# STANDING COMMITTEE ON PUBLIC ACCOUNTS

# Review of the Compliance Audit Report

**PARLIAMENT OF THE REPUBLIC OF FIJI**
**Parliamentary Paper No. 24 of 2022**

***April, 2021***

*Published and printed by the Department of Legislature, Parliament House, Government Buildings, Suva*

# TABLE OF CONTENT

# CHAIRPERSON'S FOREWORD

At the outset, this Committee report follows the Report of the Auditor General of the Republic of Fiji – Compliance Audit Report.

The Office of the Auditor General is established as an Independent Office by the Constitution of the Republic of Fiji. The function of the OAG is to conduct 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. In this regard, 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.

The Committee reviewed the Compliance Audit Report that comprised of the following audits:

1) Commencement of Quarry Development Projects and Appointment of Certified Foreman-in-Charge
2) Government Payroll System
3) Financial Management Information System (FMIS)
4) Fiji Education Management Information System (FEMIS)

The compliance audit that was conducted were focused on line agencies that were involved and how each entity comply with the relevant legislations, policies and procedures that were in place. In addition, the audit also identified gaps and areas that needs to be addressed and be strengthened.

The Committee commended the work done by the following Ministries/Departments in the administration and delivery of those programmes/services:

1. Department of Mineral Resources;
2. Ministry of Economy- Payroll Section;
3. Department of Information Technology and Computing Services; and
4. Ministry of Education, Heritage and Arts

Given the audit results, the Committee looks forward to these agencies to address those gaps identified and strengthened those areas that were highlighted. Most importantly, implement the relevant recommendations that are put forward to enhance the service delivery for each entity.

Overall, I thank the Executives of the relevant Ministries/Departments for provided its written responses to the audit issues that were raised and measures that are in place, and the Staff of the Office of the Auditor General for provided technical clarifications on those issues.

I also wish to extend my appreciation to all the Honourable Members of the Committee who were part of the successful compilation of this bipartisan report namely Hon. Joseph Nand (Deputy Chairperson), Hon. Ro Teimumu Kepa, Hon. Virendra Lal and Hon. Aseri Radrodro.

**Hon. Alvick Avhikrit Maharaj**
**Chairperson**

# COMMITTEE MEMBERS

Pursuant to SO 118 (1), "*A majority of the members of the standing committee shall constitute a quorum*". The substantive members of the Standing Committee on Public Accounts are:–

**Hon. Alvick Avhikrit Maharaj**
**(Chairperson MP)**

**Hon. Joseph Nitya Nand**
**(Deputy Chairperson MP)**

**Hon. Aseri Masivou Radrodro**
**(Opposition MP)**

**Hon. Ro Teimumu Kepa**
**(Opposition MP)**

**Hon. Virendra Lal**
**(Government MP)**

# INTRODUCTION

The Compliance Audit Report was tabled in Parliament on the 2nd of December 2020 and referred to the Standing Committee on Public Accounts, for its scrutiny.

Standing Order 109 (2) (d) allows Standing Committee on Public Accounts to examine the accounts of the Government of the Republic of Fiji in respect of each financial year and reports of the Auditor-General, and for any other matter relating to the expenditures of the Government of the Republic of Fiji or any related body or activity (whether directly or indirectly) that the committee sees fit to review.

Standing Order 110(1)(c) authorises the Standing Committee to *scrutinise the government departments with responsibility within the committee's subject area, including by investigating, inquiring into, and making recommendations relating to any aspect of such a department's administration, legislation or proposed legislative program, budget, rationalisation, restructuring, functioning, organisation, structure and policy formulation.*

# COMMITTEE PROCEDURE

The Novel Coronavirus Disease renamed as COVID-19 was declared by the World Health Organisation as a global pandemic on 11 March 2020. The Parliament of the Republic of Fiji therefore undertook necessary health precautionary measures to control the spread of the new virus strand outbreak.

In view of the above, Standing Order 112 (1) (b) provides powers to the Standing Committee on Public Accounts to compel the production of documents or other materials or information as required for its proceedings and deliberations. In this regard, the Committee conducted its review through the Virtual platform MS Teams.

During the review, the Committee resolved that the following entities identified in the audit report shall provide a substantive written submissions to the Committee:

1. Department of Mineral Resources (Ministry of Lands and Mineral Resources);
2. Ministry of Economy – Payroll Section;
3. Department of Information Technology and Computing Services; and
4. Ministry of Education, Heritage and Arts

# BACKGROUND

The Audit was conducted in accordance with the functions of the Auditor General specified in the Audit Act 1968 and Section 152 of the 2013 Constitution of the Republic of Fiji. Section 6A of the Audit Act 1969 provided powers to the Auditor General to conduct Compliance Audits.

The main objective of this audit is to determine whether an entity is achieving its objectives in compliance with relevant legislations.

The Audit covered the laws where the Department of Mineral Resources derives its powers to issue approvals of Quarry Development and the ambiguity it may have stipulated in the applicable laws. It also covers the process and lack of proper documentation when appointing qualified foreman or Quarryman to oversee quarry development projects. Further the audit focuses on the application of proper controls in the Payroll System of the Ministry of Education Payroll Section, and in its Financial Management Information System (FEMIS), and an IT audit on the IT governance structure and IT Operations that should deliver and meet the IT needs and requirements of the Ministry of Education, Heritage and Arts.

Further the sub-objectives of the audit are as follows:

1. The 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.
2. The obtaining of 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.
3. The Assessment on 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;
4. 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. The 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
6. The IT Operations Application controls in terms of the input controls, processing controls and output controls.

# GENERAL RECOMMENDATIONS

The Committee after reviewing the audit report and the responses from relevant entities in relation to the audit issues that were raised, it recommends that:

***The relevant Ministries and Departments to take note of the Committee recommendations on each Audit Topic and implement those recommendations that are yet to be fully implemented.***

# COMMITTEE FINDINGS

## PART 1: COMMENCEMENT OF QUARRY DEVELOPMENT PROJECTS & APPOINTMENT OF CERTIFIED FOREMAN-IN-CHARGE

## Approval of Commencement of Quarry Development Projects

### 1. Commencement of quarry operations without the approval of the DMR

According to the Audit report 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.

**Governance issues**

The Audit analysis of data provided, noted the following:

- Department of Environment had approved 25 EIA reports for quarry developments during the years 2014 to 20201 of which only 6 (24 per cent) 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.
- i-Taukei Lands Trust Board issued 12 leases for industrial quarries of which only 5 (42 per cent) matched the DMR's approved listing.

The above data are obtained listings of approved quarries according to records maintained by the four agencies.

**Root Cause/Implication**

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

The audit report indicated that the Manager Mines had 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.

**Response from the Entity:**

The audit recorded the Permanent Secretary Lands and Mineral Resources (PSLMR) explaining in a meeting 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.

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.

**Auditors 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.

**PAC Committee Comments/Recommendation:**

- ***The Committee notes the Ministry's comments and concurs with the OAG recommendation;***
- ***For uniformity and consistency purposes, the DMR processes and criteria needs to be communicated to other relevant agencies such as ITLTB, Department of Lands and Department of Environment;***
- ***The Department of Lands and ITLTB should strictly adhere to the Department of Mineral Resources requirements on the issuance of quarry permits; and***
- ***For those entities that are operating without proper approvals, the Ministry should ensure strict compliance.***

**2. Meeting the mandatory requirements for approval of quarry operations**

According to the Audit, the DMR through the Director Mines have used Section 2A of the Quarries Regulations 1939 to exercise its power to issue approval letters for commencement of quarry operations as captured in its Standard Operating Procedures (SOP).

According to the above process, documents required to be submitted with any application for quarry developments as legislatively mandated, 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 file.

**Other Significant Matters –**

**Governance issues**

The audit report showed project files for twenty (20) approved quarry development projects were reviewed to determine whether all mandatory requirements were met before the DMR issued approval letters for commencement of operations. From the Auditors review, it was noted that:

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

**Root Cause/Implication**

The above findings indicated that 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.

**Response from the Entity:**

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.

**Auditors 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.

**PAC Committee Comments/Recommendation**

- ***The Committee agrees with the Audit recommendations.***
- ***DMR should ensure that all relevant documents required from entities are sought and securely filed in an electronic environment.***

### 3. Notification on commencement of quarry operations

The Audit report noted that 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. 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.

**Other Significant Matters –**

**Governance issues**

The audit reviewed the twenty (20) quarry project files and noted that only one (1) file contained the two week's notification to the Inspector of Mines prior to the commencement of its operations.

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.

**Root Cause/Implication**

The audit report revealed that monitoring by the Department may need to be strengthened to ensure compliance to the regulations governing quarry operations. The audit report 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.

**Response from the Entity**: According to the Audit, DMR 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.

The Inspectorate Unit conducts quarry inspections in all the three divisions (Central/Eastern, 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.

**Auditors 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.

**PAC Committee Comments/Recommendation**

***The Committee concurs with the Audit recommendations.***

# Appointment of Certified Foreman/Quarryman in Charge

## 1. Certification of foreman/quarryman in charge of quarry development projects

According to the Audit Report, 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.

### Other Significant Matters –

### Governance issues

The Audit review of records relating to the foreman in charge/quarryman for the twenty (20) quarry development projects indicated that there were 19 identified foreman in charge.

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.

### Root Cause/Implication

The findings indicated 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.

**Response from the Entity** 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.

### Auditors 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.

### PAC Committee Comments/Recommendation

***The Committee concurs with the Audit recommendations.***

## 2. Proper notification of appointment, commencement and changes of Quarry/Foreman in Charge

The Audit Report noted that, 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.

### Other Significant Matters –

### Governance issues

The Audit revealed that 18 of the 19 quarryman filed records did not have the 14-day notification of the appointment of the quarryman by the quarry company.

### Root Cause/Implication

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.

**Response from the Entity:** 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.

### Auditors 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.

### PAC Committee Comments/Recommendation

***The Committee agrees with the Audit recommendations.***

## 3. Mandatory requirements prior to issuing quarryman certificates

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

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)

- Application to be accompanied by a fee of $33.
- Applicant has attained the age of 21 years.
- Applicant has had no less than 2 years practical experience in quarrying.
- 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.
- Applicant is proficient in rendering first aid to injured persons.
- Applicant successfully passes written or oral examination.
- 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.

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

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

**Other Significant Matters –**

**Governance issues**

The audit reviewed and analysed 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

**Root Cause/Implication:**

The audit noted that the above anomalies are a result of poor records management of quarryman information. The OAG 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.

**Response from the Entity:** DMR has agreed to the audit findings and recommendations and will be taking necessary remedial actions. 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.

**Auditors 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.

**PAC Committee Comments/Recommendation:**

***The Committee concurs with the Audit recommendations.***

# PART 2: GOVERNMENT PAYROLL SYSTEM

## 1. Security Risk Management of Shared Payroll Data not adequate

According to the Audit Report, 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. The policy establishes the requirements for protection of information assets, and may refer to other procedures or tools on how these will be protected.

The audit suggests that 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.

### Other Significant Matters –

### Governance issues:

The Audit noted that the bank listing, which is not encrypted, is sent to respective banks by the MOE (Ministry of Economy) Payroll Section through email.

The Audit also added, 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.

### Root Cause/Implication:

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.

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

**Response from the Entity:** In the Audit report the Ministry of Economy 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. 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.

### Auditors 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.

**PAC Committee Comments/Recommendation**

***The Committee notes the issues raised in the Audit Report and agrees with the response of the Ministry of Economy in dealing with these issues.***

## 2. Change Management Control not held

According to the Audit Report 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.

**Other Significant Matters –**

**Governance issues**

The Audit reported that they 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.

**Root Cause/Implications:**

The audit report noted that 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 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.

**Response from the Entity:** 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.

The payroll team at MOE also provide assistance and guidance to individual Ministries/Departments on issues on daily basis as well. 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.

**Auditors 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.

**PAC Committee Comments/Recommendation**

***That the Committee endorses the implementation of the Change Management Control over the Payroll system and ensure that proper documentation is maintained to support any system upgrade.***

### 3. System Documentation and Policy Reviews not held

The Audit Report noted that documentation of IS, applications, job roles, reporting systems and periodicity is an important reference point to align IT operations with business objectives.

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

**Other Significant Matters –**

**Governance issues:**

The Audit reported that the Payroll Section did not have:

1. a proper payroll system documentation audit trail for any system amendments without any policy reviews, and
2. 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.

The Audit report 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. The Audit further reported 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.

The Audit further stated, that 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.

**Root Cause/Implications:**

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 Audit report further concluded that lack of documentation can lead to communication gaps where poor and incorrect decisions can be made.

**Response from Entity:** The Ministry mentioned in the audit report that it is currently undergoing review of financial regulations and all the changes in the payroll system/process will be captured accordingly. The Audit report stated that 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.

**Audit Report 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.

**PAC Committee Comments/Recommendation:**

***The Committee concurs with the Audit recommendations.***

## 4. Data Accuracy and Completeness

The Audit Report noted that Information System(IS) audit and assurance professionals must obtain sufficient and appropriate evidence to draw conclusions on which to base the engagement results 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.

According to Audit Report, 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.

**Other Significant Matters –**

**Governance Issues:**

The Audit reported 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 Audit Report indicated that the salaries team received completed and signed input forms from respective ministries and departments which the payroll team processes. 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.

The data used by the Auditors and depicted in the Audit Report showed analysis that was drawn from the established staff payroll data and RFMF payroll data sets.

| 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 |

| Established Payroll Test | ACL Results | RFMF Payroll Test | ACL Results |
|---|---|---|---|
| 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 by the audit report included missing employee date of birth records, record of employment starting dates and contract end dates. The audit reported existence of duplicate bank accounts and FNPF numbers, employees reaching the compulsory retirement age and incomplete FNPF numbers recorded.

**Root Cause/Implications:**

The audit 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 audit report noted that non – review of payroll data prior to its input exposes government to the risk of incorrect classification, incorrect payment of salaries and fraud.

**Response from Entity**: The Ministry's responded stating 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.

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

**Audit 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 that is embedded in the payroll system for field formats (data entry) to either accept complete employee profile or reject incomplete data entry details.

**PAC Committee Comments/Recommendation:**

***The Committee notes with concern the accuracy of the RFMF salary processing and request that future audit report to provide an update on the progress of works undertaken by the Ministry.***

## 5. Command Line Interface (CLI)

The audit report highlighted that 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 and other documentation.

Further stating the audit report 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.

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.

### Other Significant Matters –

### Governance Issues:

The compliance audit noted the following issues which can assist in further improving the current system:

1. Graphical user interface (GUI) to be developed and used instead of CLI;
2. II. Information displayed on the panel view is not clear to end – users;
3. 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;
4. Very little familiarity of the user interface to allow users to navigate through the program easily;
5. Design lacks consistency which is not very efficient and appealing to eyes of users; and
6. Design was not responsive.

### Root Cause/Implications:

The audit report noted that 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 design of an improper UI can result in the untimely provision of first – hand information to users when needed.

### Response from Entity:

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. 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.

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.

**Auditors 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.

**PAC Committee Comments/Recommendation:**

***The Committee recommends that relevant ongoing training be undertaken to existing staff and new staff so that they are well versed with the operation of the ITCS Payroll System.***

# PART 3: FINANCIAL MANAGEMENT INFORMATION SYSTEM

## 1. Absence of Business Continuity Plan and Disaster Recovery Plan

Firstly the Audit report explains that A Business Continuity Plan (BSP) is an enterprise wide group of processes and instructions to ensure the continuation of business processes – including, 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.

Further it discusses a Disaster Recovery Plan (DRP) as 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.

The Compliance Audit highlighted that 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.

### Other Significant Matters –

### Governance Issues:

The Compliance Audit was of the view that the Business continuity and disaster recovery remained an inherent risk to all government departments. It noted that 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.

### Root Cause/Implications:

The Audit report noted that it was not provided with a BCP and DRP by the management of FMIS during the audit. The plans were also not provided at the organizational level after enquiring with the Policy Division with MOE. The Audit added to its findings that the absence of a well-defined BCP and DRP can be catastrophic in the event of a disaster or unplanned calamities.

### Response from Entity:

The Acting Manager ITCS advised the auditors that FMIS team needs to 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. 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.

**Auditors Recommendation**

The Business Continuity Plan and Disaster Recovery Plan should be formally documented, periodically tested and updated as necessary by FMIS.

**PAC Committee Comments/Recommendation:**

***The Committee notes the Ministry's comments on the development of the BCP Document and the Risk Management Framework.***

### 2. Service Level Agreement (SLA) or Memorandum of Understanding (MOU) with ITCS

The Audit highlighted quoting from the IDI Handbook on IT Audit for Supreme Audit Institutions (2014) on SLA documenting 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.

According to the Audit, the Afrosai- E IT Audit Manual 2017 (1st Ed) stated that 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.

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

1. Detailed service description which will be provided by ITCS as expected or requested by MOE;
2. Responsibilities for each party involved;
3. Applicable service hours;
4. Extent of service to be provided within the service window and outside the service window;
5. Reliability of expected services;
6. Contact points and escalation - communication channel;
7. System performance reports;
8. System security; and
9. Costs involved (if any).

**Other Significant Matters –**

**Governance Issues:**

The 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.

The audit also highlighted that 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.

**Root Causes/Implications:**

The Audit discussed that 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.

**Response from Entity:** The MOE response on the Audit findings was 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.

**Auditors 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.

**PAC Committee Comments/Recommendation:**

***The Committee notes the comments from the Ministry and recommends that future MOU be vetted by the Office of the Solicitor General.***

### 3. IT Strategic Plan

The Audit shared that The IT strategy relates to the long-term direction an organisation wants to take in leveraging IT for improving business processes. 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.

**Other Significant Matters –**

**Governance Issues:**

The Audit highlighted that 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.

The Audit also stated that the IT Strategic Plan will be helpful in planning and acquisition of resources (staff, equipment, finance, etc.) and assist in the Ministry budgeting process. The audit stated that they were advised by ITCS 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 was not available for distribution to other ministries and departments.

**Root Causes/Implications:**

The Audit further stated that in the 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.

**Response from Entity**: The Audit reported that MOE had 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 Administration Costed Operation Plan (COP) entails the work plan that the Office Services/Information Technology Division which will undertake in the new fiscal year.

**Audit 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.

**PAC Committee Comments/Recommendation:**

***The Committee notes the comments from the Ministry and recommends that it further discusses with the OAG on the need to have a separate IT Strategic Plan.***

## 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.

**Other Significant Matters –**

**Governance Issues:**

The Audit report showed that FMIS has 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.

The Audit noted 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. However the Audit noted that 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.

According to the Audit report, 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.

**Root Causes/Implications:**

Therefore, the ITCS planned risk policy and procedures is only applicable to the data centre 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.

The Audit concluded that 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.

**Response from Entity**: The Audit recorded MOE stating 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.

**Audit 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.

**PAC Committee Comments/ Recommendation:**

***The Committee notes the comments from the Ministry.***

### 5. Change Management Plan

According to the Audit, change management plan process are normally used to manage and control changes to software, hardware and related documentation. Organisations follow a defined change management procedure which requires approval from a board before being implemented into the operational environment.

The Audit further added the change management plan will minimize the impact a change can have on the business, employees, customers, and other important stakeholders.

The Audit explained that 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.

**Other Significant Matters –**

**Governance Issues:**

The audit also 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.

Comment from ITCS stated that its change management plan only reflects the data centre 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.

**Root Cause/Implications:**

The Audit report observed that 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.

**Response from Entity:** MOE have stated in the Audit report 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.

**Audits 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.

**PAC Committee Comments/Recommendation:**

***The Committee notes the comments from the Ministry.***

### 6. Absence of Information Security Policy

According to the Audit 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 Audit reported that 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.).

The Audit recorded that 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 service, 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.

**Other Significant Matters –**

**Governance Issues:**

The audit further 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. Therefore accordingly 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.

The Audit noted that 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
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, in the Audit Report 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 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.

**Root Causes/Implications:**

High information security risks according to the Audit report 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 Audit further suggests that absence of formally documented information security procedures and processes relating to FMIS can increase the risk of data manipulation and information leakage. Accordingly the audit report recorded The FMIS Section stating 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.

**Audits 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

**PAC Committee Comments/Recommendation:**

***The Committee notes the comments from the Ministry and recommends that ongoing training be undertaken to Staff for better understanding of IT Security policy.***

## 7 Incident Response Policy

The Audit Report defined Incident response management as 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.

**Other Significant Matters –**

**Governance Issues:**

The 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, 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 the audit noted that 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).

The Audit noted ITCS emphasizing that its incidence response policy only reflects the data centre 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.

**Root Causes/Implications:**

Without a proper incident management process, according to the audit report, 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.

**Response from Entity:** The audit report noted MOE stating 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.

**Audit 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.

**PAC Committee Comments/Response:**

***The Committee notes the comments from the Ministry.***

## 8 Access Control Management

According to the audit report, 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. The FMIS Section will be monitoring all user access on a quarterly basis.

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

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

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

According to audit report, the objective of logical access controls is to protect the financial applications and underlying data files from unauthorized access, amendment or deletion, have adequate 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.

## Other Significant Matters –

### Governance Issues:

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.

### Authorised PO Approvers

| PO Module Panel | Work Unit Set ID |
|---|---|
| PO 401 | WPO 07 |
| PO 348 | WPO 06 |
| PO 481 | WPO 15 |
| PO 621 | WPO 05 |

*Source: PO modules provided by FMIS*

Furthermore, the audit 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.

### Root Cause/Implications:

Our audit also noted that some current and former Permanent Secretaries have access to more than one “org in FMIS”. It was noted that review of users as prescribed in the FMIS Access and Password Policy, that requirements are not carried out which increases the risk of unauthorized access and manipulation of data input that can go undetected.

**Response from Entity**: 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.

### Auditors 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.

**PAC Committee Comments/Recommendation:**

***The Committee notes the comments from the Ministry.***

# PART 4: FIJI EDUCATION MANAGEMENT INFORMATION SYSTEM

## 1. IT Governance Framework for MEHA

The audit stated that 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.

**Other Significant Matters –**

**Governance Issues:**

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.

According to the audit the IT governance of IT operations in the public sector is provided in the Reform of the Department of ITCS Act 2016. The Act entails the procurement of ICT goods, services and works of ITCS and Government Ministries and Departments, however each agency is still responsible for the implementation of ITCS policies, reviewing its structure, size and composition.

The audit states that Ministries are still accountable and responsible for its software, systems, and hardware for the IT initiatives or IT strategic procurement which are 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.

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

**Root cause/ Implications:**

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.

**Response from Entity**: 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.

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

**Audits 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.

**PAC Committee Comments/Recommendation:**

- ***The Committee endorses the OAG recommendations.***
- ***The Ministry of Education to provide an update on the IT Governance Framework.***

## 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).

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.

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

**Other Significant Matters –**

**Governance issues:**

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.

**Root Cause /Implications:**

The Auditors were not provided with a BCP and DRP by the management of FESA and FEMIS. The audit report stated that it was not even provided from the organizational level. The absence of a well-defined BCP and DRP can be catastrophic in the event of a disaster.

**Response from Entity:** 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.

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

**Auditors Recommendation**

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

**PAC Committee Comments/Recommendation:**

- ***The Committee endorses the OAG recommendations.***
- ***The Ministry of Education to provide an update on the BCP and DRP.***

### 3 Absence of Security Information Policy

According to the audit report 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 is 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.).

**Other Significant Matters –**

**Governance issues:**

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. The Audit report 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
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.

**Root Cause/Implications:**

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.

**Response from Entity:** 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.

**Auditors 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.

**PAC Committee Comments/Recommendation:**

- ***The Committee endorses the OAG recommendation.***
- ***The Ministry of Education to provide an update on the Security Information Policy.***

### 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.

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.

**Other Significant Matters –**

**Governance issue:**

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 FEMIS server at their Data Centre and also providing network related services. There is no SLA or MOU between MEHA and ITCS.

**Root Cause/Implications:**

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.

**Response from Entity:** 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. 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.

**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.

**PAC Committee Comments/Recommendation:**

- ***The Committee endorses the OAG recommendation.***
- ***The Ministry of Education to provide an update on the SLA/MOU.***
- ***The Solicitor General's Office should vet the final version of the SLA/MOU before being sign by the two Departments***

## 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. 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.

**Other Significant Matters –**

**Governance Issues:**

The 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.

**Root Cause/ Implications:**

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.

The FEMIS servers are protected through firewall at the ITCS Data Centre. 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.

**Response from Entity:** 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 future16.

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.

**PAC Committee Comments/Recommendation:**

- The Committee endorses the OAG recommendation.
- The Ministry of Education to provide an update on the status of the Risk Management Plan.

## 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.

**Other Significant Matters –**

**Governance Issues:**

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.

**Root Cause/Implications:**

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.

**Response from Entity:** 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.

**Recommendation**

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

**PAC Committee Comments/Recommendation:**

- ***The Committee endorses the OAG recommendation.***
- ***The Ministry of Education to provide an update on the status of the Physical Security upgrade.***

## 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. Http offers displaced connection for the users and it can result in packet loss 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 sub network) 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.

**Other Significant Matters –**

**Governance Issues:**

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.

The Audit report 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.

**Root Cause/Implications:**

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.

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.

**Response from Entity:** 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".

**Auditors 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.

**PAC Committee Comments/Recommendation:**

- **The Committee endorses the OAG recommendations.**
- **The Ministry of Education to provide an update on the procurement of SSL Certificates.**

## 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.

**Other Significant Matters –**

**Governance issues:**

The Audit report 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.

**Root Cause/Implications:**

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.

**Response from Entity:** 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.

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

**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.

**PAC Committee Comments/Recommendation:**

***The Committee noted the Ministry's comments and concurs with the OAG recommendation.***

### 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.

**Governance issues:**

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.

**Root Cause/ Implications:**

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.

**Response from Entity**: 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.

**Audit 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.

**PAC Committee Comments/Recommendation:**

- ***The Committee endorses the OAG recommendations.***
- ***The Ministry of Education to provide an update on the status of the Backup processes and policies.***

# SUSTAINABLE DEVELOPMENT GOALS

The Committee continues to discuss and deliberate with interviewees from Ministries/Departments on their commitments, implementation and monitoring of the SDGs.

## GENDER ANALYSIS

The Committee noted the importance of Gender Equality while scrutinising the Auditor General’s Reports and continues to discuss and deliberate during interview sessions with Ministries and Departments.

# CONCLUSION

The Public Accounts Committee reviewed the Compliance audit report on the commencement of quarry development projects, appointment of certified foreman-in-charge, the Government Payroll System, Financial Management Information System and the Fiji Education Management Information system.

The Committee agrees with the recommendation outlined in the Audit Reports by the Office of the Auditor General and that these recommendations are the starting points for improvements and strengthening of relevant policies and procedures as discussed in the reports.

**We, the undersigned Members of the Standing Committee on Public Accounts agree with the contents of this report:**

……………………………

**Hon. Alvick Maharaj**
**(Chairperson MP)**

………………………..

**Hon. Joseph Nand**
**(Deputy Chairperson MP)**

…………………………

**Hon. Virendra Lal**
**(PAC Member/MP)**

…………………………………

**Hon. Ro Teimumu Kepa**
**(PAC Member/MP)**

……………………………

**Hon. Aseri Masivou Radrodro**
**(PAC Member/MP)**

# APPENDICES

# APPENDIX 1

# PUBLISHED WRITTEN EVIDENCE

The written evidences including supplementary evidences that are covered in this review report can be accessed on the Parliament Website using the following link: http://www.parliament.gov.fj/committees/standing-committee-on-public-accounts/