UNDP MAURITIUS

MauStats Business Continuity/Disaster Recovery Assessment

Ver 1.0

UN Internal

Digital.
For the UN family

Table of Contents

Revision History

Version:	Who:	What:	When:
0.1	Myinzu Shwe	Initial creation	18 July 2024
0.2	Myinzu Shwe	Update with information received from UNDPMau	01 August 2024
0.3	Lyle McFadyen/Myinzu Shwe	Updates with final details received from UNDPMau/ Review by Lyle McFadyen (Head, Organizational Resilience Unit, UNICC)	15 August 2024
0.4	Myinzu Shwe	Updates after review by Lyle McFadyen	19 August 2024
1.0	Lyle McFadyen	Final review	20 August 2024

Abbreviations

API	Application Programming Interface
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CD	Continuous Delivery
CI	Continuous Integration
CIB	Central Informatics Bureau
CISD	Central Information Systems Division
DevOps	Development and Operations
DMS	Data Management System
GOC	Government Online Centre
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ISO	International Organization for Standardization
ITCP	Information Technology Contingency Plan
ITSP	Information Technology Security Policy
ITSU	IT Security Unit
JWT	JSON Web Token
MauStats	Modern Statistics
MFA	Multi-Factor Authentication
MSA	MauStats Administrator
MSTT	MauStats Technical Team
OTP	One-Time Password
OWASP	Open Worldwide Application Security Project
RBAC	Role-based Access Control
SBR	Statistical Business Register
SEE	Survey of Employment and Earning
SM	Statistics Mauritius
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

1 Executive Summary

This report summarizes the information collected and evaluated during the Business Continuity/Disaster Recovery (BCDR) assessment requested by UNDP Mauritius Country Office (CO) per the Project Agreement reference UNDPMAU-2024-OPP3000210-P dated 28 May 2024. The scope of the review is focused primarily on the Modern Statistics Platform which will be henceforth referred to as "MauStats".

The BCDR assessment was conducted in July and August 2024. The data for the report is provided by UNDP Mauritius CO, which also includes questionnaires submitted to them by UNICC to acquire additional information.

This report reflects the status of the BCDR during the period of the assessment and some of the findings presented in this report may have already been addressed.

2 Introduction and Background

The Maustats platform is a system that is under development by the Statistics Mauritius (SM) with the support of UNDP Mauritius CO. It will automate data lifecycle from acquisition to dissemination and it will promote a single source of truth on data assets, also comprising a One Stop Data Hub for users to have interactive visualization with Self-Service capabilities.

Assessing the current business continuity/disaster recovery posture will highlight the risks associated with this platform. Depending on the risk tolerance of Statistics Mauritius (SM), it may also identify additional mitigation measures to protect against potential exploits. A prioritized plan for implementing the identified gaps will be proposed.

3 Scope and Purpose

The scope includes a business continuity evaluation for the MauStats platform.

The purpose is to provide an assessment report that evaluates the completeness and effectiveness of the business continuity plan, the disaster recovery plan/IT contingency plan, and the presence and maintenance of fault-tolerant and redundant systems, including hardware, backup processes, and storage.

The report will be based on best practices to support mitigation and recovery of the platform. It will also include recommendations which should be considered relevant to business continuity and disaster recovery organizational policies and procedures.

4 Context

The MauStats platform is essential for data collection, aggregation, calculation, analysis, and visualization, meeting the varied needs of Statistics Mauritius (SM). To ensure uninterrupted service, an IT Contingency Plan for the MauStats was developed to address potential disruptions and maintain business continuity.

5 Contingency Plan

5.1 Systems Overview

As outlined in the document "04.01c IT Contingency Plan-MauStats Platform v3",

Quote

> *Statistics Mauritius (SM) has developed Modern Statistics (MauStats) platform to automate and the data lifecycle from acquisition to dissemination. The platform comprises of a robust and scalable data layer with interfacing capabilities via Application Programming Interface (APIs). It will promote a single source of truth on data assets and also comprise a One Stop Data Hub for users to have interactive visualization with Do Your Own Analysis (Self-Service) capabilities.*
>
> *The MauStats design and development is following a phased approach, which offers numerous advantages and opportunities for successful implementation. This approach will benefit incremental and gradual development, enhanced capacity development, cost optimization, flexibility, adaptability, risk mitigation, increased user engagement, iterative improvement, scalability, reduced disruption, and stakeholder's alignment. These advantages contribute to the overall effectiveness and efficiency of the MauStats implementation.*

Unquote

5.2 Scope (Disasters Scenarios)

5.2.1 Existing disaster scenarios

As mentioned in the document "04.01c IT Contingency Plan-MauStats Platform v3", the contingency plan aims to maintain the persistent accessibility, reliability, and protection of the MauStats web application and its related data, safeguarding against any interruptions, crisis, or security breaches.

The disaster scenarios included in the recovery plan:

- Natural Disasters
- Hardware Failure
- Power Failure
- Network Failure

- Storage Failure
- Resource Exhausted.

5.2.2 Further disaster scenarios for consideration

The following scenarios to further consider and reflect with the evolving nature and pattern of disasters and crises:

- Cybersecurity Incidents: ransomware attacks, hacking, and data breaches
- Human Error: Accidental data deletion, misconfiguration of critical systems, etc.
- Physical Security Incidents: Workplace violence, theft, or vandalism
- Social unrest: strikes, riots, etc.
- Supply Chain Disruptions: Vendor failures, transportation delays, or resource shortages
- Technological Failures: data loss or breach
- Utility Outages: water supply disruption, or telecommunications failure.

5.3 Recovery Support Resources

5.3.1 Recovery Support Resources Strengths

Roles and Responsibilities

Strength: The roles and responsibilities of the SM Management, MauStats Core Team, MauStats Administrator, SM IT Support Team, SM Staff, and Government Online Centre (GOC) are well defined in the 04.01c IT Contingency Plan-MauStats Platform v3.

A Continuity Manager is available.

5.3.2 Recommendation for Improvement – Recovery Support Resources

StatsMau maintains the information on whom to contact during emergency situations. However, it is recommended to maintain the list with the names, contact information (phone/email) and roles within the IT Contingency document itself to facilitate the identification of appropriate contacts in the event of an emergency. Include alternates if possible. Having this information readily available would streamline communication in times of critical need.

The information would include:

- Business owners
- ICT Resources and Contacts
- Third-Party Resources.

Business Owners / ICT Resources and Contacts

Contact Name	Contact Telephone / Email	Role

Third-Party Resources

Organisation	Name/Team	Contact telephone / Email	Name of Alternate	Role & Notes

It is advisable to maintain a list in an annex to facilitate management. However, ensure that a reference to this annex is included in the relevant section. This will prevent the inconvenience of searching for contact names, numbers, or emails during critical moments.

6 MauStats Platform

6.1 Infrastructure Context

The platform is deployed in the GOC infrastructure.

6.1.1 Strengths - Infrastructure

1. There are two environments created using the GOC infrastructure – Staging and Production. For each of the environment two VMs are configured and installed one each for Application and Database. They are hosted in the Cloud. The presence of a Staging environment offer the advantages of risk mitigation (testing and quality assurance), performance evaluation, operational efficiency (streamlines deployment process), security testing (for vulnerabilities) and isolation of changes (updates can freely perform updates and tests without causing intrusive breaks to the live production environment).

2. There exist multiple internet links to ensure network availability.

3. The power grid has different power feeds and electrical power are distributed in racks with PDUs (power distribution units). The data center has generators as well as UPS' (uninterruptable power supplies).

4. GOC's data center has its own HVAC (heating, ventilation and air conditioning) which separate from the building.

5. The platform is deployed in the GOC infrastructure which is secured and protected under the restricted Data Centre Hosting Guidelines. The IT infrastructure aligns to GOC security policies and procedures which is based on the ISO 27002 standards. Note that the guidelines are created and managed by GOC.

*** The ISO 27001 certification process is currently underway at the time of this report's creation.

6. The GOC has maintenance contracts for IT assets with suppliers. Routine health assessments are scheduled and performed.

7. Availability of a reliable backup system,
   - backup software utilized is VEEAM
   - CRON job is scheduled to perform backup of the MongoDB database. MongoDB backup is copied to a separate VM. Backups are performed after every 6 hours and the last 10 backups are kept. The backup and virtual machine (VM) backup processes are conducted separately.
   - primary input and ingested data files are backed up to disk, another server on the GOC Cloud
   - full backups are performed for both the VM and Database
   - backups are encrypted
   - database backup and restore tested; a routine schedule for backup and restoration has been established.

6.1.2 Recommendations for Improvement - Infrastructure

i. GOC datacenter does not have a secondary site which may possibly result in,
   - Limited geographic redundancy: with a single data center, there's a lack of geographic redundancy. This means that in the event of a disaster, such as a natural disaster or power outage, there's a higher risk of service interruption or data loss
   - Potential for Downtime: If the sole data center experiences issues, there's no backup location to take over, which can lead to significant downtime and potential loss of business
   - Scalability Limitations: Expansion is limited by the capacity of the single location. If demand exceeds the current infrastructure, it can be difficult and time-consuming to scale up.
   - UNDPMAU may wish to consider either migrating the system to the Cloud, or leveraging a failover of the system in the Cloud

ii. Hosting environment
   - Provide a comprehensive background of the GOC data center. Include details such as whether it is a cloud environment in Azure or AWS, specify the region or availability zone, and indicate the environment in which the virtual machines (VMs) are hosted. Additionally, identify who has administrative access, including the primary contact point and an alternate. Essentially, consider the questions: "Where are the systems located, and who should be contacted in case of an issue?"

   Note: When hosted in the cloud, the provider's ISO certifications significantly alleviate the burden on UNDP-MAU

iii. Network topology
   - It is advisable to document the topology of the UNDMAU to include the following:
     a. Which ISP are onsite: name of provider, bandwidth provided, who to contact if there is an issue (primary contact plus alternate)?
     b. Include a copy of the network diagram in the annex, or provide a link to the document (regularly review the link so you know it still works)

c. Does the multiple ISP providers share the same underlying infrastructure? If so, it would be advisable to consider a second provider (who does not share underlying infrastructure outside of UNDP-MAU in case of an outage)

6.2 Recovery Plans

6.2.1 Current Recovery Plans

The MauStats Platform has a broad and strategic blueprint that is tailored to guide and steer the process of recovery initiatives from a significant disruption or disaster to cover threats as mentioned in Section 5.2.1 Existing disaster scenarios. The processes consist of:

- Incident Detection and Assessment (Incident Management)
- Activation of the Response Plan (Crisis Management)
- Isolation and Containment (Incident Management)
- Data Backup and Recovery (Recovery)
- Infrastructure Restoration (Recovery)
- Testing and Validation (Recovery)
- Communication and Documentation (Service Management)
- Post Incident Analysis (Incident Management) and Improvement (Continual Improvement)

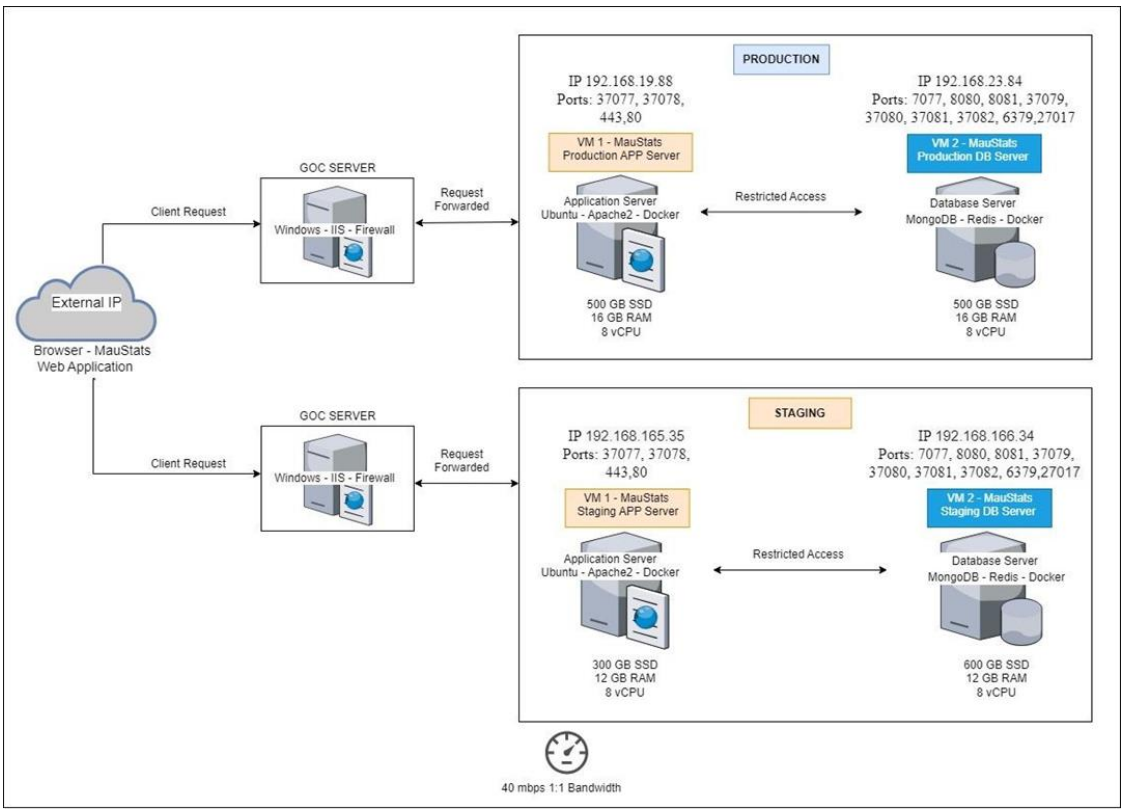
There is currently a procedure in the event there is a cyclone, with the following details:
Quote

a. *The data centre is on the 5th floor; hence the risk of flash flood is minimised.*
b. *Equipped with FM200 fire suppression system.*
c. *Risk Treatment Plans for hardware, power, network, storage failures risks are elaborated in the GOC ISMS.*
d. *Allowable downtimes are elaborated in the GOC ITCP which is currently being reviewed.*
e. *RPO - 24 hrs and RTO - 3 hrs*

Unquote

The contingency strategies for potential disruptions have been established, as illustrated in the visual representations for each scenario (refer to Sections 3.2.1 through 3.2.6 in 04.01c IT Contingency Plan-MauStats Platform v3).

The configuration and architecture diagram of the virtual machines is available.



6.2.1.1 Recommendation for Improvement – Recovery Plans

i. The necessary steps or processes have been outlined; however, they lack sufficient detail. Providing additional information would enhance their comprehensiveness, such as

   a. HOW would the incident be detected?
   b. WHO would it be escalated to? Recommend adding a checklist/procedure for each section which includes who to contact, which teams to mobilize, and so forth.
   c. WHO decides to activate the recovery plan, and WHEN?
   d. Would the incident be escalated to anyone else (IT and Information Security recovery teams, etc...?)
   e. Are there pre-defined recovery teams? Who are they? How do you contact them to activate them and get updates?
   f. Testing and validation - who will do it, how will they test? Is there a document that testers can use (a checklist?)
   g. Communication and Documentation: Needs more information... List of contact points, etc... Use the roles and responsibilities section to help flesh this out.

ii. Developing a more system/service overview that covers the following features:

   - Hosted Business-Critical Systems on the server (list of applications)

- Service Dependencies: details of any services/applications that the recovery of this service is dependent on with those that need to be recovered first (service name | description of the dependency | comments (if any))
- Service Critical Software, Certificates, Licenses and Document: If applicable, provide details of any software, licenses, certificates and documents that are required to recover this service in the event of a disaster
- Recovery Environment Requirements: Access Rights, Service Response Time, Availability Requirements.

iii. It would also be an asset to include Fall Back Procedures for the following reason, to ensure that there is an alternative path to continue operations and minimize disruptions if the primary plan fails. It offers a strategic guide to maneuver through unpredictability and maintain the course of the operation, notwithstanding unexpected obstacles.

iv. Ensure that a group of users is available to test the system upon its recovery. Additionally, develop a recovery test plan to guide them on what aspects to review and test once the system is operational again.

v. It is advisable to have an incident template prepared for use in the event of a disruption. This will facilitate the tracking of the incident and, most importantly, ensure that lessons learned are documented.

Note that natural disasters have not yet been incorporated into the IT Continuity Plan (ITCP). The plan is currently under review, and provisions for natural disasters will be included.

6.3 Recovery Plan (Disaster Recovery) Exercises

The Recovery Plans have not been tested but per information provided,

i. Resources as and when required are upgraded by GOC
ii. Regular fire drills conducted by Landscope Mauritius
iii. Regular maintenance and test of FM 200
iv. Power generator test done by Landscope every week
v. Redundancy test done at time of implementation of servers and networking equipment.

6.3.1 Recommendation for Improvement – Recovery Plan Exercises

Disaster recovery exercises offer several advantages, including the assurance of operational continuity, the enhancement of personnel competencies, the maintenance of current documentation, the optimization of recovery durations, and the reinforcing of stakeholder trust. These exercises are instrumental in guaranteeing that, should an interruption occur, the organization is equipped to actuate an efficacious response and expedite the restoration of operational functions with minimal delay.

There are several types of exercises that can be performed contingent on the availability of resources and time at the organization's disposal:

- Walkthroughs: Basic exercises that involve a step-by-step review of a plan or procedure, often with the actual emergency team.
- Tabletop Exercises (TTX): Discussion-based sessions where team members navigate through a scenario using their roles and responsibilities within the organization's emergency plan.
- Functional Exercises: More dynamic than tabletop exercises and involve simulating the emergency operations center or other aspects of the command structure to see how teams respond in real time.
- Full-Scale Exercises: Most complex and resource-intensive exercises, these involve activating all components of the emergency plan, often including coordination with external agencies and actual deployment of resources as if a real incident had occurred.

7 Business Impact Analysis (BIA)

A BIA was conducted six years ago in 2018. Although there is an ongoing GOC ITCP review, it is advisable to reassess the BIA or conduct a new BIA, given that the last assessment was completed so long ago.

7.1 Recommendation for Improvement – BIA

While conducting Business Impact Analysis (BIA) is demanding in terms of resources and time, it does help determine how disruptions may impact an organization.

Regularly conducting BIAs is essential for business continuity. The recommended frequency varies, but typically, businesses perform BIAs annually or every two years. The last BIA was completed in 2018, hence it is recommended to conduct a new Business Impact Analysis (BIA), followed by less intricate surveillance BIAs (annual review) over the subsequent two years, with this cycle repeating.

8 IT Contingency Plan and Continuous Improvement

There is a planned solution for the BC/DR once the production platform is in production. As stated in the document "04.01c IT Contingency Plan-MauStats Platform v3"

Quote

> *The ITCP is a dynamic document that undergoes regular review, updating, and testing to reflect changes in technology, business requirements, and emerging threats. Continuous improvement efforts ensure the ITCP remains effective and responsive to evolving risks and challenges.*

Unquote

9 Business and Service Continuity Governance

The document available that defines governance and policies is covered in the document “04.01c IT Contingency Plan-MauStats Platform v3”.

10 Recommendations for Improvement

i. The overall design of the document is good, but it may be better to separate technical recovery activities into a separate document (the actions that system administrators would undertake to restore the systems) and use the rest to build a high-level continuity document. Then each document can refer to the other for specific details.

ii. *"Regular training sessions should be conducted to ensure the stakeholders are familiar with the plan and their roles during an incident."* - It is advisable to establish an annual schedule for this task, as it will serve as a helpful reminder.

iii. *"The platform is deployed in the GOC infrastructure. GOC is a member of Government services and comes under critical sector. Their role is to facilitate identification, prioritization, assessment and protection of critical information infrastructure through information sharing and reporting."* - It is recommended to include more information about this environment in the contingency plan, including contact points, administrators, etc.

iv. *"The platform is deployed in the GOC infrastructure which are secured and protected under the restricted Data Centre Hosting Guidelines."* - It is recommended to provide a link to those guidelines.

v. *"Hardening of operating system, database and web server have been performed on the platform servers in both the staging and production environment."* - This should be regularly reviewed to ensure that the hardening is up to date

vi. "Symantec Endpoint Protection Antivirus and anti-malware software version 14.3 is installed by the IT unit on the staging and production servers." - Recommend removing the system version and include a contact point (and alternate) for who is responsible for maintaining this application.

vii. Incorporating hyperlinks when referencing documents within the IT Contingency Plan (for example, “The platform is deployed in the GOC infrastructure which are secured and protected under the restricted **Data Centre Hosting Guidelines**.”)

11 Conclusion

It was identified the absence of certain Business Continuity and Service Continuity governance documents and policies. Specifically, Statistics Mauritius lacks crucial elements of Business Continuity and Service Continuity (BC/DR) Governance in the following areas:

- Service Continuity vision and policy

- Business Continuity policy
- Service Continuity processes/procedures

Disaster Recovery plan management: DR plans are in place but could benefit from testing, and outcome analysis (lessons learned). Existing Disaster Recovery plans have not been recently tested. It is important to stress the importance of testing plan to assess their effectiveness and to identify areas of improvement.

The absence of such elements increases the risk of delayed decision making, assignment of responsibilities, and could affect the ability to ensure the timely restoration (services can be restored as per RTO/RPO requirements) of business-critical operations.

Adoption of best practices defined in ISO 20000 (Service Management System) and ISO 22301 (Business Continuity Management System) can help MauStats in achieving a good level of Governance.

Statistics Mauritius can accelerate their governance processes by seeking hosting facilities or providers that have the following certifications:

- ISO 22301 (Business Continuity)
- ISO 20000 (Service Management)

(It is noted that the hosting facility (GOC) is currently undergoing the process of obtaining ISO 27001 certification for information security.)