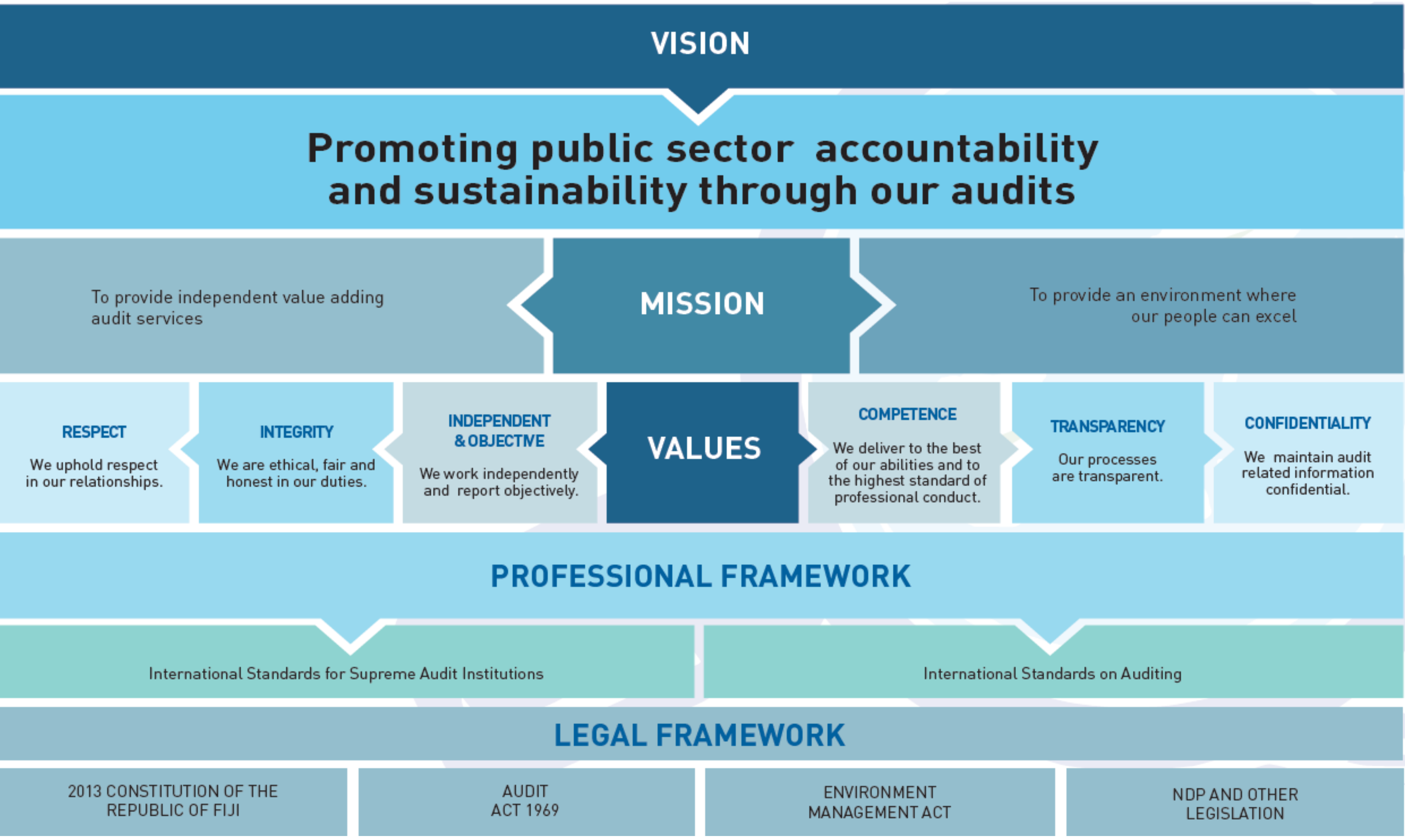
OFFICE of the AUDITOR GENERAL
Republic of Fiji

REPORT OF THE AUDITOR-GENERAL
REPUBLIC OF FIJI

COMPLIANCE AUDIT REPORT

PARLIAMENT OF FIJI
PARLIAMENTARY PAPER NO. 269 OF 2020

OFFICE *of the* AUDITOR GENERAL
Republic of Fiji



VISION

Promoting public sector accountability and sustainability through our audits

MISSION

To provide independent value adding audit services

To provide an environment where our people can excel

VALUES

RESPECT
We uphold respect in our relationships.

INTEGRITY
We are ethical, fair and honest in our duties.

INDEPENDENT & OBJECTIVE
We work independently and report objectively.

COMPETENCE
We deliver to the best of our abilities and to the highest standard of professional conduct.

TRANSPARENCY
Our processes are transparent.

CONFIDENTIALITY
We maintain audit related information confidential.

PROFESSIONAL FRAMEWORK

International Standards for Supreme Audit Institutions

International Standards on Auditing

LEGAL FRAMEWORK

2013 CONSTITUTION OF THE REPUBLIC OF FIJI

AUDIT ACT 1969

ENVIRONMENT MANAGEMENT ACT

NDP AND OTHER LEGISLATION

Location : Level 8, Ratu Sukuna House
2-10 MacArthur Street
Suva, Fiji

Postal : P O BOX 2214, Government Buildings
Address Suva, Fiji

Telephone : (679) 330 9032

Email : info@auditorgeneral.gov.fj

Website : www.oag.gov.fj

OFFICE OF THE AUDITOR GENERAL

Promoting Public Sector Accountability and Sustainability Through our Audits

6-8TH Floor, Ratu Sukuna House
2-10 McArthur St
P. O. Box 2214, Government Buildings
info@auditorgeneral.gov.fj
Suva, Fiji

Telephone: (679) 3309032
Fax: (679) 330 3812
E-mail:
Website: http://www.oag.gov.fj

File: 102

02 December 2020

The Honorable Ratu Epeli Nailatikau
Speaker of the Parliament of the Republic of Fiji
Parliament Complex
Gladstone Road
SUVA

Dear Sir

AUDIT REPORT ON COMPLIANCE AUDITS

In accordance with section 152(13) of the Constitution of the Republic of Fiji, I am pleased to transmit to you my report on Compliance audits.

A copy of the report has been submitted to the Minister for Economy who as required under section 152(14) of the Constitution shall lay the report before Parliament within 30 days of receipt, or if Parliament is not sitting, on the first day after the end of that period.

Yours sincerely

Ajay Nand
AUDITOR-GENERAL

AUDITOR-GENERAL
FIJI

Encl.

The Office of the Auditor-General – Republic of Fiji

The Office of the Auditor-General is established as an Independent Office by the Constitution of the Republic of Fiji. Its roles and responsibilities include carrying out audits to determine whether an entity is achieving its objectives in compliance with relevant legislations. These audits are carried out by the Auditor-General on behalf of Parliament.

The Auditor-General must submit a report on compliance audits carried out to Parliament. In addition, a single report may include two or more audits. This report satisfies these requirements.

The Office of the Auditor-General notes the impact of its reports to Parliament on the ordinary citizens and strives for accuracy and high quality reporting including recommendations which are not only value-adding to the entity subject to audit but its customers and the general public as well.

REPORT OF THE AUDITOR GENERAL
REPUBLIC OF FIJI

Audit Reports on:

1. COMMENCEMENT OF QUARRY DEVELOPMENT PROJECTS
   AND
   APPOINTMENT OF CERTIFIED FOREMAN-IN-CHARGE
2. GOVERNMENT PAYROLL SYSTEM
3. FINANCIAL MANAGEMENT INFORMATION SYSTEM
4. FIJI EDUCATION MANAGEMENT INFORMATION SYSTEM (FEMIS)

COMMENCEMENT OF QUARRY DEVELOPMENT PROJECTS AND APPOINTMENT OF CERTIFIED FOREMAN-IN-CHARGE

Table of Contents

Acronyms

Abbreviation	Meaning
ACP	African Caribbean Pacific Nations
DMR	Department of Mineral Resources
DoE	Department of Environment (Ministry of Waterways & Environment)
DoL	Department of Lands
DTCP	Department of Town and Country Planning
EIA	Environment Impact Assessment
EMA	Environment Management Act
EMP	Environment Management Plan
EU	European Union
ISSAI	International Standards for Supreme Audit Institutions
iTLTB	iTaukei Lands Trust Board
OAG	Office of the Auditor-General
OHS	Occupational Health and Safety
PEM	Principal Engineer Mines
PEO	Principal Environment Officer
PPQA	Policy Planning Quality Assurance
PSLMR	Permanent Secretary Lands and Mineral Resources
QFIC	Quarryman Foreman-in-charge
QOEMP	Quarry Operational Environmental Management Plan
SEM	Senior Engineer Mines
SG	Solicitor General
SOP	Standard Operating Procedures
SPC	Pacific Community
STA	Senior Technical Assistant
TOII	Technical Officer II

1.0 EXECUTIVE SUMMARY

The Office of the Auditor-General conducted a compliance audit on the approval for commencement of quarry development projects and appointment of certified foreman-in-charge of quarry, by the Department of Mineral Resources ("DMR").

Our audit was conducted in accordance with the functions of the Auditor-General specified in the Audit Act 1969 and Section 152 of the 2013 Constitution of the Republic of Fiji. These provide powers to the Auditor-General to conduct compliance audits as stipulated in Section 6A of the Audit Act 1969.

The primary objective of the audit was to obtain sufficient and appropriate audit evidence to form a conclusion on whether the Department of Mineral Resources complied with requirements of the Quarries Act 1939 and Quarries Regulations 1939 in approving the commencement of quarry development projects and appointment of certified Foreman-in-charge of quarry development.

The results of the audit from the records and information provided indicated that the approvals for commencement of quarry development projects and appointment of certified foreman in charge did not comply, in all material respects, with the requirements of the Quarries Act 1939, Quarries Regulation 1939 and the Department's Standard Operating Procedures. Poor records management is a major contributing factor to the absence of mandatory documents required to be maintained.

Our audit also highlighted the lack of coordination and information sharing between the relevant government agencies. There are significant opportunities to improve coordination with other relevant agencies to ensure that that the DMR is kept informed when applications for quarry developments are received by other government agencies.

Our audit focused on the responsibilities of the DMR in providing approvals for the period 1 January 2016 to 31 December 2019 for the following:

1. Approval and commencement processes for quarry development projects' and
2. Appointment and commencement of Quarryman/ Foreman-in-Charge

A total of twenty (20) approvals were made for the period 2016 to 2019 which were reviewed during our audit together with the records filed by the respective certified quarryman in charge.

The Office of the Auditor-General acknowledges the assistance provided during the audit and the great efforts made by the Department of Mineral Resources to promptly implement the recommendations made.

2.0 AUDITING STANDARDS

Our audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAI 4000) on compliance auditing.

3.0 SUBJECT MATTER & SCOPE OF AUDIT

The subject matter for this audit was approval process for commencement of quarry development and appointment of certified foreman in charge of the quarry by the DMR from the period 1 January 2016 to 31 December 2019.

Through this audit, we determined whether the DMR complied, with all material aspects, with the Quarries Act 1939, Quarries Regulation 1939, related standard operating procedures, and criteria specified in **Section 4.0** of this report.

4.0 AUDIT CRITERIA

The DMR, as a government agency, must operate in an environment with due consideration of legislations and policies. The criteria for the audit was based on regulations and manuals/guidelines designed to ensure compliance with laws governing quarry developments. These include:

- Quarries Act 1939
- Quarries Regulations 1939
- Environment Management Act 2005
- State Lands Act 1945
- State Lands (Leases and Licenses) Regulations 1980
- Land Use Act 2010
- Land Use Regulations 2011
- iTaukei Land Trust Act 1940
- iTaukei Land Trust (Leases and Licences) Regulations 1984
- Town Planning Act 1946
- Town Planning Act General Provisions

5.0 AUDIT METHODOLOGY

Our audit was conducted based on the information and records provided by the DMR including information requested from other relevant agencies that included Department of Environment, Department of Town & Country Planning, Department of Lands and the iTaukei Lands Trust Board. In executing this audit, various approaches were exercised which included:

(i) Documents reviews;
(ii) Interviewing relevant officials of the DMR; and
(iii) Analysing listings provided by related agencies.

6.0 AUDIT FINDINGS

6.1 Approval of Commencement of Quarry Development Projects

6.1.1 Commencement of quarry operations without the approval of the DMR

The Department of Mineral Resources (DMR) generally derives its power to issue approvals for quarry development undertakings from the provisions of Section 2A of the Quarries Regulations. The section stipulates that the Director may, by notice published in the Gazette, declare a quarry or a part of a quarry, specified in the notice to be a prescribed undertaking. The approvals issued to the quarry owners/operators or agent are in the form of a notification letter subject to specific terms and conditions.

There are other major prerequisites prior to the issuance of an approval letter from the DMR. These requirements are mandated by law which are administered by the custodian agencies. For example, approval of the Environment Impact Assessment (EIA)/Environment Management Plan (EMP) by the Department of Environment is a mandatory requirement of the Environment Management Act (EMA) 2005. The roles and responsibilities of other agencies involved with mandated requirements prior to the issuance of approval letters by the Department of Mineral Resources are discussed in Table 6.1.1.

Table 6.1.1: Roles and responsibilities of agencies

Government Agency	Roles and Responsibilities
Department of Environment (DoE)	• Conducting Environment Impact Assessment (EIA) pursuant to legal requirement in EMA 2005. • Approving EIA reports.
Department of Town & Country Planning (DTCP) & Local Authorities	• Issuance of Business Licenses for proposed operators for sand and gravel extraction. • Within Town and City areas, the zoning of development areas for sand and gravel extraction.
Department of Lands (DoL)	• To issue licenses for sand and gravel extraction on native, freehold and state land under the Rivers and Streams Act. This justification is limited to: ✓ Rivers and stream beds; and ✓ Extractions for the purpose of public access/public enjoyment. • To issue licenses for quarries under the Quarries Act but their power depends on supply to a rock crusher or treatment plant.
iTaukei Lands Trust Board (iTLTB)	• To issue licenses for sand and gravel extraction on iTaukei land under the iTaukei Land Trust Act Cap 134 and in line with common law position established in the Bailey Case in rivers and streams passing through native land.

Source: Extract from Baseline Assessment of Development Minerals in Fiji, December 2018, pp. 73-75.

The commencement of quarry operations without the approval of the Director of Mines was established from the analysis of data obtained from relevant agencies. In order to obtain an overview of whether quarry developments were subject to the approval of the Director of Mines, we obtained listings of approved quarries according to records maintained by the four agencies as stated on Table 6.1.1.

Our analysis of the data provided noted the following:

- Department of Environment had approved 25 EIA reports for quarry developments during the years 2014 to 2020[1] of which only 6 (24%) correspond to the DMR's approved listing for quarry developments.

- Department of Town & Country Planning had approved three (3) proposed subdivisions for quarries of which audit was only able to trace one (1) quarry project to the DMR's approved listing.

- Department of Lands issued leases for 18 quarry projects during the years 2014-2019 of which only one (1) quarry development project was traced to the DMR's approved listing for quarry developments.

- iTaukei Lands Trust Board issued 12 leases for industrial quarries of which only 5 (42%) matched the DMR's approved listing.

Although the above analysis was limited due to the incomplete records maintained by the DMR, there was a clear indication of quarry developments not being approved by the DMR.

During the audit, the Manager Mines explained that that there is ambiguity in the Quarries Regulations 1939 as it is unclear about the Department's role in issuing approvals/permits. The Department sought legal advice to provide clarity on its role. The legal advice indicated that there is no requirement under the Quarries Act and the Quarries Regulations for the Director of Mines to issue 'quarry permits' for quarries to be operational. The legal advice further stated that the Director of Mines may, however, wish to liaise with the other approving authorities such as Director for Environment, Director Local Government and others to be kept informed whenever these authorities receive any applications from quarries for operation or building of the same.

The Department's action on requesting legal advice is commendable. However, the lapse in time it took for the Department to arrive at the decision is of great concern, given that the Quarries regulations has been in existence since 1939.

The Permanent Secretary Lands and Mineral Resources (PSLMR) explained in a meeting[2] that the Quarries Act 1939 and its Regulations 1939, administered by the Director of Mines is in relation to Occupational Health and Safety (OHS) of the quarry operations. The registration of the quarry, obtaining of lease and work plans for the quarry in terms of business registration is not carried out by the DMR.

<u>Department's Comments</u>

The Department did try to issue a quarry permit in 2016 to Gold Rock Investment Ltd and a permit was created, however was not issued as there was no legislative power in the Quarries Act for the Department to issue Quarry permits and only an Approval to Commence Operations could be issued.

[1] Listing received on 29 May 2020

[2] Dated 23 July 2020.

Recommendation

With the legal clarification received whereby the Department is not required to issue 'quarry permits' for quarries to be operational, the Department should consider reviewing and updating the relevant legislations including taking a lead role in developing mechanisms on how collaboration between approving agencies can be improved.

6.1.2 Meeting the mandatory requirements for approval of quarry operations

Section 2A of the Quarries Regulations 1939 indicates that the Director of Mines may, by notice published in the Gazette, declare a quarry or a part of a quarry, specified in the notice to be a prescribed undertaking. DMR through the Director Mines have used this section of the regulations to exercise its power to issue approval letters for commencement of quarry operations as captured in its Standard Operating Procedures (SOP).

The DMR's SOP define the processes and parameters employed for the assessment of quarry development applications. On receipt of applications and approvals from relevant agencies, quarry proposals are assessed using the quarry development application protocols shown on ***Appendix 8.1.***

According to the above process, documents required to be submitted with any application for quarry developments as legislatively mandated[3], include the following:

1. Environmental Impact Assessment (EIA) as approved from the DoE
2. Development Lease from either the iTaukei Land Trust Board (iTLTB) or Department of Lands (DoL)
3. Written consent from the Department of Town and Country Planning (DTCP)
4. Approval and recommendations from the Local Authorities
5. Quarry Operational Environmental Management Plan (QOEMP)

The above documents together with the DMR's approval letter for commencement of quarry operations should be maintained in project files.

The DMR provided a listing of twenty (20) approved quarry development projects, within the period of 1 January 2016 to 31 December 2019. The list of the twenty (20) projects was endorsed by the Manager Mines as true record of approved quarries.

The project files for the twenty (20) approved quarries were reviewed to determine whether all mandatory requirements were met before the DMR issued approval letters for commencement of operations. From our review, we noted the following:

- None of the files contained all the mandatory required documents for approval prior to commencement of quarry operations.
- Six (6) of the files did not have any of the five (5) mandatory documents at all, while the remaining fourteen (14) files maintained partial information.

Refer Table 6.1.2 for details and Figure 6.1.2 for illustrations.

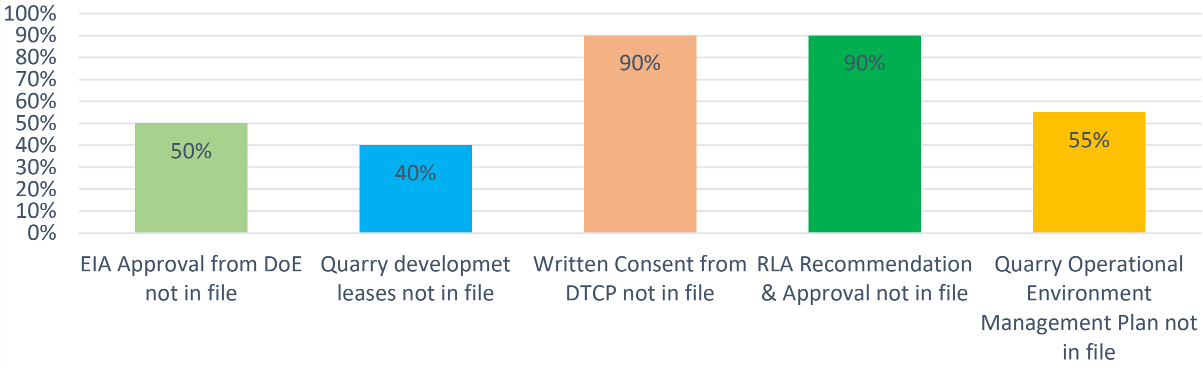
[3] ***Appendix 8.2*** details source of mandatory requirements.

Table 6.1.2: Inconsistency in maintaining mandatory required documents

[✓ Document maintained X Document not maintained]

File Reference No.	EIA - DoE Approval	Quarry Development Lease	Consent from DTCP	Local Authority Approval & Recommendation	QOEMP
1.CT 6A	X	✓	X	X	X
2. CT16AA	✓	X	X	X	✓
3. CT16BY	✓	X	X	X	✓
4. CT16CC	✓	✓	X	X	✓
5. CT16CJ	X	X	X	X	X
6. CT16CK	X	✓	X	X	✓
7. CT16CU	X	✓	X	✓	✓
8. CT16CX	✓	✓	✓	X	X
9. CT16CZ	✓	✓	X	✓	✓
10. CT16DE	X	✓	X	X	✓
11. CT16DG	✓	✓	X	X	X
12. CT16DI	✓	✓	X	X	✓
13. CT16DK	X	X	X	X	X
14. CT16DL	X	X	X	X	X
15. CT16DM	✓	✓	X	X	X
16. CT16DN	✓	✓	X	X	X
17. CT16DO	X	X	X	X	X
18. CT16DP	X	X	X	X	X
19. CT16DR	X	X	X	X	X
20. CT16DS	✓	✓	✓	X	✓

Figure 6.1.2: Inconsistency in maintaining mandatory required documents



In addition, in ten (10) of the twenty (20) cases, approval letters were not kept in project files from the DMR as required by the SOP.

The above findings indicate the records management practices in DMR are not effective whereby substantial number of documents were either misplaced or have not been properly/correctly maintained. If not addressed, there is a high risk of approvals being given for quarry developments without meeting the mandatory requirements.

DMR[4]agreed to the audit findings and recommendations and advised that necessary action will be taken to address the issues that have been raised. Upon confirmation[5], we noted that the Department has commenced remedial work beginning with the amendments to the SOP and development of a checklist for Quarry Development Approval. The documents are under the review of the Policy Planning Quality Assurance (PPQA) team at the Ministry of Lands and Mineral Resources.

Department's Comments

The approval documents are also scanned and a digital copy saved for record as well new file created for new quarry operations where a hard copy of all approval documents are kept.

To ensure the security of the files, only limited access is allowed for any movement and viewing of files at the Mines Division admin office where a biometric machine is in place for added security.

Recommendations

- **DMR should ensure that all relevant quarry documentations are properly stored and maintained. The Department could consider developing standards for the content of quarry files and verify that these standards are applied before approvals are given.**

- **DMR should strengthen its supervisory checks to ensure that processes and procedures outlined in the SOPs are complied with.**

6.1.3 Notification on commencement of quarry operations

Section 16 of the Quarries Regulations 1939 requires that the Inspector of Mines is notified two weeks prior to the commencement of a quarry operation from the quarry owners/operators, agent or foreman-in-charge of the quarry.

The duration between receiving the DMR's approval and the actual commencing date of quarrying activities varies. Therefore, following the written approval from the DMR, quarry owners/operators, agent or foreman-in-charge of the quarry are required to notify the DMR through the Inspector of Mines before actual commencement of the quarry operations.

A review of the twenty (20) quarry project files noted that only one (1) file contained the two week's notification to the Inspector of Mines prior to the commencement of its operations. Refer below for details.

[4] Exit meeting dated 23 July 2020.
[5] Signed audit verification dated 23 July 2020.

Table 6.1.3: File maintenance of two weeks' notification prior to commencement of quarry operations

Two weeks notification prior to commencement	
Maintained - 5%	
File Reference No	
CT16DI	
Not maintained - 95%	
File Reference No.	
CT16CX	CT16CK
CT16BY	CT16CZ
CT16DS	CT 16DE
CT16DK	CT16DL
CT16CJ	CT16DR
CT16DP	CT16AA
CT16DM	CT16DO
CT16CC	CT16CU
CT16DG	CT6A
CT16DN	

The implementation of Section 16 of the Quarries Regulations seemed to be heavily reliant on the quarry owners/agent or foreman-in-charge which could be beyond the control of the DMR. The limited control by the DMR, coupled with the lack of systematic monitoring, could result in the persistency of the above non-compliance in future approved quarry developments.

Discussions during the audit revealed[6] that monitoring by the Department may need to be strengthened to ensure compliance to the regulations governing quarry operations. We were also informed that certified Quarryman Foreman-in-charge (QFIC) are to be well versed with the provisions of the Quarries Regulations 1939 and there is also a level of responsibility from the quarry owners to abide by the regulations.

DMR[7] agreed to the audit findings and recommendations and have advised that necessary actions will be taken to address the issues that have been raised. The Department further stated that it will also adopt the necessary changes into the SOP for future quarry development approvals.

Department's Comments

The Inspectorate Unit conducts quarry inspections in all the three divisions (Central/Easter, Northern and Western) at least once a quarter whereby the quarry setup and site are inspected for OHS compliance as well as the record and files checked.

[6] Discussions dated 17 March 2020.

[7] Exit meeting dated 23 July 2020.

Recommendations

- **The Department should consider including a clause in its Quarry Approval Letters stating that the quarry operators are mandated to provide a notification letter to the Department two weeks prior to commencement of its operation with penalties being clearly outlined for non-compliance as required under Section 67 of the Quarries Regulations 1939.**

- **The Department should consider strengthening its monitoring role as custodian of the Quarries Regulations 1939, by establishing a timely and properly structured monitoring system.**

6.2 Appointment of Certified Foreman/Quarryman in Charge

6.2.1 Certification of foreman/quarryman in charge of quarry development projects

Section 8 (1) of the Quarries Regulations 1939 requires that every quarry should be under the control and supervision of a quarryman-in-charge unless an inspector may, if he or she thinks fit, exempt any quarry from this requirement. In addition, Section 9 of the Quarries Regulations 1939 requires that no person shall be employed or shall act in the capacity of foreman-in-charge of a quarry unless he or she is the holder of a quarryman's certificate granted by an inspector or other person authorised in writing in that behalf by the Minister.

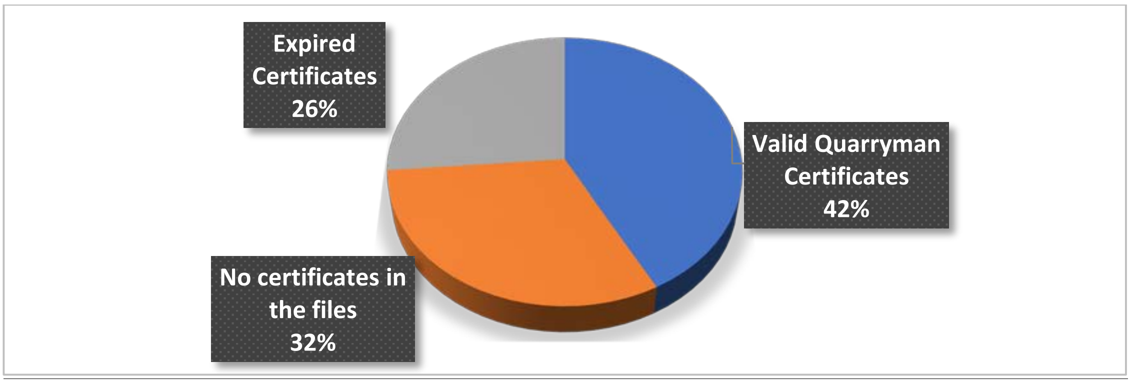
Furthermore, Section 10 of the Quarries Regulations 1939 stipulates that a quarryman certificate remains in force for a period of two (2) years from the date of issue subject to the foreman undergoing satisfactory written or oral examination that the inspector deems necessary. Upon expiration of a quarryman certificate it can be further extended for a period not exceeding two (2) years.

Our review of records relating to the foreman in charge/quarryman for the twenty (20) quarry development projects and detailed in **Section 6.1** of this report indicated that there were 19 identified foreman in charge. From the twenty (20) quarry development projects, two quarries[8] did not commence operations.

Review of the quarryman records revealed that eleven (11) of the nineteen certificates had expired or were not maintained:

- 8 of the identified quarryman held valid quarryman certificates for a two-year period;
- 6 of the quarryman filed records that did not contain the quarryman certificates and;
- 5 of the quarryman certificates located in the respective files had expired with no further documentation regarding their renewal.

Figure 6.2.1: Certification of foreman/quarryman in charge of quarry development projects



For the anomalies noted, refer to ***Appendix 8.3*** for further details.

[8] File References - CT16CK and CT16CJ

The findings indicate that the absence of relevant documentation and poor records maintenance which limit the Department's compliance to regulations, processes and procedures. Furthermore, the anomalies found could also be attributed to the absence of proper database to capture information in digital format.

DMR[9]has agreed to the audit findings and recommendations and will be taking appropriate action to remedy the issues that have been raised.

Department's Comments

The Department has created an excel sheet where the quarryman records are updated from the hard copy record book. However, the Department will look into having checks on the updating of this excel sheet on a quarterly basis by the relevant supervisor.

This excel sheet will also be saved in both the shared drive and backed up on an external hard drive to ensure no loss of information.

Recommendations

- **The Department should expedite the creation of the database for maintaining records on quarryman.**
- **Supervisory checks should be strengthened to ensure that processes and procedures outlined in the Quarries Act and Regulations 1939 are complied with.**

6.2.2 Proper notification of appointment, commencement and changes of Quarry/Foreman in Charge

Section 11 of the Quarries Regulations 1939 requires that the appointment of every foreman-in-charge shall be notified in writing by the person appointing him or her to the Inspector within 14 days after such appointment. Similarly, the quarryman must notify the Inspector within 7 days after he or she assumes control and supervision of the quarry.

Section 15 of the Quarries Regulations 1939 stipulates that in the event that the foreman-in-charge of the quarry have changed, it is required that the Inspector is properly notified in writing within 7 days of the change.

Our review revealed that 18 of the 19 quarryman filed records that did not have the 14-day notification of the appointment of the quarryman by the quarry company. Furthermore, the seven-day notification requirement from the quarryman to the inspector, in writing, after he or she assumes control and supervision of the quarry could not be verified. There were no records provided to substantiate this, increasing the risk of quarry operations not being effectively monitored.

[9] Exit meeting dated 23 July 2020.

DMR[10]has agreed to the audit findings and recommendations and will be taking the appropriate action to remedy the issues that have been raised. The Department stated going forward they will ensure the relevant clauses are part of the quarry approval letters and that these changes are incorporated into their SOP as well for issuance of new quarry approvals.

Department''s Comments

A checklist has been created for the issuance of quarryman's certificates whereby all proper documentation has to be submitted by the applicant before the certificate is created and endorsed only by the Inspector of Mines or the Manager Mines. The clause in the quarry approval letter stating that the quarry operators are required by law to provide a notification letter to the Department within 14 days of appointing a Quarryman, has been in practice.

Recommendations

- **Supervisory checks should be strengthened by the Department to ensure that processes and procedures outlined in the quarries regulations are complied with at all times.**
- **The Department should include a clause in the quarry approval letter stating that the quarry operators are required by law to provide a notification letter to the Department within 14 days of appointing a Quarryman.**
- **When acknowledging the appointment of the quarryman, the Department should include a clause in its acknowledgement letter that the quarryman is required by law to provide a notification letter to the Department within 7 days after he or she assumes control and supervision of the quarry.**

6.2.3 Mandatory requirements prior to issuing quarryman certificates

Section 10 of the Quarries Regulations 1939 sets out the requirement for the certification of a quarryman as shown below:

1.	Applications to be submitted to an Inspector at the Department of Mineral Resources in accordance with Form 4. (Refer ***Appendix 8.4*** for copy of Form 4 extracted from Schedule 1 of the Quarries Regulations)
2.	Application to be accompanied by a fee of $33.
3.	Applicant has attained the age of 21 years.
4.	Applicant has had no less than 2 years practical experience in quarrying.
5.	Applicant is fully conversant with the provisions of the Quarries Regulations and of all regulations made under the provisions of the Explosives Act 1927 relating to the handling, storage and use of explosives.
6.	Applicant is proficient in rendering first aid to injured persons.
7.	Applicant successfully passes written or oral examination.
8	Quarryman's certificate to remain in force for 2 years and may, on application being to an inspector accompanied by a fee of $16.50.

All applications for quarryman certification are endorsed by an authorized Inspector/ Director of Mines after they are processed, vetted and recorded in the register for quarryman's

[10] Exit meeting dated 23 July 2020.

certificate. The processing and vetting protocols are captured in the Department's SOP that is supplementing the Quarries Act and Quarries Regulations.

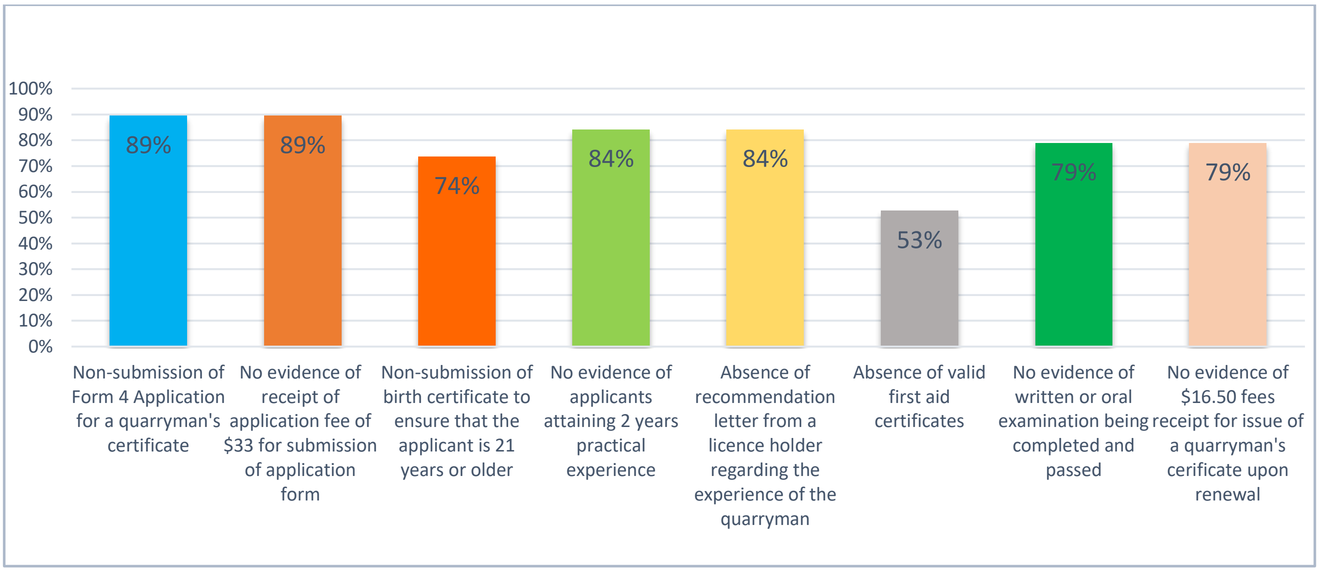
We noted that the SOP has not been formally endorsed by the Department of Mineral Resources.

We reviewed and analyzed the records filed by 19 identified quarryman to determine if all requirements specified in Section 10 of the Quarries Regulations 1939 and the SOP have been met prior to issuing a quarryman's certificate.

The following anomalies were noted and also depicted in Figure 6.2.2 below:

- 17 of the 19 quarryman filed records which did not have Form 4 Applications;
- 17 of the quarryman filed records that did not contain evidence of receipt of application fee of $33 for submission of application form;
- 14 of the quarryman filed records that did not contain birth certificates to ensure that the applicant is 21 years or older;
- 16 of the quarryman filed records which did not contain evidence of applicants attaining two-year practical experience;
- 16 of the quarryman filed records that did not contain recommendation letters from a license holder regarding the experience of the quarryman;
- 10 of the quarryman records filed did not contain valid first aid certificates;
- 15 of the quarryman filed records that did not contain written or oral examination being completed and passed; and
- 15 of the quarryman filed records that did not contain evidence of payment of $16.50 fees for issue of a quarryman's certificate upon renewal.

Figure 6.2.2: Anomalies noted prior to issuing quarryman's certificate



The above anomalies are a result of poor records management of quarryman information. We observed that records relating to the above are all kept in paper files. To retrieve information on one particular quarryman required going through numerous unorganized files of other quarryman since the documents are not maintained and filed separately. This practice proved very cumbersome during the audit. Also, there was no mechanism to track the history of a particular quarryman so that well-informed decisions are made in a timely manner.

Improper record keeping disrupts the consistent flow of work processes which can be associated with lack of transparency and accountability in issuing quarryman's certificates.

DMR[11] has agreed to the audit findings and recommendations and will be taking necessary remedial actions.

Department"s Comments

The Department keeps all its quarryman certificates in one file. The recommendation of creating separate files for each quarryman will be effected and the Department will look into creating separate digital and hard copy folders for each quarryman.

The Department has created an excel sheet where the quarryman records are updated from the hard copy record book. However, the Department will look into having checks on the updating of this excel sheet on a quarterly basis by the relevant supervisor.

Recommendations

- **DMR should consider maintaining separate files for quarryman whereby all information/documents regarding a particular quarryman is maintained and updated accordingly.**

- **DMR should consider the creation of a database to electronically maintain information on quarryman.**

[11] Exit meeting dated 23 July 2020.

7.0 CONCLUSION

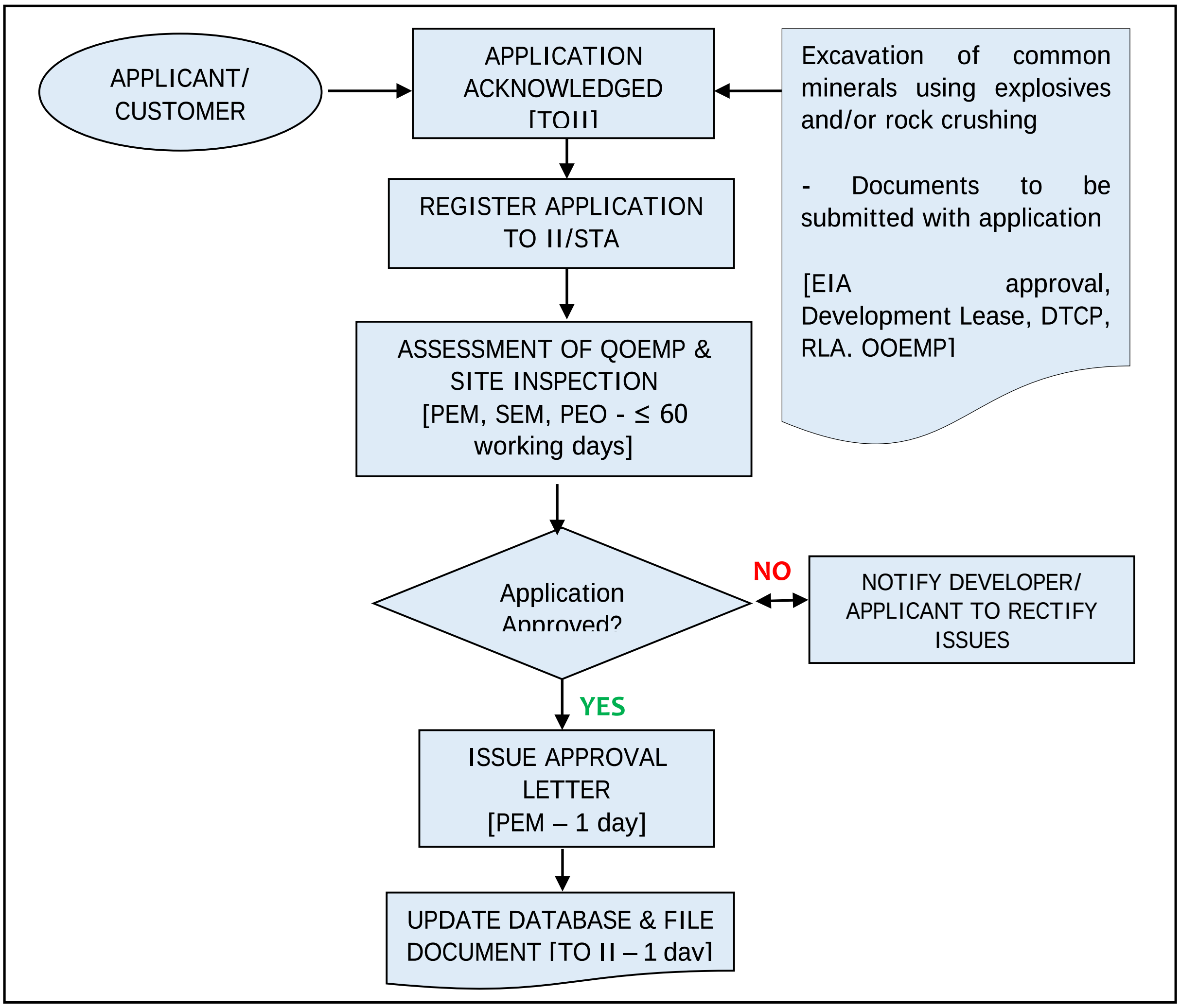
There is clear evidence of all quarry operations not being approved by the Department of Mineral Resources. Approvals were also granted by Department of Environment, Department of Town & Country Planning, Department of Lands and the iTaukei Land Trust Board without consultation with the Department. This is significantly attributed to the ambiguity in the Quarries Act 1939 on whether a central agency should consider and approve the operation of quarries. This could be addressed through review of the legislation which must be vigorously pursued.

We were not able to determine whether standard requirements adopted by the Department for approval of quarries was also being followed by these agencies while granting approvals. We were also not able to confirm whether controls placed by the DMR on operation of quarries were also observed in the quarry operations approved by other agencies.

There is a lot of room for improvement in record keeping in relation to quarry operations by the DMR. In the absence of proper record keeping, we were not able to determine whether all twenty (20) quarry developments from 2016 to 2019 met all the requirements before approvals were provided by the DMR. There is an opportunity for the DMR to update and digitize records in relation to quarry operations.

8.0 APPENDICES

Appendix 8.1: Quarry Development Application Process


APPLICANT/ CUSTOMER
APPLICATION ACKNOWLEDGED [TO II]
Excavation of common minerals using explosives and/or rock crushing
- Documents to be submitted with application
[EIA approval, Development Lease, DTCP, RLA. QOEMP]
REGISTER APPLICATION TO II/STA
ASSESSMENT OF QOEMP & SITE INSPECTION [PEM, SEM, PEO - ≤ 60 working days]
Application Approved?
NO
NOTIFY DEVELOPER/ APPLICANT TO RECTIFY ISSUES
YES
ISSUE APPROVAL LETTER [PEM – 1 day]
UPDATE DATABASE & FILE DOCUMENT [TO II – 1 day]

Source: Department of Mineral Resources Standard Operating Procedures

Appendix 8.2 Mandatory Requirements prior to commencement of quarry operations

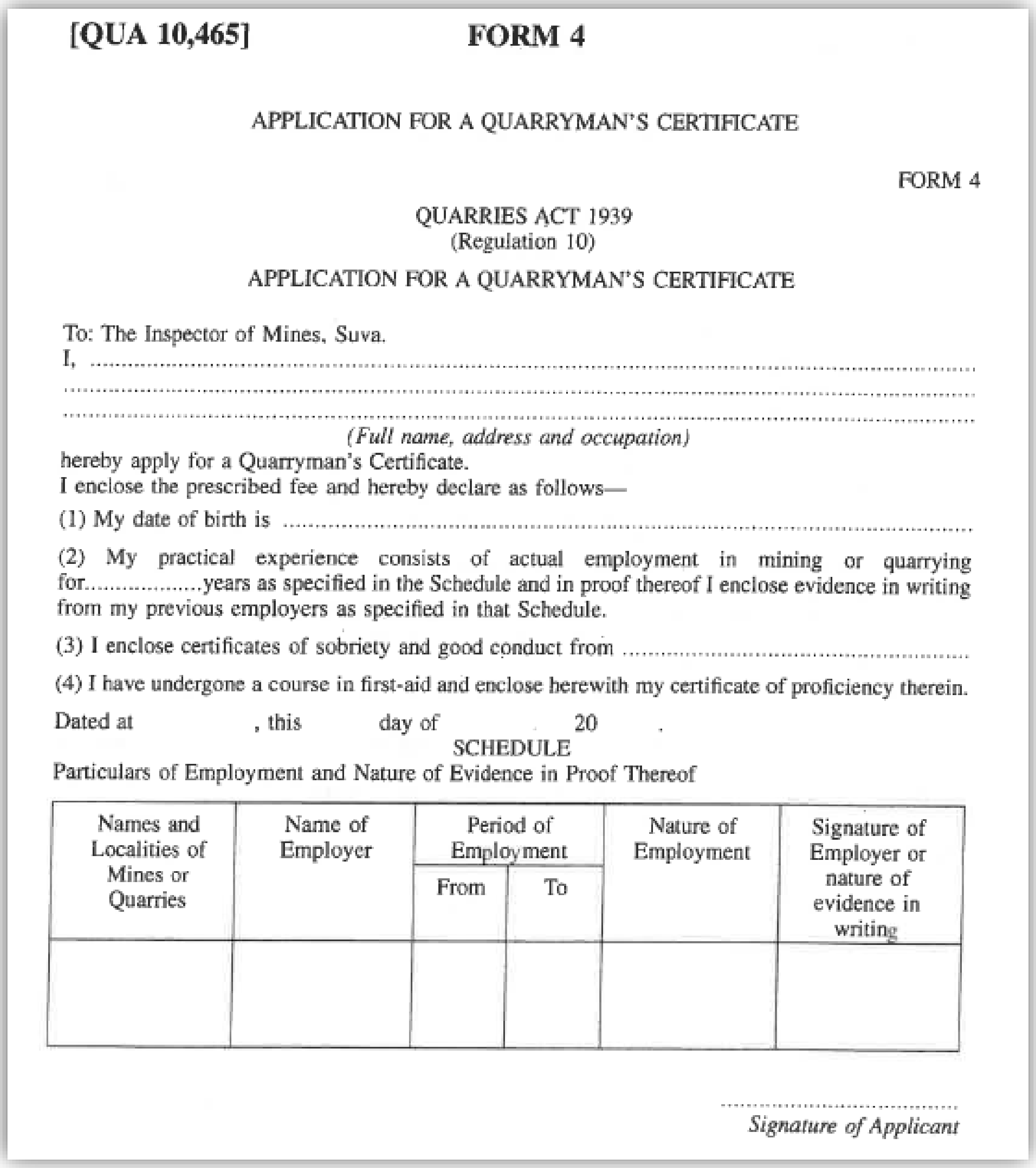
Environmental Management Act 2005	*EIA Approval* - Requires that all quarry development projects must be subject to the EIA process and that proposals are not permitted unless the EIA report has been approved. *QOEMP* – Further required by Section 32, Subsection 1, that a proponent must prepare and implement any environmental or resource management plan, monitoring programme, and protection plan or mitigation measure that is required as a condition of any approved EIA. Though silent on the specifications of plans under each form of development project, in relation to quarry projects, the plan pertains to Quarry Operational Environmental Management Plans (QOEMPs) which includes an explosives management plan, crushing/processing system, site management, environmental risks mitigation, quarry closure & rehabilitation and quarry Occupational Health & Safety (OHS) plan for each quarry site that the Department has to monitor.
State Lands Act 1945 and State Lands (Leases and Licenses) Regulations 1980	Deals with, amongst others, the land leasing for quarrying purposes.
Land Use Act 2010 and Land Use Regulations 2011	In managing the land reform program, the Land Use Division under the Director of Lands administers the Land Use Act 2010 and Land Use Regulations 2011 by granting leases for designated land which includes proposals for quarry projects.
iTaukei Land Trust Act 1940 and iTaukei Land Trust (Leases and Licences) Regulations 1984	Deals with issuing of native land leasing for quarrying purposes.
Town Planning Act 1946	Schedule for Sections 8 and 9 of the Town Planning Act stipulates that matters which may be dealt with by General Provisions in a town planning scheme, include, inter alia, quarry projects. The Town Planning Act further requires that any land development should not be permitted without the written permission of the Local Authority. The Local Authority shall then within (30) days from the receipt of the application refer the application to the Director of Town and Country Planning in accordance with Section 7 (3) of the Town Planning Act, denoting that prior consent of the Director of Town and Country Planning shall be obtained before Local Authorities grant or refuse permission for a development project.

Appendix 8.3 Anomalies noted during quarryman file review

File No.	Approval Date	Rock Source	Type of Operation	Status of Operations	Non-compliance Noted
CT16DS	Approval letter not sighted in file.	River Gravel	Screening and crushing	Operational	Quarryman filed records did not contain the quarryman certificates.
CT16DP	Approval letter not sighted in file.	Hard Rock	Rock blasting and crushing	Closed	Quarryman filed records did not contain the quarryman certificates.
CT16DM	29 September 2017	Hard Rock	Rock Extraction and crushing	Operational	Quarryman filed records did not contain the quarryman certificates.
CT.16CZ	06 December 2018	Hard Rock	Rock Blasting and crushing	Operational	Quarryman filed records did not contain the quarryman certificates.
CT.16DR	Approval letter not sighted in file.	Hard Rock	Rock blasting, (Seasonal crushing)	Operational	Quarryman filed records did not contain the quarryman certificates.
CT16CC	03 August 2018	Hard Rock	Rock extraction and crushing	Temporary suspension	Quarryman filed records did not contain the quarryman certificates.
CT16DI	18 October 2017	River Gravel	Screening and crushing	Operational	Quarryman filed records did not contain the quarryman certificates.
CT16DE	01 December 2016	Hard Rock	Rock blasting and crushing	Closed	Quarryman changed during the quarry operations and it was noted that quarryman certificates had expired and audit could not substantiate the renewal of the certificates as it could not be found in the respective quarryman files.
CT16AA	Approval letter not sighted in file.	Hard Rock	Rock blasting (seasonal crushing)	Operational	Quarryman certificates had expired and audit could not substantiate the renewal of the certificates as it could not be found in the respective quarryman files.
CT16DK	Approval letter not sighted in file.	Hard Rock	Rock blasting and crushing	Closed	Quarryman certificates had expired and audit could not substantiate the renewal of the certificates as it could not be found in the respective quarryman files.
CT16BY	Approval letter not sighted in file.	Hard Rock	Rock blasting, screening and crushing	Temporary suspension	Quarryman certificates had expired and audit could not substantiate the renewal of the certificates as it could not be

File No.	Approval Date	Rock Source	Type of Operation	Status of Operations	Non-compliance Noted
					found in the respective quarryman files.
CT16DG	07 September 2017	Hard Rock	Rock blasting and crushing	Closed	Quarryman certificates had expired and audit could not substantiate the renewal of the certificates as it could not be found in the respective quarryman files.
CT.6A	18 October 2018	Hard Rock	Rock blasting	Operational	Quarryman certificates had expired and audit could not substantiate the renewal of the certificates as it could not be found in the respective quarryman files.

Appendix 8.4 Extract of Form 4 Application for a quarryman's certificate



[QUA 10,465] **FORM 4**

APPLICATION FOR A QUARRYMAN'S CERTIFICATE

FORM 4

QUARRIES ACT 1939
(Regulation 10)

APPLICATION FOR A QUARRYMAN'S CERTIFICATE

To: The Inspector of Mines, Suva.
I, ...
....
....
(Full name, address and occupation)
hereby apply for a Quarryman's Certificate.
I enclose the prescribed fee and hereby declare as follows—

(1) My date of birth is ....

(2) My practical experience consists of actual employment in mining or quarrying for..................years as specified in the Schedule and in proof thereof I enclose evidence in writing from my previous employers as specified in that Schedule.

(3) I enclose certificates of sobriety and good conduct from ....

(4) I have undergone a course in first-aid and enclose herewith my certificate of proficiency therein.

Dated at , this day of 20 .

SCHEDULE

Particulars of Employment and Nature of Evidence in Proof Thereof

Names and Localities of Mines or Quarries	Name of Employer	Period of Employment		Nature of Employment	Signature of Employer or nature of evidence in writing
		From	To		

....
Signature of Applicant

GOVERNMENT PAYROLL

SYSTEM

Table of Content

Acronyms

Abbreviation	Meaning
CLI	Command Line Interface
EIN	Employee Identification Numbers
FNPF	Fiji National Provident Fund
FRCS	Fiji Revenue and Custom Services
GUI	Graphical User Interface
ICT	Information and Communication Technology
IDI	INTOSAI Development Initiative
IS	Information System
ISAAS	Information System Audit and Assurance Standards
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
ISSAI	International Standards of Supreme Audit Institutions for ISSAI
ITCS	Information Technology and Computing Services
MoE	Ministry of Economy
RFMF	Royal Fiji Military Forces
SLA	Service Level Agreement
UI	User Interface
VPN	Virtual Private Network
WBC	Westpac Bank Corporation

Executive Summary

Introduction

The Office of the Auditor-General conducted an Information System (IS) audit on the Ministry of Finance and National Planning Payroll System under the responsibility of the Ministry of Economy (MoE) through the Payroll Section.

The MoE Payroll Section is the central executing agency that controls and maintains the Government Payroll Systems which is a comprehensive fortnightly salary and weekly wage earners system for government employees. Information is stored for each Department's employee in order to fulfil the personal, accounting, legal and taxation requirements. This enables Government to make correct and prompt payment of employee pay every fortnight and issue of various detailed reports to departments, banks, insurance company and other related institutions. The payroll system also stores the After-Care Fund, Pensions, Special Constables and the Royal Fiji Military Forces (RFMF) staff information but with different databases stationed at Information Technology and Computing Services (ITCS) Data Centre.

Audit Focus

Our audit focused on the application controls of the payroll system and the general controls surrounding the payroll system that the MoE Payroll Section is responsible for. Data analysed relates to the period 2018/2019 financial year only for the Established Staff and RFMF Staff.

Significant Findings

- Security risks management of shared payroll data with third parties
- Need for a change management plan;
- Requirement of system documentation and policy reviews;
- Accuracy of and completeness of data sets extracted for analysis; and
- Command line interface to be more user friendly.

Audit Conclusion

The results of the audit from the records and information provided indicated that the Payroll Section:

- needs to strengthen the internal controls policies for processing payroll, specifically from the data input processes;
- should ensure proper security are present when sharing payroll data; and
- needs to focus on improving its current legacy payroll system used or have an automated integrated payroll system.

1.0 Auditing Standards

We have conducted this audit in accordance with the International Standards of Supreme Audit Institutions for ISSAI 1 on Lima Declarations, ISSAI 5300 for IT Audit professional in conducting IT Audits, Information Systems Audit and Control Association (ISACA) IS Audit and Assurance Standards (ISAAS) and International Standards Organization (ISO) IT Standards.

2.0 Reference to Comments

Comments provided by the Payroll Section of the MoE for the IT audit conduct on 6 February 2020 have been incorporated in this report.

3.0 Subject Matter and Scope

The subject matter for this audit was to obtain assurance on the government payroll system processes and related general controls to safeguard the resources of government maintained by the payroll system for the 2018/2019 financial year.

4.0 Audit Objective

The objectives of the audit were to:

I. Determine whether the Payroll Section has established effective application and general controls framework for the management of payroll operations;
II. Assess whether the data maintained and stored in the payroll system is accurate (data integrity) and complete;
III. Review and evaluate the adequacy of policies and procedures which are in place for preparation, handling and input of data for application; and
IV. examine the applicable general and application controls.

5.0 Audit Criteria

The criteria used for this audit are based on regulations and manuals designed to ensure compliance with the IDI Active IT Audit Manual and the ISO35800 on IT-Governance of IT for the organization and ISO27001 on Information Security Management.

6.0 Methodology

Audit techniques used for gathering evidence and conducting audit analysis included the following:

i. documentary reviews and interview of key personnel at the MoE Payroll Section and the ITCS Payroll Administrator; and
ii. analysis of data on established staff government payroll data and the RFMF payroll data maintained by ITCS.

7.0 Audit Findings

7.1 Security Risk Management of Shared Payroll Data not adequate

The organization's information security policy covers all operational risks and is able to reasonably protect all business-critical information assets from loss, damage or abuse[1].

This policy establishes the requirements for protection of information assets, and may refer to other procedures or tools on how these will be protected. The policy should be available to all employees responsible for information security, including users of business systems who have a role in safeguarding information (personnel records, financial input data, etc.)[2].

We noted that the bank listing, which is not encrypted, is sent to respective banks by the MoE Payroll Section through email. The MoE stated that the Payroll Section was previously sending files through emails with an encrypted version[3].

Additionally, all employee payroll taxes and deductions data are disbursed to relevant authorities through email without any encryption. This has been noted to be the standard procedure used for sharing and communicating of confidential employee data to banks and the taxation authority.

The Ministry stated that it is currently using one of the main bank services provider corporate online loading services on the banks portal to load salaries and wages and only certain authorized senior officers of the Payroll Section are able to load and make changes on the portal. Similarly, for tax authority, the data is directly uploaded on its portal[4]. The only exception is for one bank where the non – encrypted staff listing is still sent by email because it does not provide the same service.

The use of legacy system and lack of awareness on the risk of sending critical information via email to banks and taxation authority is susceptible to information leakage by hackers and vulnerable to cyber – crime activity.

MoE mentioned that the Payroll Section will provide the initiatives undertaken with FRCS which will become effective from 1st August, 2020 on the new taxation portal to be posted online and also provide the encryption process provided by the banks to be detailed with a Security Risk Management Plan[5].

The likelihood for risks on loss of data and/or compromising personal data to outside parties due to packet sniffing[6] or data leakage can go undetected if proper control mechanism is not present.

[1] ISO 27000 series Information Security Management System and other internal policy, procedures or applicable regulations.
[2] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)
[3] Management response on 06/02/20
[4] Management response on 06/02/20
[5] Management response on 06/02/20
[6] A computer program that can intercept and log traffic that passes over a computer network.

Recommendations

Payroll Section should consider:

1. **Using a secured information sharing tools such as special platforms to upload data directly to banks rather than using emails.**
2. **Use of two-way encryption to protect the data being shared over a network.**
3. **Using virtual private network (VPN) or private cloud services to share information and at the same time protect the information being shared between entities.**

7.2 Change Management Control not held

The change management plan process is normally used to manage and control changes to software, hardware and related documentation. Change management is necessary where the impact of an unapproved or accidental change could have severe risks and financial consequence for an organisation. Organisations follow a defined change management procedure which requires approval from a board before being implemented into the operational environment.[7]

We were informed by the Payroll Section and ITCS at the time of audit on 23/10/19 that there was an update made to the legacy system but there was no documentation available to confirm about the upgrade of the system.

MoE advised that the changes to the payroll system is an ongoing process whereby the Ministry is continuously upgrading the payroll system and its reporting requirements to ensure that the Government payroll is compliant to FNPF, FRCS, General Ledger and related stakeholder requirements[8].

Furthermore, MoE stated that any changes to the payroll system or processes is endorsed by the Permanent Secretary for MoE and communicated to the payroll users through a MoE circular. In addition, payroll users are provided on-the-job training if there are any new features for implementation in the payroll system. Payroll user group meetings are conducted on a monthly basis where payroll related issues faced at Ministry/Department level are discussed and also the upgrades/changes to the payroll system are discussed[9].

The payroll team at MoE also provide assistance and guidance to individual Ministries/Departments on issues on daily basis as well[10]. Payroll section will provide the change management plan which is already a work in progress as part of the scoping exercise to review the legacy payroll system and make submissions for the new payroll system requirements[11].

In the absence of documented change management plan and lack of control over change management process for the payroll system increases the risk of impact on user with a legacy

[7] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[8] Management response on 06/02/20
[9] Management response on 06/02/20
[10] Management response on 06/02/20
[11] Exit meeting minutes on 21/02/20

of failed change and change saturation. Hence it is required to ensure that no unnecessary changes are made to the system and all changes for the system to be documented[12].

Recommendations

Payroll Section should:

1. **Implement Change Management Control over the payroll system.**
2. **Have a proper documentation maintained for any system upgrades for future reference.**

7.3 System Documentation and Policy Reviews not held

Documentation of IS, applications, job roles, reporting systems and periodicity is an important reference point to align IT operations with business objectives[13].

Regularly reviewing policies and procedures keeps an organization up to date with regulations, technology, and industry best practices that are consistent and effective.

We observed that the Payroll Section did not have:

I. a proper payroll system documentation audit trail for any system amendments without any policy reviews, and
II. provision of service level agreement (SLA) with ITCS which clearly outlined the roles and responsibilities of the two parties, environment and infrastructure that the system should operate in together with the required polices that govern the system.

We noted that the Payroll Section has a very high dependency on policies issued by ITCS, some of which, were not regularly updated to match the new system upgrades. These include policies for password, back-up and emails. We further observed that some policies such as meant for technologies or software which have reached its end life and/or no longer supported by the manufacturers are still being used. As end-users of the payroll system, the Section did not customize them to match their role in managing the system.

Furthermore, the Payroll Section did not provide documentation to confirm all policies are updated for any changes in the system to be determined. MoE stated that when the payroll system was implemented, it should have been accompanied with the system documentation and the Ministry will look for the initial documentation and the documentation with respect to changes. The Ministry stated that during the review of the financial regulations, all the changes that have been occurred until the date of review is incorporated in the respective financial regulations[14].

In the absence of an SLA, it was difficult to draw a line between the responsibilities of the Payroll Section and the service provider because we noted that ITCS staff have super-user access to the payroll system whilst at the same time provide the hosting services too. The Ministry mentioned that is currently undergoing review of financial regulations and all the changes in the payroll system/process will be captured accordingly[15].

[12] Management response on 06/02/20
[13] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[14] Management response on 06/02/20
[15] Management response on 06/02/20

The Payroll Section will be providing the plan which is in progress with proper system documentation and also the review of policies specifically to be documented about the new payroll system requirements[16].

Lack of documentation can lead to communication gaps where poor and incorrect decisions can be made.

Recommendations

MoE should:

1. **Draw a SLA between MoE and ITCS which would clearly state the responsibilities of the parties involved in providing the service in terms of the infrastructure and security required for smooth operations of the system.**
2. **Ensure all the policies relating to the system by ITCS has to be frequently updated, as and when there is a change in the system to operate in a safe and secure environment that is not vulnerable to any threats or failure.**
3. **Ensure that processes for system documentation are in place for an audit trail for proper tracking of the system upgrades and changes in future.**

7.4 Data Accuracy and Completeness

IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw conclusions on which to base the engagement results[17] to place due emphasis on the accuracy and completeness of the information when information obtained from the enterprise is used by the IS audit to perform audit procedures[18].

Completeness of input data is to ensure that all the key transaction information has been entered before the transaction can be posted to the accounts[19].

We observed from the analysis of payroll data provided by ITCS for the period ending 31 July 2019 that the accuracy and completeness of data cannot be fully reliable upon due to anomalies identified after the payroll data analysis from the same data source.

The salaries team receives completed and signed input forms from respective ministries and departments which the payroll team processes[20]. It is the responsibility of the respective accounting heads to ensure that the employee details are correctly stated and provided to the Payroll-Section of MoE and the Payroll Section processes the input forms accordingly[21].

The data used for our analysis was drawn from the established staff payroll data and RFMF payroll data sets. The findings presented in **Table 7.1** is the summary of analysis on the irregularities which were noted while details are shown in **Appendix 1**.

Table 7.1: OAG data analysis results

[16] Management response on 06/02/20
[17] ISAAS 1205 Evidence Clause 1205.1
[18] ISAAS 1205 Evidence
[19] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[20] Management response on 06/02/20
[21] Management response on 06/02/20

Established Payroll Test	ACL Results	RFMF Payroll Test	ACL Results
Blank Birth Dates	8	Blank Birth Dates	73
Blank Employment Start Dates	20	Blank Employment Start Dates	29
Blank Employment Termination/End Dates	66	Blank Employment Termination/End Dates	77
Duplicate data based on the Employee number, TIN number (FRCS), FNPF number and Bank Account number.	2	Duplicate data based on the Employee number, TIN number (FRCS), FNPF number and Bank Account number.	nil
Officers who are more than 55 years of age has not been removed from the system.	124	Officers who are more than 55 years of age has not been removed from the system.	224
Inconsistent FNPF number.	52	Inconsistent FNPF number.	12

***Source: OAG analysis from* data provided by ITCS**

As shown above, common exceptions which were noted included missing employee date of birth records, record of employment starting dates and contract end dates. The existence of duplicate bank accounts and FNPF numbers, employees reaching the compulsory retirement age and incomplete FNPF numbers recorded.

The analysis result shows that the employees data input detailed information needs to be properly verified and validated before it is entered into the payroll system.

The Ministry stated that all Accounting Heads have been directed to update the missing information of individual officers in the payroll system and this has been an ongoing exercise. A follow up would be done soon to ensure that the blank fields are updated accordingly in the payroll system[22].

Non – review of payroll data prior to its input exposes government to the risk of incorrect classification, incorrect payment of salaries and fraud.

Payroll Section will provide an update after consulting with the departments affected about the information missing from the data extracted from ITCS payroll database[23].

Recommendations

Payroll Section should ensure that:

1. **Input controls are strengthened for creation of employee profile in the payroll system.**

2. **In consultation with ITCS, establish an automated control is embedded in the payroll system for field formats (data entry) to either accept complete employee profile or reject incomplete data entry details.**

7.5 Command Line Interface (CLI)

[22] Management response on 06/02/20
[23] Exit meeting minutes on 21/02/20

The objective of a system design is to take various components of the system and design the solution in detail including screen layouts, business rules, process diagrams, pseudo code[24] and other documentation[25].

A good user interface (UI) provides a "user-friendly" experience that allow the user to interact with the software or hardware in a natural and intuitive way. A user interface should have a clear, concise, familiar, responsive, consistent and efficient way of making work easier and more accessible by end – users. A good interface makes it easy for users to tell the computer what they want to do, for the computer to request information from the users, and for the computer to present understandable information[26].

Clear communication between the user and the computer is the working premise of good UI design. As for the graphical user interface (GUI) is a form of user interface that allows users to interact with electronic devices through graphical icons and audio indicator such as primary notation, instead of text-based user interfaces, typed command labels or text navigation[27].

Whereas the command-line interface is a means of interacting with a computer program where the user issues commands to the program in the form of successive lines of text. The program which handles the interface is called a command-line interpreter or command-line processor[28].

Discussion with the ITCS Payroll Section System Administrator on 29/05/19 confirmed that the payroll platform was not always responsive and ITC is requested at all times for the use of command scripts. The Ministry stated that during monthly payroll user group meetings until to date, users have not raised concern with respect to the payroll system not being user friendly[29]. However, for the new users it is the responsibility of the Accounting Heads to ensure that they undergo proper on- the-job training for them to get familiarized with the system[30].

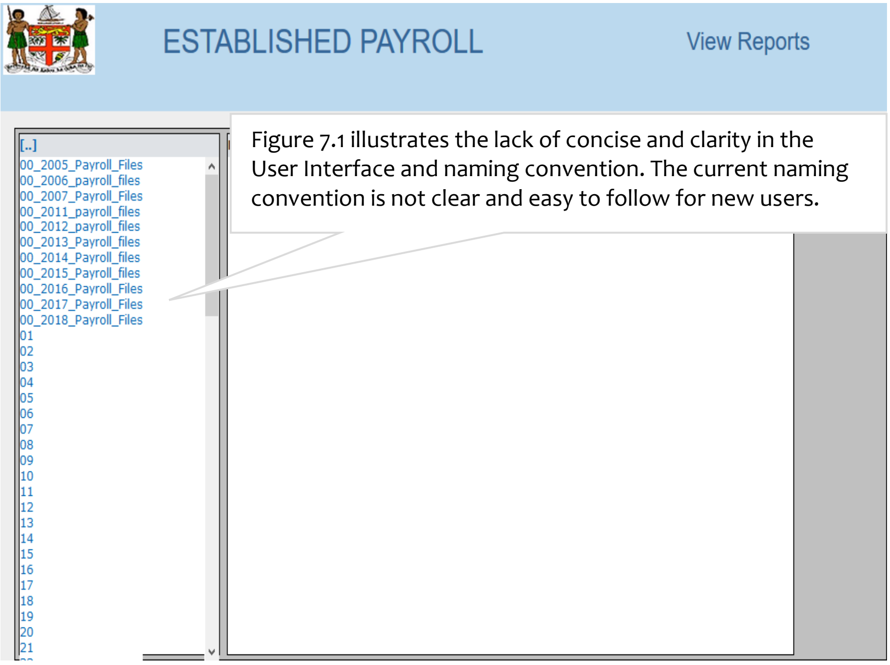
We noted the following issues which can assist in further improving the current system:

I. Graphical user interface (GUI) to be developed and used instead of CLI;
II. Information displayed on the panel view is not clear to end – users;
III. User interface is not concise. For instance, when accessing the “Pay Enquiries” panel and noted that the “Allowances/Deductions” panel is not interfaced using the same view panel but one needs to go through the “Allowances/Deductions” panel separately to view these details rather than from the same “Pay Enquiry” panel. It is like explaining a feature in one sentence instead of three or label an item with one word instead of two by keeping things clear and concise at the same time;
IV. Very little familiarity of the user interface to allow users to navigate through the program easily;
V. Design lacks consistency which is not very efficient and appealing to eyes of users; and
VI. Design was not responsive.

Refer below for illustration of details.

[24] This is an artificial and informal language that helps programmers develop algorithms.
[25] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[26] Critical Human Factors in UI Design-How technology can inform anticipatory interfaces for limited situational awareness.
[27] Critical Human Factors in UI Design-How technology can inform anticipatory interfaces for limited situational awareness.
[28] Critical Human Factors in UI Design-How technology can inform anticipatory interfaces for limited situational awareness.
[29] Management response on 06/02/20
[30] Management response on 06/02/20

Figure 7.1: Established Payroll File Panel



[..]
00_2005_Payroll_Files
00_2006_payroll_files
00_2007_Payroll_Files
00_2011_payroll_files
00_2012_payroll_files
00_2013_Payroll_files
00_2014_Payroll_files
00_2015_Payroll_files
00_2016_Payroll_Files
00_2017_Payroll_Files
00_2018_Payroll_Files
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21

Figure 7.1 illustrates the lack of concise and clarity in the User Interface and naming convention. The current naming convention is not clear and easy to follow for new users.

***Source:* Information provided by Payroll Section**

The design of an improper UI can result in the untimely provision of first – hand information to users when needed. Payroll Section stated that it will provide the plan status which is in progress as part of the scoping exercise to improve the legacy payroll system[31].

Recommendation

While the planned replacement of the system is noted and may take time, the MoE should consider upgrading the current system from a CLI to a GUI and re – design the interface that are simple, easy to learn and easy to use which gives the interface a consistent presentation.

[31] Management response on 06/02/20

8.0 Conclusion

Based on the results of audit procedures performed, we conclude that the Payroll Section can further strengthen the controls relating to processing payroll. There cases where inefficiencies have been highlighted through our use of data analytics should be reviewed in detail.

The current payroll system is old and has not been regularly updated. The replacement of the system and its full roll-out to all Ministries and Departments will take time and require substantial funding. The initiative taken by the Ministry is supported. Meanwhile, the current system should be strengthened to mitigate the high risk of loss that could arise from payroll fraud and data theft.

APPENDIX 1: ACL DATA ANALYSIS OUTPUT

Appendix 1.1: Established Payroll Blank Birth Dates

EMPLOYEE_ID	MINISTRY
96173	MINISTRY OF ITAUKEI AFFAIRS
96753	MINISTRY OF ITAUKEI AFFAIRS
96767	MINISTRY OF ITAUKEI AFFAIRS
97022	MINISTRY OF ITAUKEI AFFAIRS
96700	MIN OF EMPLY, PROD & INDUST REL
98016	MINISTRY OF FOREIGN AFFAIRS
96777	JUDICIAL
95761	INDEPENDENT COMMISSIONS

Appendix 1.2: Established Payroll Incomplete Start Dates

EMPLOYEE_ID	MINISTRY
95278	OFFICE OF THE PRESIDENT
96680	OFFICE OF THE PRESIDENT
95423	MINISTRY OF ITAUKEI AFFAIRS
96004	MINISTRY OF ITAUKEI AFFAIRS
97022	MINISTRY OF ITAUKEI AFFAIRS
96330	MINISTRY OF DEFENCE
97057	MINISTRY OF DEFENCE
96700	MIN OF EMPLY, PROD & INDUST REL
96315	MINISTRY OF FOREIGN AFFAIRS
96316	MINISTRY OF FOREIGN AFFAIRS
96317	MINISTRY OF FOREIGN AFFAIRS
96799	MINISTRY OF FOREIGN AFFAIRS
98016	MINISTRY OF FOREIGN AFFAIRS
98044	MINISTRY OF FOREIGN AFFAIRS
98122	MINISTRY OF FOREIGN AFFAIRS
95669	OFFICE OF AUDITOR GENERAL
95791	JUDICIAL
96550	MIN RURAL & MARITIME DEV & NAT DISASTER
62552	MINISTRY OF CIVIL SERVICE
96065	MINISTRY OF CIVIL SERVICE

Appendix 1.3: Established Payroll Incomplete End/Termination Dates

EMPLOYEE_ID	Start Date	MINISTRY
60790	9/16/1997	OFF ATTORNEY GENERAL
63022	11/5/2001	MINISTRY OF FINANCE
64519	7/2/2005	MINISTRY OF ITAUKEI AFFAIRS
58384	3/16/1993	MIN OF EMPLY, PROD & INDUST REL
61654	4/9/1999	MIN OF EMPLY, PROD & INDUST REL
62902	8/20/2001	MIN OF EMPLY, PROD & INDUST REL
64042	4/8/2004	MIN OF EMPLY, PROD & INDUST REL
61550	12/1/1998	MINISTRY OF FOREIGN AFFAIRS
53243	9/24/1991	OFFICE OF AUDITOR GENERAL
57305	1/25/1994	OFFICE OF AUDITOR GENERAL
93387	3/18/2013	OFFICE OF AUDITOR GENERAL
93747	10/16/2013	OFFICE OF AUDITOR GENERAL
48404	8/12/1988	JUDICIAL
53482	11/1/1991	JUDICIAL
53960	5/11/1992	JUDICIAL
58053	9/28/1992	JUDICIAL
58073	5/21/2002	JUDICIAL
58108	10/21/1992	JUDICIAL
59118	10/11/1994	JUDICIAL
59128	10/26/1994	JUDICIAL
60354	7/15/1996	JUDICIAL
60988	1/1/1998	JUDICIAL
61369	8/10/1998	JUDICIAL
61507	12/28/1998	JUDICIAL
61898	4/12/1999	JUDICIAL
62377	11/1/2000	JUDICIAL
62396	11/13/2000	JUDICIAL
62883	7/25/2001	JUDICIAL
63169	1/7/2002	JUDICIAL
63226	11/16/2001	JUDICIAL
63458	6/12/2002	JUDICIAL
63996	2/12/2004	JUDICIAL
64160	9/23/2004	JUDICIAL
64163	8/30/2004	JUDICIAL
64165	8/30/2004	JUDICIAL
64178	8/30/2004	JUDICIAL
64200	8/30/2004	JUDICIAL
64228	9/15/2004	JUDICIAL
64272	10/20/2004	JUDICIAL
64783	11/30/2005	JUDICIAL
64788	12/5/2005	JUDICIAL
64840	12/5/2005	JUDICIAL
64939	5/1/2006	JUDICIAL

EMPLOYEE_ID	Start Date	MINISTRY
90127	8/10/2006	JUDICIAL
90149	8/10/2006	JUDICIAL
90152	8/10/2006	JUDICIAL
90186	8/10/2006	JUDICIAL
44382	1/17/2000	LEGISLATURE
47493	3/25/1991	LEGISLATURE
48827	4/10/1989	OFFICE OF DIRECTOR PUBLIC PROSECUT
59134	11/19/1994	OFFICE OF DIRECTOR PUBLIC PROSECUT
59849	2/15/1995	OFFICE OF DIRECTOR PUBLIC PROSECUT
61014	11/24/1997	OFFICE OF DIRECTOR PUBLIC PROSECUT
49253	1/2/1989	MIN RURAL & MARITIME DEV & NAT DISASTER
48831	4/3/1989	MINISTRY OF CIVIL SERVICE
53613	1/15/1992	MINISTRY OF CIVIL SERVICE
53664	1/2/1992	MINISTRY OF CIVIL SERVICE
58858	1/3/1994	MINISTRY OF CIVIL SERVICE
59256	1/2/1995	MINISTRY OF CIVIL SERVICE
62010	12/13/1999	MINISTRY OF CIVIL SERVICE
90280	1/2/2007	MINISTRY OF CIVIL SERVICE
90305	1/4/2007	MINISTRY OF CIVIL SERVICE
90527	1/2/2008	MINISTRY OF CIVIL SERVICE
91434	1/29/2010	MINISTRY OF CIVIL SERVICE
94716	2/27/2015	MINISTRY OF CIVIL SERVICE
95938	1/3/2017	MINISTRY OF CIVIL SERVICE

Appendix 1.4: Established Payroll Duplicates

TIN	FNPF	Bank_Acc1	Accumulated GROSS_PAY	EMPLOYEE_NR	GRADE
170254XXX	MN1231XXXXQ	6654XXX	94,769.28	96778	XX
170254XXX	MN1231XXXXQ	6654XXX	13,192.6	90594	LG04

Appendix 1.5: Established Payroll for Officers more than 55 years

EMPLOYEE_ID	BIRTH_DATE	Department
20852	12/26/1947	OFFICE OF THE PRESIDENT
16920	9/21/1952	PRIME MINISTER'S OFFICE-GEN AD
44636	7/20/1963	MINISTRY OF FIJIAN AFFAIR
93979	11/16/1958	OHS SERVICES SUVA
09441	8/14/1956	FIJI EMBASSY INDONESIA
43138	3/27/1961	FIJI EMBASSY MALAYSIA
46326	4/28/1962	FIJI EMBASSY LONDON
46933	11/16/1960	FPRUN (GEVEVA)
47298	12/24/1954	FIJI EMBASSY TOKYO
47787	4/6/1961	FIJI EMBASSY SOUTH AFRICA
48207	10/8/1963	HIGH COMMISSION SOUTH KOREA
60586	11/16/1963	FIJI EMBASSY PNG
63613	1/1/1960	FPRUN (GEVEVA)
94759	2/19/1955	FIJI EMBASSY BRUSSELS
94841	8/29/1960	OVERSEAS MISSIONS DELHI
95099	9/20/1961	FIJI EMBASSY SOUTH AFRICA
96701	4/7/1962	FIJI EMBASSY NEW YORK
40679	7/13/1959	HIGH COURT
45869	11/25/1961	GENERAL ADMINISTRATION
46419	12/30/1961	HIGH COURT
46904	4/13/1961	HIGH COURT
58862	9/23/1957	HIGH COURT
91704	8/2/1962	HIGH COURT
91780	6/16/1954	HIGH COURT
93476	12/13/1963	HIGH COURT
94926	6/30/1955	HIGH COURT
05138	12/18/1945	LEGISLATURE
14118	10/9/1950	LEGISLATURE
19775	6/18/1957	LEGISLATURE
30280	5/7/1954	LEGISLATURE
40262	7/12/1959	LEGISLATURE
53179	9/13/1948	LEGISLATURE
59806	4/3/1951	LEGISLATURE
61804	12/23/1953	LEGISLATURE
62913	6/10/1959	LEGISLATURE
64562	8/16/1960	LEGISLATURE
94416	7/8/1950	LEGISLATURE
94422	3/24/1962	LEGISLATURE
94930	1/11/1953	LEGISLATURE
96737	2/3/1957	LEGISLATURE
98133	10/14/1956	LEGISLATURE
98134	6/16/1952	LEGISLATURE
98136	9/27/1962	LEGISLATURE

EMPLOYEE_ID	BIRTH_DATE	Department
98137	9/10/1963	LEGISLATURE
98138	9/17/1960	LEGISLATURE
47738	11/8/1960	PUBLIC SERVICE COMMISSION
95519	3/23/1962	PUBLIC SERVICE COMMISSION
49773	6/12/1960	OFF DIR PUBLIC PROSECUT
96788	3/12/1961	OFF DIR PUBLIC PROSECUT
19162	2/25/1952	DOCTORS PE AND ALLOWANCES
40809	11/29/1953	DOCTORS PE AND ALLOWANCES
45510	10/23/1956	DOCTORS PE AND ALLOWANCES
45511	4/2/1957	DOCTORS PE AND ALLOWANCES
46027	10/8/1960	DOCTORS PE AND ALLOWANCES
46650	3/31/1958	DOCTORS PE AND ALLOWANCES
46884	3/28/1960	DOCTORS PE AND ALLOWANCES
47039	9/11/1962	DOCTORS PE AND ALLOWANCES
48750	3/5/1960	DOCTORS PE AND ALLOWANCES
53581	2/18/1963	DOCTORS PE AND ALLOWANCES
58687	6/28/1962	DOCTORS PE AND ALLOWANCES
62552	4/21/1959	DOCTORS PE AND ALLOWANCES
63773	10/27/1956	DOCTORS PE AND ALLOWANCES
64816	1/1/1964	DOCTORS PE AND ALLOWANCES

Appendix 1.6: Established Payroll - Incomplete FNPF Numbers

EMPLOYEE_ID	FNPF	Department
95304	NON-MEMBER	ADMINISTRATION
93979	NON MEMEBER	OHS SERVICES SUVA
09441	RY718	FIJI EMBASSY INDONESIA
40671	0	HIGH COURT
61359	0	FIJI COURT OF APPEAL
91372	0	HIGH COURT
91704	NOMBER	HIGH COURT
91779	NONMEMB	HIGH COURT
91780	NONMEM	HIGH COURT
92162	NMEMBER	HIGH COURT
92170	N/MEB	MAGISTRATES COURT
92998	NMBRR	FIJI COURT OF APPEAL
94025	0	MAGISTRATES COURT
94107	NONMEMBER	HIGH COURT
94656	0	HIGH COURT
94657	0	MAGISTRATES COURT
94895	0	HIGH COURT
94926	0	HIGH COURT
95100	0	HIGH COURT
95145	0	HIGH COURT
95500	0	MAGISTRATES COURT

EMPLOYEE_ID	FNPF	Department
96340	0	MAGISTRATES COURT
96901	0	MAGISTRATES COURT
96902	0	HIGH COURT
96980	0	MAGISTRATES COURT
40219	0	LEGISLATURE
62942	0	LEGISLATURE
92347	PENSION	LEGISLATURE
94413	0	LEGISLATURE
94416	0	LEGISLATURE
94930	0	LEGISLATURE
95437	0	PUBLIC SERVICE COMMISSION
95519	NON MEMEBERS	PUBLIC SERVICE COMMISSION
90459	0	OFF DIR PUBLIC PROSECUT
94279	0	OFF DIR PUBLIC PROSECUT
96787	0	OFF DIR PUBLIC PROSECUT
96788	0	OFF DIR PUBLIC PROSECUT
45510	0	DOCTORS PE AND ALLOWANCES
61146	UG736	DOCTORS PE AND ALLOWANCES
62511	0	DOCTORS PE AND ALLOWANCES
62542	0	DOCTORS PE AND ALLOWANCES
62552	NON-MEMBER	DOCTORS PE AND ALLOWANCES
63417	0	DOCTORS PE AND ALLOWANCES
63773	NONMEMBER	DOCTORS PE AND ALLOWANCES
63882	0	DOCTORS PE AND ALLOWANCES
64816	0	DOCTORS PE AND ALLOWANCES
90414	0	DOCTORS PE AND ALLOWANCES
92166	0	DOCTORS PE AND ALLOWANCES
94358	0	DOCTORS PE AND ALLOWANCES
94934	0	DOCTORS PE AND ALLOWANCES
95131	0	DOCTORS PE AND ALLOWANCES
96319	0	DOCTORS PE AND ALLOWANCES

Appendix 1.7: RFMF Payroll Blank Birth Dates

EMPLOYEE_ID	Department
34156	FMF OFFICERS
34147	FMF STRATEGIC HQ ORS
29598	L.S.U OTHER RANKS
33785	FMF ENGRS OTHER RANK
34245	NAVY OFFICERS
24883	TF OFFICERS
29438	TF OFFICERS
25206	TF OTHER RANKS
25916	TF OTHER RANKS
29400	TF OTHER RANKS
34083	TF OTHER RANKS
34267	TF OTHER RANKS
34762	1 FIR OFFICERS
25397	1 FIR OTHER RANKS
27054	1 FIR OTHER RANKS
29663	1 FIR OTHER RANKS
29730	1 FIR OTHER RANKS
27975	1FIR UNDOF SYRIA-OFFICERS
34424	1FIR UNDOF SYRIA-OFFICERS
34739	1FIR UNDOF SYRIA-OFFICERS
34741	1FIR UNDOF SYRIA-OFFICERS
34742	1FIR UNDOF SYRIA-OFFICERS
34743	1FIR UNDOF SYRIA-OFFICERS
24183	1FIR UNDOF SYRIA-OTHER RANKS
25947	1FIR UNDOF SYRIA-OTHER RANKS
26073	1FIR UNDOF SYRIA-OTHER RANKS
26309	1FIR UNDOF SYRIA-OTHER RANKS
26461	1FIR UNDOF SYRIA-OTHER RANKS
26690	1FIR UNDOF SYRIA-OTHER RANKS
26871	1FIR UNDOF SYRIA-OTHER RANKS
27582	1FIR UNDOF SYRIA-OTHER RANKS
27921	1FIR UNDOF SYRIA-OTHER RANKS
27925	1FIR UNDOF SYRIA-OTHER RANKS
28091	1FIR UNDOF SYRIA-OTHER RANKS
28961	1FIR UNDOF SYRIA-OTHER RANKS
28969	1FIR UNDOF SYRIA-OTHER RANKS
29043	1FIR UNDOF SYRIA-OTHER RANKS
30411	1FIR UNDOF SYRIA-OTHER RANKS
31014	1FIR UNDOF SYRIA-OTHER RANKS
34426	1FIR UNDOF SYRIA-OTHER RANKS
34427	1FIR UNDOF SYRIA-OTHER RANKS
34428	1FIR UNDOF SYRIA-OTHER RANKS
34430	1FIR UNDOF SYRIA-OTHER RANKS

EMPLOYEE_ID	Department
34431	1FIR UNDOF SYRIA-OTHER RANKS
34432	1FIR UNDOF SYRIA-OTHER RANKS
34433	1FIR UNDOF SYRIA-OTHER RANKS
34434	1FIR UNDOF SYRIA-OTHER RANKS
34435	1FIR UNDOF SYRIA-OTHER RANKS
34436	1FIR UNDOF SYRIA-OTHER RANKS
34437	1FIR UNDOF SYRIA-OTHER RANKS
34439	1FIR UNDOF SYRIA-OTHER RANKS
34744	1FIR UNDOF SYRIA-OTHER RANKS
34745	1FIR UNDOF SYRIA-OTHER RANKS
34747	1FIR UNDOF SYRIA-OTHER RANKS
34750	1FIR UNDOF SYRIA-OTHER RANKS
34751	1FIR UNDOF SYRIA-OTHER RANKS
34752	1FIR UNDOF SYRIA-OTHER RANKS
34753	1FIR UNDOF SYRIA-OTHER RANKS
34754	1FIR UNDOF SYRIA-OTHER RANKS
34755	1FIR UNDOF SYRIA-OTHER RANKS
34756	1FIR UNDOF SYRIA-OTHER RANKS
34758	1FIR UNDOF SYRIA-OTHER RANKS
34759	1FIR UNDOF SYRIA-OTHER RANKS
34760	1FIR UNDOF SYRIA-OTHER RANKS
70965	1FIR UNDOF SYRIA-OTHER RANKS
71552	1FIR UNDOF SYRIA-OTHER RANKS
71658	1FIR UNDOF SYRIA-OTHER RANKS
34421	FIR SINAI OFFICERS
25635	FIR SINAI OTHER RANKS
30358	FIR SINAI OTHER RANKS
33547	FIR SINAI OTHER RANKS
21298	HEADQUARTERS LFC ORS
34157	FIR OFFICERS

Appendix 1.8: RFMF Payroll Incomplete Start Dates

EMPLOYEE_ID	DEPARTMENT
34698	TF OTHER RANKS
34292	1 FIR OFFICERS
25472	1 FIR OTHER RANKS
70960	1 FIR OTHER RANKS
34424	1FIR UNDOF SYRIA-OFFICERS
34425	1FIR UNDOF SYRIA-OFFICERS
27925	1FIR UNDOF SYRIA-OTHER RANKS
34426	1FIR UNDOF SYRIA-OTHER RANKS
34427	1FIR UNDOF SYRIA-OTHER RANKS
34428	1FIR UNDOF SYRIA-OTHER RANKS
34429	1FIR UNDOF SYRIA-OTHER RANKS
34430	1FIR UNDOF SYRIA-OTHER RANKS
34431	1FIR UNDOF SYRIA-OTHER RANKS
34432	1FIR UNDOF SYRIA-OTHER RANKS
34433	1FIR UNDOF SYRIA-OTHER RANKS
34434	1FIR UNDOF SYRIA-OTHER RANKS
34435	1FIR UNDOF SYRIA-OTHER RANKS
34436	1FIR UNDOF SYRIA-OTHER RANKS
34437	1FIR UNDOF SYRIA-OTHER RANKS
51920	1FIR UNDOF SYRIA-OTHER RANKS
34421	FIR SINAI OFFICERS
24259	FIR SINAI OTHER RANKS
24485	FIR SINAI OTHER RANKS
33547	FIR SINAI OTHER RANKS
71195	FIR SINAI OTHER RANKS
71505	FIR SINAI OTHER RANKS
71929	FIR SINAI OTHER RANKS
77267	FIR SINAI OTHER RANKS
77299	FIR SINAI OTHER RANKS

Appendix 1.9: RFMF Payroll Incomplete End/Termination Dates

EMPLOYEE_ID	Department
33235	FMF OFFICERS
32694	FMF STRATEGIC HQ ORS
32729	FMF STRATEGIC HQ ORS
33183	FMF STRATEGIC HQ ORS
33332	FMF STRATEGIC HQ ORS
34038	FMF STRATEGIC HQ ORS
34068	FMF STRATEGIC HQ ORS
34216	FMF STRATEGIC HQ ORS
34218	FMF STRATEGIC HQ ORS
34244	FMF STRATEGIC HQ ORS
34270	FMF STRATEGIC HQ ORS
34531	FMF STRATEGIC HQ ORS
34532	FMF STRATEGIC HQ ORS
34533	FMF STRATEGIC HQ ORS
34534	FMF STRATEGIC HQ ORS
34535	FMF STRATEGIC HQ ORS
34536	FMF STRATEGIC HQ ORS
34537	FMF STRATEGIC HQ ORS
34541	FMF STRATEGIC HQ ORS
34546	FMF STRATEGIC HQ ORS
34548	FMF STRATEGIC HQ ORS
34555	FMF STRATEGIC HQ ORS
34556	FMF STRATEGIC HQ ORS
34559	FMF STRATEGIC HQ ORS
34560	FMF STRATEGIC HQ ORS
34562	FMF STRATEGIC HQ ORS
34564	FMF STRATEGIC HQ ORS
34565	FMF STRATEGIC HQ ORS
34566	FMF STRATEGIC HQ ORS
34569	FMF STRATEGIC HQ ORS
34577	FMF STRATEGIC HQ ORS
34582	FMF STRATEGIC HQ ORS
34584	FMF STRATEGIC HQ ORS
34585	FMF STRATEGIC HQ ORS
34590	FMF STRATEGIC HQ ORS
34593	FMF STRATEGIC HQ ORS
34597	FMF STRATEGIC HQ ORS
34598	FMF STRATEGIC HQ ORS
34600	FMF STRATEGIC HQ ORS
34602	FMF STRATEGIC HQ ORS
34604	FMF STRATEGIC HQ ORS
33251	FORCE TRNG GROUP-OFFICERS
34763	1 FIR OFFICERS

EMPLOYEE_ID	Department
25829	1 FIR OTHER RANKS
26198	1 FIR OTHER RANKS
26425	1 FIR OTHER RANKS
27057	1 FIR OTHER RANKS
27675	1 FIR OTHER RANKS
27963	1 FIR OTHER RANKS
28033	1 FIR OTHER RANKS
29666	1 FIR OTHER RANKS
30621	1 FIR OTHER RANKS
31402	1 FIR OTHER RANKS
31504	1 FIR OTHER RANKS
31650	1 FIR OTHER RANKS
33185	1 FIR OTHER RANKS
33337	1 FIR OTHER RANKS
33433	1 FIR OTHER RANKS
33541	1 FIR OTHER RANKS
33703	1 FIR OTHER RANKS
33825	1 FIR OTHER RANKS
33965	1 FIR OTHER RANKS
34204	1 FIR OTHER RANKS
34305	1 FIR OTHER RANKS
34329	1 FIR OTHER RANKS
34351	1 FIR OTHER RANKS
34371	1 FIR OTHER RANKS
34394	1 FIR OTHER RANKS
34398	1 FIR OTHER RANKS
34409	1 FIR OTHER RANKS
34761	1FIR UNDOF SYRIA-OFFICERS
1454B	1FIR UNDOF SYRIA-OTHER RANKS
1607B	1FIR UNDOF SYRIA-OTHER RANKS
51920	1FIR UNDOF SYRIA-OTHER RANKS
27267	FIR SINAI OFFICERS
34318	FIR SINAI OTHER RANKS
31885	HEADQUARTERS LFC OFFICERS

Appendix 1.10: RFMF Payroll for Officers more than 55 years

EMPLOYEE_ID	BIRTH_DATE	Department
21266	1/1/1952	FMF OFFICERS
21878	5/2/1958	FMF OFFICERS
22325	8/21/1957	FMF OFFICERS
22629	11/15/1959	FMF OFFICERS
22974	11/10/1952	FMF OFFICERS
23536	12/23/1962	FMF OFFICERS
23538	11/17/1962	FMF OFFICERS
23854	2/7/1961	FMF OFFICERS
23917	7/9/1963	FMF OFFICERS
24054	9/13/1963	FMF OFFICERS
24486	1/6/1963	FMF OFFICERS
24647	7/17/1963	FMF OFFICERS
24856	10/14/1961	FMF OFFICERS
28724	12/27/1945	FMF OFFICERS
34737	8/22/1945	FMF OFFICERS
22623	4/4/1961	FMF STRATEGIC HQ ORS
23071	9/25/1959	FMF STRATEGIC HQ ORS
23437	4/12/1962	FMF STRATEGIC HQ ORS
23469	3/4/1962	FMF STRATEGIC HQ ORS
23599	10/10/1962	FMF STRATEGIC HQ ORS
23745	10/1/1960	FMF STRATEGIC HQ ORS
23859	3/23/1963	FMF STRATEGIC HQ ORS
24013	1/29/1963	FMF STRATEGIC HQ ORS
24072	1/23/1962	FMF STRATEGIC HQ ORS
24091	7/25/1963	FMF STRATEGIC HQ ORS
24315	5/25/1963	FMF STRATEGIC HQ ORS
24385	9/21/1961	FMF STRATEGIC HQ ORS
24402	4/23/1961	FMF STRATEGIC HQ ORS
24441	12/11/1963	FMF STRATEGIC HQ ORS
24527	12/10/1961	FMF STRATEGIC HQ ORS
24890	1/7/1963	FMF STRATEGIC HQ ORS
25978	2/18/1963	FMF STRATEGIC HQ ORS
26529	7/24/1963	FMF STRATEGIC HQ ORS
26597	10/9/1963	FMF STRATEGIC HQ ORS
26701	6/2/1962	FMF STRATEGIC HQ ORS
26869	8/23/1963	FMF STRATEGIC HQ ORS
27912	5/14/1963	FMF STRATEGIC HQ ORS
28368	10/3/1963	FMF STRATEGIC HQ ORS
24258	6/16/1962	L.S.U OFFICERS
23528	4/4/1960	L.S.U OTHER RANKS
23653	4/19/1963	L.S.U OTHER RANKS
23937	3/10/1963	L.S.U OTHER RANKS
23944	8/12/1962	L.S.U OTHER RANKS

EMPLOYEE_ID	BIRTH_DATE	Department
24064	6/2/1962	L.S.U OTHER RANKS
24114	6/17/1963	L.S.U OTHER RANKS
24144	10/29/1962	L.S.U OTHER RANKS
24171	5/6/1963	L.S.U OTHER RANKS
24308	4/13/1963	L.S.U OTHER RANKS
24309	1/28/1963	L.S.U OTHER RANKS
24501	9/9/1963	L.S.U OTHER RANKS
24805	6/18/1963	L.S.U OTHER RANKS
25086	8/25/1962	L.S.U OTHER RANKS
26065	3/15/1963	L.S.U OTHER RANKS
26367	2/20/1962	L.S.U OTHER RANKS
26432	2/19/1962	L.S.U OTHER RANKS
26560	9/7/1962	L.S.U OTHER RANKS
26786	3/10/1963	L.S.U OTHER RANKS
26862	5/12/1963	L.S.U OTHER RANKS
27170	6/16/1963	L.S.U OTHER RANKS
27568	8/16/1963	L.S.U OTHER RANKS
27736	12/25/1963	L.S.U OTHER RANKS
22943	5/14/1960	FORCE TRNG GROUP-OFFICERS
23081	12/19/1962	FORCE TRNG GROUP-ORS
23732	7/19/1962	FORCE TRNG GROUP-ORS
23791	9/8/1961	FORCE TRNG GROUP-ORS
23977	12/18/1963	FORCE TRNG GROUP-ORS
24053	8/28/1963	FORCE TRNG GROUP-ORS
24307	11/13/1963	FORCE TRNG GROUP-ORS
24343	7/22/1963	FORCE TRNG GROUP-ORS
24362	9/30/1963	FORCE TRNG GROUP-ORS
25258	7/6/1963	FORCE TRNG GROUP-ORS
25483	7/18/1963	FORCE TRNG GROUP-ORS
25610	2/13/1963	FORCE TRNG GROUP-ORS
26518	9/3/1963	FORCE TRNG GROUP-ORS
26940	8/22/1962	FORCE TRNG GROUP-ORS
27474	10/5/1963	FORCE TRNG GROUP-ORS
21808	11/10/1955	FMF ENGRS OFFICERS
24368	2/2/1963	FMF ENGRS OFFICERS
21706	1/15/1957	FMF ENGRS OTHER RANK
21787	11/6/1956	FMF ENGRS OTHER RANK
22055	3/1/1956	FMF ENGRS OTHER RANK
22131	10/8/1957	FMF ENGRS OTHER RANK
22351	4/27/1959	FMF ENGRS OTHER RANK
22707	10/2/1960	FMF ENGRS OTHER RANK
23254	8/30/1963	FMF ENGRS OTHER RANK
23258	8/3/1963	FMF ENGRS OTHER RANK
23299	4/4/1961	FMF ENGRS OTHER RANK
23343	11/23/1963	FMF ENGRS OTHER RANK

EMPLOYEE_ID	BIRTH_DATE	Department
23495	7/20/1963	FMF ENGRS OTHER RANK
23553	9/18/1963	FMF ENGRS OTHER RANK
25035	9/21/1963	FMF ENGRS OTHER RANK
25576	12/12/1960	FMF ENGRS OTHER RANK
25663	10/16/1962	FMF ENGRS OTHER RANK
25670	12/4/1962	FMF ENGRS OTHER RANK
25840	3/22/1963	FMF ENGRS OTHER RANK
27090	4/19/1962	FMF ENGRS OTHER RANK
27100	5/26/1963	FMF ENGRS OTHER RANK
27131	1/4/1963	FMF ENGRS OTHER RANK
27229	1/25/1963	FMF ENGRS OTHER RANK
27696	4/12/1963	FMF ENGRS OTHER RANK
31783	1/1/1963	FMF ENGRS OTHER RANK
NJ399	3/8/1963	FMF ENGRS OTHER RANK
25300	9/9/1963	NAVY OFFICERS
27625	10/19/1962	NAVY OFFICERS
25208	1/28/1963	NAVY OTHER RANKS
26154	11/24/1963	NAVY OTHER RANKS
26205	8/22/1963	NAVY OTHER RANKS
26223	1/23/1963	NAVY OTHER RANKS
26227	1/11/1963	NAVY OTHER RANKS
26228	2/22/1963	NAVY OTHER RANKS
21345	6/28/1950	TF OFFICERS
21493	5/20/1954	TF OFFICERS
21793	1/23/1958	TF OFFICERS
21798	12/23/1955	TF OFFICERS
21804	5/18/1957	TF OFFICERS
21851	11/6/1957	TF OFFICERS
21909	3/11/1957	TF OFFICERS
22604	4/1/1960	TF OFFICERS
22627	2/14/1959	TF OFFICERS
22893	11/24/1958	TF OFFICERS
23267	10/8/1959	TF OFFICERS
23288	2/25/1960	TF OFFICERS
23296	4/3/1962	TF OFFICERS
23453	12/30/1957	TF OFFICERS
23616	2/29/1960	TF OFFICERS
23638	12/18/1956	TF OFFICERS
23918	5/8/1956	TF OFFICERS
24742	6/29/1959	TF OFFICERS
25072	9/12/1960	TF OFFICERS
25161	10/22/1962	TF OFFICERS
27718	1/22/1961	TF OFFICERS
24125	8/15/1962	TF OTHER RANKS
25180	9/15/1963	TF OTHER RANKS

EMPLOYEE_ID	BIRTH_DATE	Department
25440	7/29/1963	TF OTHER RANKS
27138	9/28/1962	TF OTHER RANKS
27805	6/17/1960	TF OTHER RANKS
27870	5/16/1953	TF OTHER RANKS
29092	7/2/1963	TF OTHER RANKS
24153	8/12/1963	1 FIR OTHER RANKS
24779	7/26/1963	1 FIR OTHER RANKS
25472	11/8/1963	1 FIR OTHER RANKS
25754	12/4/1963	1 FIR OTHER RANKS
25927	12/27/1962	1 FIR OTHER RANKS
26035	9/2/1963	1 FIR OTHER RANKS
26979	9/26/1963	1 FIR OTHER RANKS
24150	7/9/1962	1FIR UNDOF SYRIA-OTHER RANKS
24603	10/25/1963	1FIR UNDOF SYRIA-OTHER RANKS
24649	12/30/1963	1FIR UNDOF SYRIA-OTHER RANKS
25032	10/30/1963	1FIR UNDOF SYRIA-OTHER RANKS
26070	10/15/1963	1FIR UNDOF SYRIA-OTHER RANKS
27606	7/19/1962	1FIR UNDOF SYRIA-OTHER RANKS
27688	10/29/1963	1FIR UNDOF SYRIA-OTHER RANKS
28009	10/7/1963	1FIR UNDOF SYRIA-OTHER RANKS
28071	10/4/1963	1FIR UNDOF SYRIA-OTHER RANKS
29596	1/1/1960	1FIR UNDOF SYRIA-OTHER RANKS
30348	6/17/1953	1FIR UNDOF SYRIA-OTHER RANKS
33810	2/14/1962	1FIR UNDOF SYRIA-OTHER RANKS
23567	12/16/1962	FIR SINAI OTHER RANKS
23594	9/24/1962	FIR SINAI OTHER RANKS
24334	5/15/1963	FIR SINAI OTHER RANKS
24485	5/11/1963	FIR SINAI OTHER RANKS
25881	5/25/1963	FIR SINAI OTHER RANKS
22480	1/1/1959	HEADQUARTERS LFC OFFICERS
23814	10/18/1959	HEADQUARTERS LFC OFFICERS
22720	5/12/1958	HEADQUARTERS LFC ORS
23558	2/11/1961	HEADQUARTERS LFC ORS
23626	4/6/1963	HEADQUARTERS LFC ORS
23744	2/20/1963	HEADQUARTERS LFC ORS
23832	3/16/1963	HEADQUARTERS LFC ORS
24093	4/25/1963	HEADQUARTERS LFC ORS
24302	12/25/1959	HEADQUARTERS LFC ORS
24392	1/3/1963	HEADQUARTERS LFC ORS
24434	9/1/1963	HEADQUARTERS LFC ORS
24878	2/20/1962	HEADQUARTERS LFC ORS
24974	8/11/1962	HEADQUARTERS LFC ORS
25324	9/20/1963	HEADQUARTERS LFC ORS
25826	9/16/1963	HEADQUARTERS LFC ORS
26003	6/10/1962	HEADQUARTERS LFC ORS

EMPLOYEE_ID	BIRTH_DATE	Department
26018	9/14/1961	HEADQUARTERS LFC ORS
26052	2/28/1963	HEADQUARTERS LFC ORS
26165	10/20/1963	HEADQUARTERS LFC ORS
26896	10/10/1963	HEADQUARTERS LFC ORS
27102	12/2/1959	HEADQUARTERS LFC ORS
27177	4/28/1963	HEADQUARTERS LFC ORS
27254	10/18/1963	HEADQUARTERS LFC ORS
27897	12/25/1963	HEADQUARTERS LFC ORS
28108	8/8/1963	HEADQUARTERS LFC ORS
22833	6/24/1960	FIR OFFICERS
24455	12/10/1961	FIR OFFICERS
22541	6/27/1959	FIR OTHER RANKS
23067	8/18/1961	FIR OTHER RANKS
23647	6/30/1962	FIR OTHER RANKS
24033	9/20/1963	FIR OTHER RANKS
24107	7/11/1963	FIR OTHER RANKS
24128	8/4/1963	FIR OTHER RANKS
24168	5/12/1963	FIR OTHER RANKS
24169	8/10/1963	FIR OTHER RANKS
24173	2/12/1963	FIR OTHER RANKS
24435	8/15/1963	FIR OTHER RANKS
24545	10/6/1962	FIR OTHER RANKS
24704	4/23/1963	FIR OTHER RANKS
24783	9/23/1963	FIR OTHER RANKS
24921	7/12/1963	FIR OTHER RANKS
24995	5/21/1963	FIR OTHER RANKS
25002	7/17/1963	FIR OTHER RANKS
25238	2/27/1963	FIR OTHER RANKS
25343	4/5/1963	FIR OTHER RANKS
25595	2/28/1963	FIR OTHER RANKS
25636	11/21/1963	FIR OTHER RANKS
25730	6/29/1963	FIR OTHER RANKS
25798	7/22/1963	FIR OTHER RANKS
25828	8/9/1963	FIR OTHER RANKS
25922	10/11/1963	FIR OTHER RANKS
26026	6/1/1963	FIR OTHER RANKS
26334	8/9/1963	FIR OTHER RANKS
26503	5/7/1963	FIR OTHER RANKS
26747	11/27/1963	FIR OTHER RANKS
26804	3/3/1963	FIR OTHER RANKS
26860	10/22/1963	FIR OTHER RANKS
27484	5/25/1963	FIR OTHER RANKS
27504	11/2/1963	FIR OTHER RANKS
27549	5/19/1963	FIR OTHER RANKS
27889	6/25/1961	FIR OTHER RANKS

EMPLOYEE_ID	BIRTH_DATE	Department
27960	7/8/1963	FIR OTHER RANKS

Appendix 1.11: RFMF Payroll Blank Bank Account Details

EMPLOYEE_ID	Department
23437	FMF STRATEGIC HQ ORS
30698	FORCE TRNG GROUP-OFFICERS
25300	NAVY OFFICERS
25989	TF OFFICERS
27617	TF OFFICERS
29438	TF OFFICERS
27860	TF OTHER RANKS
26936	1FIR UNDOF SYRIA-OFFICERS
28294	1FIR UNDOF SYRIA-OTHER RANKS
30950	HEADQUARTERS LFC ORS
23303	FIR OTHER RANKS
25272	FIR OTHER RANKS

FINANCIAL MANAGEMENT

INFORMATION SYSTEM

Table of Content

Acronyms

Abbreviation	Meaning
AP	Accounts Payable Module
AR	Accounts Receivable Module
BCP	Business Continuity Plan
COBIT	Control Objectives for Information and related Technology
COP	Costed Operational Plan
CS	Common Services Module
DRP	Disaster Recovery Plan
FA	Fixed Asset Module
FD	Fund Accounting Module
FMIS	Financial Management Information System
GL	General Ledger Module
ICT	Information and Communication Technology
IDI	INTOSAI Development Initiative
IS	Information System
ISAAS	Information System Audit and Assurance Standards
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standards Organization
ISSAI	International Standards of Supreme Audit Institutions for ISSAI
ITCS	Information Technology and Computing Services
MoE	Ministry of Economy
MS	Master Security Module
ORGS	Organization
PO	Purchases Module
SGO	Solicitor General's Office
SLA	Service Level Agreement
WPO	Work Unit Set ID for Purchase Module

Executive Summary

Introduction

The Office of the Auditor-General conducted an Information Systems (IS) audit on the financial management information system (FMIS) under the responsibility of the Ministry of Economy (MoE) through the FMIS Section.

The FMIS was endorsed for implementation by Cabinet on 9th March, 2004 as one of the financial management reform initiative of government to strengthen financial governance across government.

There are a total of forty-two (42) Ministries/Departments using FMIS with a range of financial modules such as accounts receivable (AR), fixed assets (FA), general ledger (GL), accounts payable (AP), Purchasing (PO) module, Fund Accounting (FD) module, Master Security (MS) module and Common Services (CS) module.

The FMIS software is supplied by the SSDGA Global Technologies Inc. for which an annual license fees are paid by the MOE.

Audit Focus

Our audit focused on the system assurance based on the general controls and application controls surrounding the FMIS that the MoE is responsible with.

Significant Findings

- Absence of business continuity plan, disaster recovery plan, service level agreement, IT strategy plan and risk management plan;
- No presence of a change management plan, information security policy and incidence response policy;
- No periodic reviews of policies and procedures over the FMIS; and
- Access control management of system users needs to be properly monitored and reviewed.

Audit Conclusion

FMIS Section needs to:

- Reinforce the general control policies surrounding the application; and
- Develop the required plans necessary for documented policies, manuals and plans

1.0 Auditing Standards

We have conducted this audit in accordance with the International Standards of Supreme Audit Institutions for ISSAI 1 on Lima Declarations, ISSAI Guidelines and Standards, Information Systems Audit and Control Association (ISACA), Information System Audit and Assurance Standards (ISAAS) and International Standards Organization (ISO) IT Standards.

2.0 Reference to Comments

Comments provided by the FMIS Section of the MOE and Department of Information Technology Computing Services (ITCS) have been incorporated in this report.

3.0 Subject Matter and Scope

The subject matter for this audit was to obtain the system assurance on the FMIS general controls and application controls of the FMIS system.

Our audit focused on the system assurance based on the general controls and application controls surrounding the FMIS that the MoE is responsible to monitor and safeguard the resources of government maintained by the system.

4.0 Audit Objective

The objectives of the audit were to:

i. Assess whether the general controls in the areas of organization and management controls, IT operational, physical controls (access and environment), logical access controls, program change controls and the business continuity and disaster recovery controls exist; and

ii. Review the application controls in terms of the input controls, processing controls and output controls to ensure integrity, confidentiality and availability of information at all times.

5.0 Audit Criteria

The MoE as a government agency must operate in environment with due considerations of legislations and policies. The criteria for the audit are based on regulations and manuals designed to ensure compliance with:

- ISO27001 on Information Security Management;
- ISO 38500 on Governance;
- COBIT control framework for IT Governance;
- ISSAI 5300 Guideline for IT Audit professional in conducting IT Audits;
- ISSAI 5310 Information Systems Security Review Methodology;
- ISAAS 1008 Criteria;
- IDI Handbook on IT Audit for SAI; and
- AFROSAI – IT Audit Manual.

6.0 Methodology

Our auditing methodology enables us to carry out the audit and using the system-based audit approach in the conduct phase with reference to the ISSAI 4000 compliance audit standards.

Audit techniques used for gathering evidence and conducting IT audit analysis included the following:

i. documentary reviews of general controls and application controls including the interview of key personnel at the FMIS Section of MoE and the ITCS; and
ii. evaluation of the questionnaire responses by the FMIS Section of MoE.

7.0 Audit Findings

7.1 Absence of Business Continuity Plan and Disaster Recovery Plan

Business Continuity Plan (BCP) is the process an organisation uses to plan and test the recovery of its business processes after a disruption. It also describes how an organisation will continue to function under adverse conditions that may arise (for example, natural or other disasters)[1].

A BCP is an enterprise wide group of processes and instructions to ensure the continuation of business processes - incl., but not limited to IT - in the event of an interruption. It provides the plans for the enterprise to recover from minor incidents to major disruptions. The plan is usually owned and managed by the business units and a disaster management or risk prevention function in the enterprise[2].

Disaster Recovery Plan (DRP) is the process of planning and testing for recovery of IT infrastructure after a natural or other disaster. It is a subset of Business Continuity Planning. BCP applies to the organisational business functions whereas DRP to the IT resources that support the business functions[3].

The objective of having a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) with the associated controls is to ensure that the organization can still accomplish its mission. This will not lose the capability to process, retrieve and protect information maintained in the event of interruption or disaster leading to temporary or permanent loss of computer facilities.

Business continuity and disaster recovery remain an inherent risk to all government departments. There needs to be close alignment between the disaster recovery plans and business expectations set out in the business continuity plans. FMIS is making use of infrastructure as a service provided by ITCs and also needs to consider how these systems can be recovered in the event of hardware failures, network failures, program failures and other unforeseen circumstances.

We were not provided with a BCP and DRP by the management of FMIS during our audit. Furthermore, plans were also not provided at the organizational level after enquiring with the Policy Division with MoE. The Acting Manager ITCS advised us that FMIS team needs develop its own BCP for its FMIS because ITCS only have its own backup and restore plan and only applicable to the ITCS data centre alone[4]. MoE stated that it will develop its BCP Document and Risk Management Framework for 2020 and this will include Risk Management Plans from each Divisions, including the FMIS Section, developed by the respective Divisions[5].

The absence of a well-defined BCP and DRP can be catastrophic in the event of a disaster or unplanned calamities.

[1] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)
[2] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[3] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)
[4] ITCS email response on 02/08/20 to FMIS Manager
[5] MoE management comments on 30/09/2020

Recommendation

The BCP and DRP should be formally documented, periodically tested and updated as necessary by FMIS.

Timeline of Action: 30 December 2020

Responsible for Action: Head of Administration Unit

7.2 Service Level Agreement (SLA) or Memorandum of Understanding (MOU) with ITCS

The SLA documents the various parameters that the IT organisation uses to provide service to the business. The parameters in the SLA are generally agreed to by the business owners and the IT Organisation[6].

An internal service level agreement is between the IT organization and the business owners. Failure to adhere to service level agreements affects meeting of users' requirements. The IS operations and business owners should agree on capacity management, IT financial management and availability management[7].

Hence, the SLA or MOU should clearly specify the following requirements with:

I. Detailed service description which will be provided by ITCS as expected or requested by MoE;
II. Responsibilities for each party involved;
III. Applicable service hours;
IV. Extent of service to be provided within the service window and outside the service window;
V. Reliability of expected services;
VI. Contact points and escalation - communication channel;
VII. System performance reports;
VIII. System security; and
IX. Costs involved (if any).

Our audit noted that the Department of ITCS is providing MoE the infrastructure as a service by hosting the FMIS server at their Data Centre and also providing network related services. However, there is no SLA or MOU between MoE and ITCS.

Business operations can be affected and processes not executed on a timely basis as issues might take long to be resolved due to unclear/ no understanding of specific responsibilities of each party.

The services which are provided by the hosting party can result in unreliable services (not meeting expectations of services required), absence of system performance monitoring and reporting, can

[6] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)
[7] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)

incur costs but can be controlled with an SLA or MOU to provide a secure system of operations and periodic reviews to deliberate on possible risks and threats.

The MoE stated that the audit recommendation will be discussed with the relevant stakeholders and an SLA or MOU drawn up with the Department of ITCS to demarcate clear line of responsibilities and continually support the government's financial platform noting the risk assessments carried out around these areas[8].

Recommendation

The FMIS Section in consultation with ITCS should draw up a SLA or a MOU to ensure that the responsibility of each department is known and implemented.

Timeline of Action: 30 December 2020

Responsible for Action: Manager FMIS Section

7.3 IT Strategic Plan

Government will explore options to provide the necessary infrastructure to embrace new technology. Appropriate new technology will be adopted to raise overall efficiency and productivity and to improve service delivery across all sectors. A facilitative environment will be created to assist the importation of new and modern technology.[9]

An IT strategy plan describes how the IT department can assist the organisation in achieving its objectives and is an integral part of the business strategy. The IT strategy relates to the long-term direction an organisation wants to take in leveraging IT for improving business processes.[10] Therefore in an ideal organizational level IT strategic plan exists, it translates business objectives into IT goals and requirements, addresses the needed IT resources to support the business, and it is reviewed and updated periodically.

The FMIS Section does not have an IT Strategy but works in consultation with the Department of ITCS for procurement and execution of its IT projects. Since the FMIS does not have a documented IT direction and spending for the medium term (3 – 5 years) aligned to the national development plan, then the scope for better strategic planning should take into account all the current government initiatives. Therefore, the IT Strategic Plan will be helpful in planning and acquisition of resources (staff, equipment, finance, etc.) and assist in the Ministry budgeting process. ITCS advised us that their ITS strategic plan is based on the 5-20-year national development plan where its Annual Corporate Plan is drawn specifically for ITCS but this is not available for distribution to other ministries and departments[11].

The MoE further emphasized that there is an existing Strategic Plan that is aligned to the annual costed operational plan from the envisioned National Development Plan. The IT section is part of the Office Services Unit and the overarching Administration Division within the MOE. The

[8] FMIS management comments on 30/09/20

[9] 5 Year & 20 Year National Development Plan 2017

[10] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)

[11] ITCS email response on 02/08/20 to FMIS Manager

Administration Costed Operation Plan (COP) entails the work plan that the Office Services/Information Technology Division which will undertake in the new fiscal year[12].

Absence of an IT Strategy, can result in an unclear strategic and business direction for IT projects, poor project and budget planning, poor project monitoring and implementation of projects, possibility of compromising timeliness and quality of work, and the limitation of identifying risks and monitoring it.

Recommendation

The FMIS Section should prepare an IT Strategic plan/ IT strategy from the organizational strategic plan for a proper direction and monitoring of anticipated IT projects aligned to the National Development Plan.

Timeline of Action: 30 December 2020

Responsible for Action: Head of Administration Unit

7.4 Risk Management Plan

The risk management plan is embedded in the responsibilities of the organization's management and IT regularly assess and report IT related risks and organizational impact. Exposures of any problems are followed up, with special attention paid to any potential negative effects on the overall objectives of the organization.[13]

Our audit of the FMIS noted that there is no risk management framework present in the Ministry to facilitate the design and development of its risk management plan in order to identify and document the risk with control measures that will mitigate the risks identified or to be kept at a minimum. However, the Ministry is in the process of setting up a Risk Unit which will work with the respective divisions in the MoE to identify and manage the risks. External risks like the hosting of the system at ITCS of its hardware without proper disaster recovery planned site is still exposed to increased risk of data loss in the case of a disaster.

ITCS confirmed that its risk management plan only reflects the data center and is confidential but this can be modified to make it suitable for other Govnet user environment which needs to be vetted and approved but will take a longer process of about 2-3 months. Hence the ITCS planned risk policy and procedures is only applicable to the datacentre which will need to be reviewed by the ITCS Policy Review Committee before its vetted by Solicitor General's Office(SGO) and then approved by ITCS Steering Committee for ITC use only[14].

Since there's no existing risk management framework to support the development of a risk management plan to be executed when mitigating risks or lower the risks from occurring at the FMIS Section of the Ministry then the vulnerability against unforeseen risks to happen or might happen still needs to be tested provided if a disaster recovery plan (DRP) is present.

[12] FMIS management comments on 30/09/20

[13] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)

[14] ITCS email response on 02/08/20 to FMIS Manager

MoE stated that the formulated IT Committee will work to develop a BCP Document and Risk Management Framework this year, 2020/2021. This will include Risk Management Plans from each Divisions, including the FMIS Section (FMIS), developed by respective Divisions[15].

Recommendations

1. **FMIS Section should prioritize the setup of the Risk Unit as FMIS is a mission critical system and the risks could have a huge impact on the system which will affect all the Ministries and Departments which use the system; and**

2. **External risks associated to the FMIS should also be considered.**

Timeline of Action: 30 December 2020

Responsible for Action: Head of Administration Unit

7.5 Change Management Plan

The change management plan process is normally used to manage and control changes to software, hardware and related documentation. Change management is necessary where the impact of an unapproved or accidental change could have severe risks and financial consequence for an organisation. Organisations follow a defined change management procedure which requires approval from a board before being implemented into the operational environment.[16]

The change management plan will minimize the impact a change can have on the business, employees, customers, and other important stakeholders. The purpose of the process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services and respond to the customer's changing business requirements while maximizing value at minimal cost. Our audit noted that the FMIS Section does not have a change management plan process in place to account and document to control the system lifecycle innovations and alterations.

ITCS stated that its change management plan only reflects the data center and is confidential but will need to be modified to make it suitable for other Govnet environment, reviewed by ITCS Policy Review Committee, vetted by SGO and approved by ITCS Steering Committee which takes about 2-3 months for the finalization process[17].

In the absence of documented change management plan and lack of control over change management process for the FMIS increases the risk of impact on user with a legacy of failed change and change saturation. Hence, it is required to ensure that no unnecessary changes are made to the system and all changes for the system needs to be documented.

[15] FMIS management comments on 30/09/20
[16] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[17] ITCS email response on 02/08/20 to FMIS Manager

MoE have stated that it will develop a Change Management Planning Document to control over any future changes to the FMIS including proper documentation processes that is aligned to best practice & requirements[18].

Recommendation

1. **FMIS Section to develop and implement a Change Management Plan for the FMIS system.**

2. **FMIS Section to have a proper documentation maintained for any system upgrades for future reference.**

Timeline of Action: 31 July 2021

Responsible for Action: Manager FMIS Section

7.6 Absence of Information Security Policy

This policy establishes the requirements for protection of information assets, and may refer to other procedures or tools on how these will be protected. The policy should be available to all employees responsible for information security, including users of business systems who have a role in safeguarding information (personnel records, financial input data, etc.).[19]

Information security is inherently risky and confidentiality remains critical for the different levels of user access. The failure to promptly terminate system access by officers that have left the services, and for the continuous periodic user access rights review are some prevalent deficiencies identified. Examples extracted will be discussed in the later issues based on data provided by the FMIS Section.

Our audit noted that the FMIS Section does not have an Information Security Policy but places heavy reliance on ITCS policies which may have not been updated. Hence the responsibility for security processes and controls is often spread throughout ministries and departments as well rather than with a small group of individuals with clear accountability. This can increase the likelihood of controls failing. We also observed that with appropriate risk management principles and accountabilities, this will be connected to IS security-related activities. An information security policy should have the following features and content:

1. Responsibilities of different set of users
2. Procedures for non – compliance and breaches
3. Acceptable use policy
4. Anti – virus policy
5. Back – up and restoration policy
6. Change management policy
7. Clean disk policy
8. Data access policy
9. Database management policy
10. Data storage policy
11. Disaster recovery plan policy

[18] FMIS management comments on 30/09/20
[19] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

12. Information classification policy
13. Log management policy
14. Password management policy
15. Security awareness and training policy
16. User access management policy
17. Bluetooth baseline requirement policy
18. Remote access policy
19. Router and switch security policy
20. Wireless communication standard and
21. Wireless communication policy.

ITCS stressed that its information security policy only reflects the data centre and is confidential based on the Information Security Management System (ISMS) standard for ITCS processes and documents that deal deals with information security but will need to be modified to make it suitable for other Govnet environment, reviewed by ITC Policy Review Committee, vetted by SGO and approved by ITCS Steering Committee which takes about 2-3 months for the finalization process[20].

High information security risks may arise from the absence of proper structures, processes and policies, such as the misappropriation of assets, unauthorised disclosure of information, unauthorised access, and vulnerability to logical and physical attacks, disruption and information unavailability, misuse of information, noncompliance with personal data laws and regulations, and failure to recover from disasters.

Absence of formally documented information security procedures and processes relating to FMIS can increase the risk of data manipulation and information leakage. The FMIS Section stated that it will develop its Information Security Policy and align to the requirements of the ISO 27001 on Information Security Management Framework and best practice[21].

Recommendation

The IT Security Policy should be documented, and periodically updated at all levels of access and sharing as necessary to safeguard the FMIS data used as information for decision-making purposes.

Timeline of Action: 30 December 2020

Responsible for Action: Head of Administration Unit

7.7 Incident Response Policy

Incident response management is the systems and practices used to determine whether incidents or errors are recorded, analysed and resolved in a timely manner. Problem management aims to resolve issues through investigation and in-depth analysis of a major or recurring incident in order to identify the root cause.[22]

[20] ITCS email response on 02/08/20 to FMIS Manager

[21] FMIS management comments on 30/09/20

[22] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

Our audit noted that the Ministry does not have an Incident Response Policy to follow through when incidents happen where the normal organizational flow is followed to escalate incidents. However, an issue register is maintained by the FMIS Section where issues identified are recorded by Ministry staff. It was noted that but there were delays in addressing and providing timely responses to resolve the issues due to absence of proper channels for escalation of issues.

Alternatively, re-occurring issues can be resolved through awareness session channelled to the FMIS Section designated officer(s) and to be documented at all times with actions taken for issues like unauthorized user access or intrusion (security), network failures (operational), low functionality of software (service delivery) or lack of end user skills (training).

ITCS emphasized that its incidence response policy only reflects the data center and is confidential but will need to be modified to make it suitable for other Govnet environment, reviewed by ITC Policy Review Committee, vetted by SGO and approved by ITCS Steering Committee which takes about 2-3 months for the finalization process[23].

Without a proper incident management process to resolve issues through investigation and in-depth analysis of a major or recurring incident in order to identify the root-cause can result in FMIS Section in not capturing all incidents, near-misses and hazards that need to be reviewed, investigated and actioned within the required timeline.

MoE stated that it will develop an Incident Response Policy to direct incident management and improves quality delivery platforms that will ultimately lead to efficiency within operations by addressing gaps within existing structure[24].

Recommendations

1. **FMIS Section should create an Incident Response Policy**.

2. **FMIS Section to review its current incident response practices so that ongoing issues are appropriately highlighted and captured in a computerized log for future audit trail.**

Timeline of Action: 30 December 2020

Responsible for Action: Manager FMIS and Head of Administration Unit

7.8 Access Control Management

In a government environment, access control is important because many government entities process sensitive data and privacy concerns limit who should view various parts of the information. Access controls ensures that only users with the process credentials have access to sensitive data.[25] The FMIS Section will be monitoring all user access on a quarterly basis.[26]

The four (4) major processes under the PO Module[27] are:

[23] ITCS email response on 02/08/20 to FMIS Manager
[24] FMIS management comments on 30/09/20
[25] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[26] FMIS Access and Password Policy S6.12 (2015)
[27] FMIS Access and Password Policy S8.2.1 (2015)

i) Standard Order Entry (PO401);
ii) Approval (PO348);
iii) Receiving (PO481); and
iv) Invoicing (PO621)

No PO Approver should have access to (i), (iii) and (iv).[28]

The objective of logical access controls is to protect the financial applications and underlying data files from unauthorized access, amendment or deletion, have aadequate input validation controls, appropriate management of source documents, data collection and entry, adequate processes for error handling and management of data entry authorization into the application.

Our analysis of four organizations (ORGS) selected through random sampling of all purchase order (PO) users noted that the PO users were categorized by Work Unit Set ID against each Work Unit ID which represents a Module View Panel. **Table 1.2** provides the detail.

Table 1.2: Authorized PO Approvers

PO Module Panel	Work Unit Set ID
PO401	WPO07
PO348	WPO06
PO481	WPO15
PO621	WPO05

Source: **PO Modules provided by FMIS**

Furthermore, it was noted that the PO approvers should have access to PO348 which is represented by Work Unit Set ID WPO06. However, PO Approvers also have access to Work Unit WPO07, WPO15 and WPO05 in some cases. These "Approvers" should not have access for "Preparers" as well due to the risk of data manipulation by the same user accessing the module panel using the same access.

The system does not enforce the business rules of FMIS. Access to PO Approvers are granted by FMIS after this is approved by the Head of Departments from the agency level. Our audit also noted that some current and former Permanent Secretaries have access to more than one "org in FMIS". Refer to **Table 1.3** for sample of Permanent Secretaries details extracted.

Table 1.3: Permanent Secretary with more "Org" Access

User Access Status	Orgs Accessed	No. of Orgs Access	User Access Status	Orgs Accessed	No. of Orgs Access	User Access Status	Orgs Accessed	No. of Orgs Access
Current PSRM	1481	8	Current A/PSMEHA	1702	3	Former PSMEHA	1702	4
	1868			2100			2222	
	3030			2222			2500	
	3686			0568			3200	
	4040			1481			0568	4
	4041			1868			1481	

[28] FMIS Access and Password Policy S8.2.3 (2015)

User Access Status	Orgs Accessed	No. of Orgs Access	User Access Status	Orgs Accessed	No. of Orgs Access	User Access Status	Orgs Accessed	No. of Orgs Access
	4042		Current PSITA	3030	7	Former PSSI	1868	
	4083			4040			3030	
Current PSPMO	0201	5		4041		Former PSYS	1868	3
	0270			4083			2100	
	0800		Former PSW	4040	5		2500	
	2222			4041		Current DSG	0300	5
	4289			4042			1515	
Former PSMOFA	0800	2		4081			1600	
	1571			4083			1667	
Former PSMYS	2100	2	Former A/PSLMR	3333	2		2100	
	2500			3379		Former PSMEIRP	0707	2
Former PSMOF	0467	2	Former PSMEHA	2100	3		3200	
				2222		Former PSITA	1481	2
	1763			2500			1868	
							1763	

Source: **PO Modules Access provided by FMIS**

It was noted that review of users as prescribed in the FMIS Access and Password Policy requirements is not carried out which increases the risk of unauthorized access and manipulation of data input that can go undetected.

FMIS Section has mentioned that it has commenced conducting a gap assessment to review the existing platform and amend where necessary. The revised policy should be adequate to align to operational requirements and address arising needs[29].

Recommendations

1. **FMIS Section should work with Ministries and Departments to review the access on panels and remove those that should not be granted to PO approvers;**

2. **FMIS Section should periodically review all users and access; and**

3. **FMIS Section should review and update the FMIS Access and Password Policy to accommodate scenarios such as Permanent Secretaries having access to more than organization.**

Timeline of Action: 30 December 2020

Responsible for Action: Manager FMIS Section

[29] FMIS management comments on 30/09/20

8.0 Conclusion

The results of the audit from the records and information provided indicated that the FMIS Section of MoE needs to strengthen the general controls and plans necessary for the data input and processing.

The response provided by the FMIS Section and proposed actions are viewed very positively and will assist in enhancing the IT systems used by Ministries and Departments.

FIJI EDUCATION

MANAGEMENT INFORMATION

SYSTEM

Table of Content

Acronyms

Abbreviation	Meaning
BCP	Business Continuity Plan
COBIT	Control Objectives for Information and related Technology
COP	Costed Operational Plan
DMZ	Demilitarized Zone
DRP	Disaster Recovery Plan
FEMIS	Fiji Education Management Information System
FESA	Fiji Education Staffing Appointment
FESP	Fiji Education Sector Program
ICT	Information and Communication Technology
HTTP	Hypertext Transfer Protocol
IDI	INTOSAI Development Initiative
IS	Information System
ISAAS	Information System Audit and Assurance Standards
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
ISSAI	International Standards of Supreme Audit Institutions for ISSAI
IT	Information Technology
ITCS	Information Technology and Computing Services
MEHA	Ministry of Education, Heritage and Arts
SLA	Service Level Agreement
SSL	Secure Sockets Layer

Executive Summary

Introduction

The Office of the Auditor-General conducted an Information System (IS) audit on the Fiji Education Management Information System (FEMIS) under the responsibility of the Ministry of Education, Heritage and Arts (MEHA) through the IT Department.

The IT Department within MEHA is the executing unit that controls and maintains the FEMIS database which is a comprehensive database on schools, students, teachers and properties. Prior to the FEMIS, there was a Fiji Education Staffing Appointment (FESA) system application developed for the Ministry of Education in 2005 with the assistance of the Fiji Education Sector Program (FESP). It commenced in mid-2003 for a three to five-year period, providing assistance to Ministry of Education in a range of education and administrative support projects. FESA was originally developed for application within the personnel section of the Ministry in order to manage personnel and staff establishment information for the Ministry's schools and offices.

Audit Focus

The Office of the Auditor-General carried out an IT audit on the *IT Governance structure and IT Operations that should deliver and meet the IT needs and requirements* of the MEHA.

Significant Findings

The findings from the IT audit of FEMIS of MEHA are:

- IT governance framework for MEHA;
- Absence of business continuity plan and disaster recovery plan;
- Absence of security information policy;
- No presence of service level agreement or memorandum of understanding;
- No risk management plan in place;
- Physical security access;
- Location of the test and live server environment; and
- Irregular backups.

Audit Conclusion

The results of the audit from the records and information provided indicate that the MEHA – IT Department needs to strengthen the general controls by revising and updating policies for the system to reinforce and improve the Ministry's IT governance and IT operations components.

Overall, MEHA requires special attention on the use of unsecured internet protocol for http network to be addressed and the frequency of backups to be scheduled so that assurance of business continuity in the operations of MEHA remains paramount.

1.0 Auditing Standards

We have conducted this audit in accordance with the International Standards of Supreme Audit Institutions for ISSAI 1 on Lima Declarations, ISSAI 5300 for IT Audit professional in conducting IT Audits, Information Systems Audit and Control Association (ISACA) Information System Audit and Assurance Standards (ISAAS) and International Standards Organization (ISO) IT Standards.

2.0 Reference to Comments

Comments provided by the IT Department of the MEHA have been incorporated in this report.

3.0 Subject Matter and Scope

The subject matter for this audit was to obtain the system assurance on the MEHA Information Technology (IT) Operations and related IT governance controls to safeguard the resources of the FEMIS and FESA systems.

We assessed the FEMIS practices undertaken by the IT Department to:

i. validate the IT governance practices in place; and
ii. review and evaluate the IT operations based on the adequacy of policies and procedures are in place for preparations, handling and input of data for the application, and examine the general and application controls.

4.0 Audit Objective

The principal objective of the audit is to perform sufficient audit work to obtain assurance on the level of controls used by the FEMIS system to safeguard the resources of the government maintained through the system. The other objectives of undertaking the FEMIS system audit include:

- IT Governance in the areas of organization and management controls, IT operational, physical controls (access and environment), logical access controls – the objective will be to see whether logical access controls, acquisition and program change controls and the business continuity and disaster recovery controls.
- IT Operations Application controls in terms of the input controls, processing controls and output controls.

5.0 Audit Criteria

The criteria which was used to assess the IT governance and IT operations is drawn from the IDI Active IT audit manual and the AFROSAI – E IT audit manual based on the COBIT framework, ISO38500 on IT Governance for the organization and ISO27001 on Information Security Management.

6.0 Methodology

Our auditing methodology enables us to carry out effective and efficient audits and also enables us to probe more usefully into issues of accountability, transparency and probity so as to make recommendations on internal controls.

This IT audit used the risk-based audit approach when analysing the overall control environment of the IS of the FEMIS that was carried out before the commencement of the audit to assist in the assessment of the inherent and control risks associated with the audit. Also, this IT audit focused on the system-based audit approach in the conduct phase with reference to the ISSAI 4000 compliance audit standards.

Audit techniques used for gathering evidence and conducting audit analysis included the following:

i. documentary reviews and interview of key personnel at the IT Department of MEHA and the Information Technology and Computing Services (ITCS); and
ii. evaluation of the questionnaire responses by the IT Department of MEHA.

7.0 Audit Findings

Question: ***Is there a reliable IT Governance structure to deliver and meet the IT needs requirement of the MEHA?***

Organizations require a structured approach for managing the IT system environment and other related challenges to ensure that agreed objectives for IT with good management controls in place and effective monitoring of performance to keep on track and avoid unexpected outcomes[1].

With reference to IT governance in an organization with a focus on projects, there is a need to understand the management framework in place on whether periodic analysis and revisions of the controls has been imposed by the framework to ensure that IT is aligned to the business needs of MEHA. Also, in the same process this is to ensure that there are organizational structures, policy, and procedures in place that enables MEHA to meet its mandate for its business goals[2]. Discussed below are the findings to corroborate the need of having a proper IT governance in place.

7.1 IT Governance Framework for MEHA

Control Objectives for Information and related Technology (COBIT) is a control framework for IT governance, which defines the reasons IT governance is needed, the stakeholders and what it needs to accomplish. It is a roadmap to good IT governance. COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure[3].

IT operations in MEHA were noted to lack good governance in the absence of internal IT policies, poor IT formal communication and absence of evidence on work carried out in maintenance, monitoring and evaluation of IT processes. The audit team was not provided with minutes of meetings relating to matters or issues pertaining to IT charter, IT strategic plan, IT steering committee meeting outcomes, IT business plan and IT work plan.

Even though the IT governance of IT operations in the public sector is provided in the Reform of the Department of ITCS Act 2016 where the procurement of ICT goods, services and works of ITCS and Government Ministries and Departments but each agency is still responsible for the implementation of ITCS policies, reviewing its structure, size and composition.

Ministries are still accountable and responsible for its software, systems, and hardware for the IT initiatives or IT strategic procurement recommended to the ITCS Steering Committee for endorsement and final approval. Hence a proper IT Governance Framework by the Ministry can ensure that there is clear strategic and business direction for IT projects, there is proper project and budget planning, consistent project monitoring and implementation, appropriate timelines not to compromise quality of work and ensure that risks are identified and monitored.

Through this IT governance framework, the Ministry should ensure that all three levels - strategic, tactical and operational responsibilities are covered. On the strategic level like the Ministry's executive management meetings has the responsibility to evaluate, direct, monitor and mitigate risks whilst the tactical level like an IT steering committee is to plan, check and supervise. Whereas at the operational level, it will be responsible with the detailed IT activities required for MEHA.

[1] Global Technology Audit Guide – Auditing IT Governance (2012)
[2] IT Governance Institute (2007)
[3] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

These three levels will facilitate the creation of the IT Governance Charter of the IT Department at the Ministry.

Without a well-established and reputable IT governance framework, there is a high risk of absence of directions for new technology and innovations to support the MEHA business in a reengineering process when acquired or to be developed.

MEHA stated that currently, the MEHA Strategic Plan 2019-2023 provided detailed explanations which incorporates the IT Governance to some extent. The IT directions and activities are also included in the 2020-2021 Costed Operational Plan (COP). The MEHA ICT Unit has a Business Plan aligned to the COP. There is no separate document for IT Governance Framework[4].

Also, the MEHA Head of Corporate Services will establish the suitability and priority of formulating an IT Governance Framework including consultations with Government ITCS[5].

Recommendations

1. **MEHA should formulate its own IT Governance Framework to ensure that proper planning and accountability of responsibility is present to support the Ministry's strategic plan to achieve improvements in productivity, cycle times and quality plans of any new IT projects.**

2. **MEHA should also establish an IT Governance Charter to outline the decision-making rights and accountability framework for IT governance that will enable the intended culture in the use of IT within MEHA.**

7.2 Absence of Business Continuity Plan and Disaster Recovery Plan

Business Continuity Plan (BCP) is the process an organisation uses to plan and test the recovery of its business processes after a disruption. It also describes how an organisation will continue to function under adverse conditions that may arise (for example, natural or other disasters).[6]

A BCP is an enterprise-wide group of processes and instructions to ensure the continuation of business processes - incl., but not limited to IT in the event of an interruption. It provides the plans for the enterprise to recover from minor incidents to major disruptions. The plan is usually owned and managed by the business units and a disaster management or risk prevention function in the enterprise.[7]

Disaster Recovery Plan (DRP) is the process of planning and testing for recovery of IT infrastructure after a natural or other disaster. It is a subset of Business Continuity Planning. BCP applies to the organisational business functions whereas DRP to the IT resources that support the business functions.[8]

The objective of having a BCP and DRP with the associated controls is to ensure that the organization can still accomplish its mission. This will not lose the capability to process, retrieve

[4] Management response – 09/11/20
[5] Management response – 09/11/20
[6] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)
[7] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[8] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

and protect information maintained in the event of interruption or disaster leading to temporary or permanent loss of computer facilities.

Business continuity and disaster recovery remain an inherent risk to all government departments. There needs to be close alignment between the disaster recovery plans and business expectations set out in the business continuity plans. FEMIS is making use of infrastructure as a service provided by ITC and also needs to consider how these systems can be recovered in the event of hardware failures, network failures, program failures and other unforeseen circumstances.

We were not provided with a BCP and DRP by the management of FESA and FEMIS. Furthermore, this was not even provided from the organizational level. ITC stated that the IT Department of MEHA needs to develop its own BCP for its systems hosted by ITC because ITC only have its own backup and restore plan which is only applicable to the ITC data centre alone.

The absence of a well-defined BCP and DRP can be catastrophic in the event of a disaster.

MEHA stated that the Head Corporate Services will prioritize the development of BCP and DRP plans that formally document existing DRP and BCP[9].

Recommendation

The BCP and DRP should be formally documented, periodically tested and updated as necessary.

7.3 Absence of Security Information Policy

This policy establishes the requirements for protection of information assets, and may refer to other procedures or tools on how these will be protected. The policy should be available to all employees responsible for information security, including users of business systems who have a role in safeguarding information (personnel records, financial input data, etc.).[10]

Information security is fundamentally risky and confidentiality remains critical for the different levels of user access. The failure to promptly terminate system access by officers that have left the services, and for the continuous periodic user access rights review are some prevalent deficiencies identified.

We noted that the MEHA does not have an Information Security Policy but places heavy reliance on the outdated ITCS policies. Hence the responsibility for security processes and controls is often spread throughout ministries and departments as well rather than with a small group of individuals with clear accountability. This can increase the likelihood of controls failing. We have also observed that with appropriate risk management principles and accountabilities then this will be connected to IS security-related activities. An information security policy should have the following features and content:

1. Responsibilities of different set of users
2. Procedures for non – compliance and breaches
3. Acceptable use policy
4. Anti – virus policy

[9] Management response – 09/11/20
[10] IDI Handbook on IT Audit for Supreme Audit Institutions (2014)

5. Back – up and restoration policy
6. Change management policy
7. Clean disk policy
8. Data access policy
9. Database management policy
10. Data storage policy
11. Disaster recovery plan policy
12. Information classification policy
13. Log management policy
14. Password management policy
15. Security awareness and training policy
16. User access management policy
17. Bluetooth baseline requirement policy
18. Remote access policy
19. Router and switch security policy
20. Wireless communication standard and
21. Wireless communication policy.

ITCS stressed that its information security policy only reflects the data centre and is confidential based on the FEMIS standard for IT processes and documents that deals with information security but will need to be modified to make it suitable for other Govnet environment, reviewed by ITC Policy Review Committee, vetted by SG's Office and approved by ITC Steering Committee which takes about 2-3 months for the finalization process before this is rolled out.

A lot of information security risks may arise from the absence of proper structures, processes and policies, such as the misappropriation of assets, unauthorised disclosure of information, unauthorised access, and vulnerability to logical and physical attacks, disruption and information unavailability, misuse of information, noncompliance with personal data laws and regulations, and failure to recover from disasters.The failure to develop and formally document information security procedures and processes relating to FEMIS increases the risk of data manipulation and information leakage.

MEHA stated that currently, MEHA has a FEMIS Policy and uses the overarching policies of Government ITCS on IT Security and its Head of Corporate Services will need to prioritize development of a separate IT Security policy[11].

Recommendation

The IT Security Policy should be documented, and periodically updated at all levels of access and sharing as necessary to safeguard the FEMIS data used as information for decision making purposes.

[11] Management response – 09/11/20

7.4 Service Level Agreement (SLA) or Memorandum of Understanding (MOU) with ITC

An internal service level agreement is between the IT organization and the business owners. Failure to adhere to service level agreements affects meeting of users' requirements. The IS operations and business owners should agree on capacity management, IT financial management and availability management.[12]

An SLA or MOU is a contractually binding agreement between a client and external service provider, or an internal service agreement between two business units within a ministry or department. SLAs are used to define service standards, and identify and correct service-level issues to mitigate their impact on operations. There's no existing SLA or MOU between the MEHA IT Department and the Department of ITCS.

Hence, the SLA or MOU should clearly specify the following requirements with:

- Detailed service description which will be provided by ITCS as expected or requested by MEHA.
- Responsibilities for each party involved.
- Applicable service hours.
- Extent of service to be provided within the service window and outside the service window.
- Reliability of expected services.
- Contact points and escalation - communication channel.
- System performance reports.
- System security.
- Costs involved (if any).

Our audit noted that ITCS is providing the IT Infrastructure as a service to MEHA, however there is no formal agreement between the MEHA IT Department and the Department of ITCS is hosting the FMIS server at their Data Centre and also providing network related services. There is no SLA or MOU between MEHA and ITCS. Business operations can be affected and process not executed on a timely basis as issues might take long to be resolved due to unclear/ no understanding of specific responsibilities of each party.

The services which are provided by the hosting party can result in unreliable services (not meeting expectations of services required), absence of system performance monitoring and reporting, can incur costs but can be controlled with an SLA or MOU to provide a secure system of operations and periodic reviews to deliberate on possible risks and threats.

MEHA stated that a SLA is ideal and the MEHA IT Department will liaise with ITCS to draw up an SLA. However, one of the disadvantages of SLA's could be that sometimes it can make service worse because they let the provider take the full amount of time specified in the SLA. If the provider is allowed three days to fix something that takes five minutes, then the provider will probably take three days. Attention needs to be given to non-compliance and how will this be captured in the SLA[13]. Given that there is no_contractual relationship between MEHA and ITC except that they are both part of the same government machinery and ITCS responsibilities are mandated through the legislations, it may be difficult to put in place an SLA.

[12] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)

[13] Management response – 09/11/20

Recommendation

MEHA in consultation with ITCS should consider having a SLA or MOU on the type of services that would be provided by ITCS and what would be MEHA's responsibilities.

7.5 Risk Management Plan

The risk management plan is embedded in the responsibilities of the organization's management and IT regularly assess and report IT related risks and organizational impact[14]. Risk management guidelines provides principles, a framework and a process of managing risk to be used by any organization regardless of its size, activity or sector[15].

Our audit of the FEMIS noted that there's no risk management framework available at MEHA to facilitate the design and development of its risk management plan in order to identify and document the risk with control measures that will mitigate the risks identified or to be kept at a minimum.

MEHA needs to design a risk management plan that covers both the internal and external risks. External risks are specifically mentioned as ITCS provide infrastructure as a service and external threats such as hacking and malware attacks in this way is ignored on the assumption that ITCS will take care of these risks. These external risks can lead to financial claims such as legal issues since the privacy of student information can be jeopardized. This is also one of the reasons why IT risks management plan is a priority for any organization.

The Ministry should have its risk management plan and policy that is assigned with sufficient resources to identify and manage risks before the IT Department can draw its business unit's operational risks from this plan to be identified with its mitigated controls populated for its risk library appetite.

MEHA stated that different Sections/Units within MEHA understand the common risks and have risk mitigation strategies incorporated in their Business Plan/ Work Plan. Setting up of a Risk Unit is ideal, however, due to budget constraints this is not feasible in the current financial year. This could be considered by the HR Section of MEHA in the future[16].

The FEMIS servers are protected through firewall at the ITCS Data Center. Currently, the MEHA IT Department does not have the budget and resources to establish a Tier 3 ISO compliant data centre needed to host the FEMIS servers at our premises[17].

One of the tasks in the MEHA Strategic Plan 2019-2023 is project design for ISO27005, Risk Management Standard and guidelines for information security risk assessment and treatment.

Recommendation

MEHA should plan on preparing its risk management plan based on an internationally recognized framework that provides the principles and guidelines on managing risks.

[14] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[15] ISO 31000 Risk Management Guideline
[16] Management response – 09/11/20
[17] Management response – 09/11/20

7.6 Physical Security

Physical security is primarily concerned with restricting physical access by unauthorised people to controlled facilities, although there are other considerations and situations on which physical security measures are valuable[18].

We noted that the MEHA does not have proper physical security access controls at the IT Department Office at the Level 1 of Senikau House points of entry. This creates the risk of unauthorised personnel entering the Office and gaining access to the IT Department work environment without proper physical access controls in place.

MEHA stressed that the building floor including the MEHA IT Department room is planned for renovation. The plan already includes improved physical access security at the level and a more secured ICT room and a tender regarding this has been called.[19]

Recommendation

MEHA should implement appropriate physical/environment access security controls to restrict access to the Senikau House IT Department room building.

7.7 Use of unsecured Internet Protocol (http)

The hypertext transfer protocol (http) is a communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client browser[20]. Http offers displaced connection for the users and it can result in packet loss[21] and the data that are lost or dropped in transit during travel across a computer network cannot be recovered.

In computer security, a demilitarized zone (DMZ) or is a perimeter network on which a network area (a subnetwork) that sits between an internal network and an external network. For instance, the FEMIS systems accessed by approved users can be made from any internet services provider that is accessing through the ITCS government network domain.

As there are so many different possible types of unauthorized access attacks that can take place when considering internal and external attackers, it is not possible to give procedures for handling them, but rather a series of options which are not limited to accessing unsecured networks[22].

We noted that the MEHA makes use of the internet access for collection of personal information for students, teachers and schools for FEMIS. However, use of unsecured internet protocol for communication connection can result in loss of data and is also vulnerable to hackers. Such form of information and communication exchange does not offer reliable exchange of information as the information that flows from one point to another is not encrypted through a DMZ because the data can be interfered.

[18] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)

[19] Management response – 09/11/20

[20] Government Accountability Office Federal Information System Controls Audit Manual (FISCAM)

[21] Accessing the internet where small units of data called packets are sent and received but fails to reach intended destination.

[22] Safeguarding your Technology – Protecting your System: User Access Security

Therefore, the packet loss identified was due to an inefficiency of a component that carries data across a network could have resulted from outdated router, a loose cable connection or a bad Wi-Fi signal.

MEHA stated that the procurement of SSL Certificates is included in MEHA's Operational Plan and the MEHA IT Department is currently liaising with the Government ITCS regarding recommendations for the SSL Certificates. Even the MEHA IT Department Job number 103 includes encrypting passwords with a priority of "Work to start as soon as immediate priorities are cleared".[23]

Recommendations

1. **MEHA should implement cryptography and encryption techniques to secure the data so that it can only be decrypted with a special algorithm.**

2. **MEHA should also advocate that using an unsecured network would be permissible if the connection requires some sort of login or registration and restrict using of sensitive data on unsecured public networks.**

7.8 Physical Location of Test and Live Environment

It may require the use of manual or automated processes for the business to function with limited capacity and the DRP typically concerns itself with ensuring that the IT infrastructure is robust enough to recover from a disaster. The planning is also aligned with the BCP to ensure that the mission critical processes that are in the BCP and which are supported by IT systems are also considered critical by the IT department[24].

We noted that the physical location for the test and live environment is located at the Government ITCS Department and that the test environment is used as the backup storage in the same physical environment. To ensure business continuity and to minimize the loss due to unforeseen circumstances then a backup with disaster recovery is to have a DR site and use of remote storage to minimize the impact.

Loss of hardware and data due to business disruptions that can be caused by fire, and/or other natural disasters could very critical because both the environments are physically located at the same location.

MEHA stated that the Government ITCS has informed MEHA that ITCS is backing up FEMIS/FESA. Their backups are stored at a different location. MEHA IT Department will work towards the BCP and DRP in consultation with the relevant stakeholders[25].

At present MEHA maintains fully redundant servers of identical hardware specification configured identically to production hardware to operate as production servers in the event of production hardware failure. Additionally, the redundant server's function as the MEHA training environment

[23] Management response – 09/11/20
[24] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[25] Management response – 09/11/20

to ensure all software, databases, firewall and connectivity are fully operational at all times, allowing fast failover as required[26].

Recommendation

MEHA should seriously consider developing and implementing its BCP and DRP without delay so that the plan is tested in order to identify mitigating factors during unforeseen situations.

7.9 Irregular Back Ups

Solution design also includes specific backup and recovery procedures that the organisation needs to follow so that the data is backed up in a periodic basis. Recovery procedures ensure that the backed-up data is able to be recovered and that sufficient versions of backups are stored both at the local site and at a remote site[27].

Audit noted that all the backups were not regularly maintained and monitored by MEHA. In order to prevent the loss of critical data, MEHA should ensure that backups are done frequently and on a regular schedule.

The unavailability of backup data with the inability to locate media when needed or the inability to transport data within the prescribed timeframe increases the risks associated with BCP. Therefore, the risk of losing data and information during a disaster to recover places a higher risk on MEHA operations and administration of students, teachers and schools' resources.

MEHA stated that the live FEMIS data is backed up in the FEMIS Training database servers daily. A backup plan will be worked on and the Government ITCS does the off-site backups[28].

Recommendation

MEHA IT Department should develop and implement a backup policy and then comply with the policy by scheduling regular backups internally and also with off – site backups as well.

[26] Management response – 09/11/20
[27] AFROSAI – E IT AUDIT MANUAL 2017 (1st Ed.)
[28] Management response – 09/11/20

8.0 Conclusion

Based on the results of the audit procedures performed, we conclude that the MEHA IT Department can improve the general controls by revising and updating policies for the system as discussed in the audit findings that is aligned to the COBIT framework on IT governance.

One notable area that requires special attention is the use of unsecured internet protocol for http network to be addressed and the frequency of backups to be scheduled so that there is assurance of business continuity.

MEHA has acknowledged the recommendations in this report but have indicated that some of the recommendations have cost and resource implication. Currently, the MEHA business needs are driving the FEMIS development. MEHA has further stated that the recommendations are a good starting point for this and MEHA IT Department will work on the recommendations[29].

[29] Management response – 09/11/20

OFFICE of the AUDITOR GENERAL
Republic of Fiji

www.oag.gov.fj