br>Coverage of all critical areas of the DITES in the team. Roles and responsibility requirements for the team members. | |
| **Information Required:**<br>▪ Organisational chart of DITES<br>▪ DITES chart of business continuity team<br>▪ Role/responsibility description of the business continuity team members<br>▪ Correspondence/meeting minutes on issues of business continuity<br>▪ Business continuity plan | **Analysis Method(s):**<br>▪ Document review / Interview relevant staff to assess that all critical areas of DITES are represented in the business continuity team or equivalent<br>▪ Document review to assess that there is adequate ownership and assignment of Business continuity responsibility on the senior management. For example, has the management identified the level and urgency of recovery, and is this reflected in the policy?<br>▪ Document review to assess that all critical departments have assigned team members for disaster recovery and their roles are clearly laid out.<br>▪ Interview a sample staff in business continuity team / |

| | |
|---|---|
| | equivalent to assess that they are aware of their roles for business continuity for each critical business organisation/department. |
| **Audit Conclusion:** | |

| Business Impact Assessment | |
|---|---|
| **Audit objective**: To assess whether the business impact assessment and risk assessment have been completed and a risk management system is in place. | |
| **Audit Issue 3: Risk Assessment**<br>Have business impact analysis and risk assessments been carried out and critical data, application software, operations and resources been identified and prioritised? | |
| **Criteria:**<br>▪ Enterprise Risk Management framework or equivalent<br>▪ Business Continuity Policy or equivalent<br>▪ Completion of the Business Impact Assessment and identification of critical data, application software, operations and resources. | |
| **Information Required:**<br>▪ Risk Assessment report(s)<br>▪ Business impact assessment report(s)<br>▪ List of critical data, application software, operations and resources for each function<br>▪ List of residual risks<br>▪ List of related stakeholders<br>▪ Review report(s) on risk and business impact assessment<br>▪ Enterprise risk assessment policy/ framework<br>▪ Minutes of meetings on risk assessment and business impact assessment. | **Analysis Methods:**<br>▪ Document review to assess that the risk assessment was carried out, probable threats and their impacts are identified.<br>▪ Document review to assess that all functional areas were considered in the risk assessment and impact assessment.<br>▪ Document review to assess that the impact analysis evaluated the impact of any disruption in relation to time and other related resources and systems.<br>▪ Document review to assess that the decision on residual risks were taken at appropriate level.<br>▪ Document review to assess that DITES has determined RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) for each critical application.<br>▪ Document review to assess that the RTOs and RPOs are practical and reasonable for each application and line of business or function.<br>▪ Document review to assess that the senior management involvement/ approval.<br>▪ Document review to assess that relevant stakeholders were involved in risk identification and impact assessment. |
| **Audit Conclusion:** | |

| |
|---|
| **Audit Issue 4: Risk Management**<br>Is a risk management process (including mitigation and tracking, etc.) in place and have emergency processing priorities been established? |

**Criteria:**

- Coverage of the risk management process vis-a-vis risk assessment and business impact assessment.
- Risks and emergencies are promptly addressed as per organisation's agreed parameters.

| **Information Required:** | **Analysis Methods:** |
|---|---|
| ▪ Information Required<br>▪ Risk Management process document<br>▪ Risk Assessment and Business Impact Assessment Report(s)<br>▪ List of all relevant personnel, members of the BCP team with roles and responsibilities<br>▪ List of prioritized items for emergency process<br>▪ List of residual risks identified<br>▪ List of instances of emergency process being invoked<br>▪ Emergency process/response reports. | ▪ Document review to assess that the risk management process addresses all high priority items.<br>▪ Interview and document review to assess that all relevant personnel, including senior management are aware of their role and responsibilities and carry them out.<br>▪ Document review to assess that the residual risks do not have material impact on the organisation.<br>▪ Document review and observation to assess that the emergency instances are adequately handled.<br>▪ Document review to assess impact of the emergency.<br>▪ Review meeting minutes or list of risks to determine that risks have been assigned, mitigation activities defined, and that risks are tracked periodically and status updated. |

**Audit Conclusion:**

| Documentation |
|---|
| **Audit objective:** The business continuity plan is adequately documented to conduct effective interim business activities and recovery procedures after a business interruption. |
| **Audit Issue 7: Documented plans for back-up and recovery procedures, roles and responsibilities**.<br>Does the organisation have a documented disaster recovery plan that is readily available for back-up and recovery? |

**Criteria:**

Availability and currency of the business continuity and disaster recovery plan

| **Information Required:** | **Analysis Methods:** |
|---|---|
| ▪ Business continuity plan<br>▪ Disaster recovery plan<br>▪ Version/currency of business continuity and disaster recovery plan<br>▪ Distribution list of business continuity and disaster recovery plans to all concerned. | ▪ Document review to assess the currency of the business continuity plan.<br>▪ Document review to assess the currency of the disaster recovery plan<br>▪ Verify if the latest version of business continuity plan and the disaster recovery plan are communicated to all concerned.<br>▪ Determine if the business continuity and disaster recovery plan documents are available at off-site to be available in case of a disaster.<br>▪ Verify that roles and responsibilities of back-up and disaster recovery team/ related staff are clearly listed out.<br>▪ Interview a sample of staff to assess whether disaster recovery procedures are known and understood. |

**Audit Conclusion:**

| Security | |
|---|---|
| **Audit objective:** To assess whether business continuity plan and disaster recovery plan ensure security of data, application software, hardware and data centre. | |
| **Audit Issue 9: Efficiency of Security Indicators**<br>To determine whether the data, application software, hardware and data centre are secured appropriately during the back-up disaster recovery procedures? | |
| **Criteria:** Security baselines for the organisation like procedures laid down in the IT security policy and disaster recovery plans | |
| **Information Required:**<br>▪ Inventory of data, application software and hardware<br>▪ Inventory of back-up data files and application software<br>▪ Access control logs of the data files, application software as well as hardware<br>▪ Security plan for the back-up site and disaster recovery site. | **Analysis Method(s):**<br>▪ Verify if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process.<br>▪ Verify if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software.<br>▪ Verify if there has been any breach of security through examination of access control logs (physical and logical). |
| **Audit Conclusion:** | |

| Disaster Recovery Policy | |
|---|---|
| **Audit objective:** To assess whether the Business Continuity Plan includes back-up and recovery plans for hardware, data, application software and data centre (recovery) and have been suitably implemented | |
| **Audit Issue: Policy**<br>Have the data and program back-up procedures been devised and implemented effectively? | |
| **Criteria:**<br>▪ Determine the frequency of back-ups of DITES.<br>▪ Document back-up and recovery plans. | |
| **Information Required:**<br>▪ Back up plans and procedures for the hardware, data, application software<br>▪ Back-up logs/ Version logs<br>▪ Roles and responsibilities for back-up<br>▪ List of storage locations and periodicity<br>▪ Retention schedule<br>▪ Security arrangement for back-up site<br>▪ Disaster logs<br>▪ Roles and responsibilities for recovery | **Analysis Method(s):**<br>▪ Document review to assess that the back-up plan includes all critical hardware, data, and application software.<br>▪ Document review to assess that detailed back-up procedures have been devised.<br>▪ Document review to assess that the back-up plan is adequately implemented.<br>▪ Analysis of logs to assess the back-up is taken at determined timelines and is retained for the specified time period.<br>▪ Verify that the right version of back up is available. |

| | |
|---|---|
| activities<br>▪ Impact assessment of disasters<br>▪ Report on disaster recovery activities. | ▪ Document review to assess the adequacy of back-up location and the mode of transport of back up files etc. to the back-up location.<br>▪ Verify that the security, logical or physical is adequate for the back-up site.<br>▪ Verify that the back-up files can be used for recovery.<br>▪ Document review to assess that back-up procedures are implemented minimizing loss of time and resources.<br>▪ Document review to assess that detailed recovery procedure (s) has been devised and includes resetting of system parameters, installation of patches, establishing the configuration settings, availability of the system documentation and operating procedures, reinstallation of application and system software, availability of most recent backup, and testing of system.<br>▪ Document review to assess that recovery procedures are implemented minimizing loss of time and resources.<br>▪ Document review/ Interview staff to assess that the relevant staff have been trained on the back-up and recovery procedures. |
| **Audit Conclusion:** | |

| Testing the BCP/DRP | |
|---|---|
| **Audit objective:** To assess whether DITES's has tested its business continuity/disaster recovery procedures | |
| **Audit Issue: Trials**<br>Have the responsible entities tested BC and DR procedures, and what changes, (if any) have been made, because of the test? | |
| **Criteria:**<br>The entities should test the documented BCP and DRP procedures via drills or mock-ups to ensure that they work in actual conditions. Personnel involved in ensuring continuity should be aware of their roles. | |
| **Information Required:**<br>▪ BCP and DR procedures & Test procedures<br>▪ List of items for which business continuity/disaster recovery plan has to be tested<br>▪ Frequency of testing of business continuity plan and disaster recovery plan<br>▪ List of tests conducted<br>▪ List of test criteria like RTOs and RPOs etc.<br>▪ List of testing methods employed<br>▪ Test results & actions taken or test recommendations<br>▪ Follow up action on test results. | **Analysis Methods:**<br>▪ Document review to assess whether all relevant items are covered for testing.<br>▪ Document review to assess whether the tests are conducted are right intervals, in time.<br>▪ Document review to assess that the tests were conducted against identified criteria.<br>▪ Document review to assess that the tests were conducted using appropriate testing methods.<br>▪ Document review to assess that the recommendations are conveyed to appropriate authorities for follow-up.<br>▪ Document review to assess that the test recommendations are adequately followed up and the business continuity plan or the disaster recovery plan are adequately updated. |
| **Audit Conclusion:** | |