SCHEME OF SERVICE

Organisation: Financial Intelligence Unit

Post: Analyst (Operations)

Salary: Rs 47950 x 1050 - 49000 x 1100 - 54500 x 1450 - 58850 x 1750 - 62350 x 1850 - 67900 x 1900 - 75500 x 2250 - 86750 x 2500 - 94250 x 2750 - 97000 (FIU 9) PRB 2026

Qualifications:

A. By selection from officers who are on permanent and pensionable establishment for at least three years at the Financial Intelligence Unit and who possess a degree in Economics or Law or Finance or Computer Science from a recognised institution or an equivalent qualification to the Financial Intelligence Unit;

Note

In the absence of qualified serving officers at A above, by selection from among candidates who possess a degree in Economics or Law or Finance or Computer Science from a recognized institution or an equivalent qualification acceptable to the Financial Intelligence Unit;

B. Candidates should:

a) reckon at least three years' experience in the relevant field;

b) have good analytical and communication skills;

c) be able to establish priorities and paying attention to details and data accuracy;

d) be computer literate; and

e) have the ability to work under pressure and meet deadlines.

Role and Responsibilities: To support the different divisions of the Financial Intelligence Unit in view of attaining the objectives of the Financial Intelligence and Anti-Money Laundering Act.

Duties:

To perform any of the following duties:

Financial Investigative Analysis Division:

1. to investigate reports on suspicious transactions and carry out related research analysis in view of adding value to information received and held by the FIU.
2. to gather and document facts and findings coherently and comprehensively for dissemination reports.
3. to produce analytical charts including those obtainable from appropriate analytical software.

4. to conduct operational analysis and identify conspiratorial activities, to establish relationship and linkages between people, organization, events and effectively present the findings, to track down consignment and exportation of jurisdictional issues in the investigation of suspicious money laundering activities.
5. to apply knowledge of AML/CFT legal framework in FIU's analysis and dissemination works.
6. To collect, collate and input relevant statistics in a structured manner.
7. To support strategic analysis work of the FIU.
8. To assist in the collection, evaluation and grading of information to be captured from open/commercial sources for purpose of research and analysis.
9. To prepare brief/reports on works of international organisations involved in AML/CFT, namely FATF, Egmont Group, FSRBs, UNODC and other related bodies.
10. To design and carry out regular surveys for FIU.
11. To assist in the preparation of FIU's publications and contribute to knowledge management at the FIU.
12. To assist in quantitative research on the impact of money laundering in Mauritius and update on a regular basis.
13. To assist in the editorial works for the organisation's website contents, reports and other communications of the FIU.
14. To undertake computer and other research work, as required by the FIU, including checks, computerised or otherwise, of private, internal and government databases; perform evaluation and assessment thereof; and prepare concise reports of findings from any research done, checks performed and intelligence gathered.
15. To mentor Intelligence Officers and fill the gap and conducting specific assignments when required.

System Administration Unit:

1. To conduct full lifecycle administrative management of all servers, operating systems, and peripheral devices, including development, test, production and failover servers and equipment.
2. To act as liaison for software providers as assigned for the purpose of resolving problems with software in use at the FIU.
3. To monitor the physical storage and bandwidth requirements to ensure optimal performance of applications, data storage and reliability.
4. To oversee initiation, verification, and maintenance of backups.
5. To create and present technical designs, architectures and strategies for a relevant operating system environment at the FIU.
6. To manage the wiring, installation and programming related to various data processing and peripheral equipment.

7. To be responsible for the administration of systems software and hardware, installing new operating environments and implementation of new operating system patches, upgrades and releases, and identifying integration issues with developers or vendors.
8. To assist in the monitoring of projects of the FIU by carrying out proper research and determining significant features, advantages of various database systems.
9. To write, prepare and review bid specifications of IT equipment for purchases, and to review hardware/software systems, cable installations and other recommendations based upon specifications.
10. To be involved in all phases/steps of the System Development Life Cycle.
11. To maintain proper register and record all movements of IT equipment.
12. To be responsible for keeping data of the FIU secured through managing access, privileges and information migration and seeking approval / informing the Director.
13. To deal with enquiries for various sources (staff, outside vendors, service providers) for the purpose of providing technical assistance, advice and support.
14. To carry out incident analysis tracking, recording and response.

Security Unit:

1. To make regular risk assessment of the information base and physical security of the organisation.
2. To make necessary recommendations regarding Incident Reporting and Response Procedures to address FIU's security breaches such as policy violations, as well as complaints, privacy and copyright infringements as and when required.
3. To recommend controls on value, threat, vulnerability and cost of FIU's information system and provide periodic reporting to Director.
4. To conduct periodic vulnerability assessment of the assets of FIU, analyze the logs of the various systems for initiating preventive measures and check new virus threats and generate reports.
5. To establish and maintain a system that fosters appropriate, demonstrable and coordinated security policies, procedures and practices that are compliant with related laws, regulations, policies, security and professional standards. This includes ensuring the existence in the organisation for user management - User ID, conduct review / audit to assess that the access privileges are on a need-to-know basis.
6. Evaluate and recommend new information on security technologies and counter measures against threats to information / piracy.
7. To ensure security of the system both from inside and outside, and to be responsible for solving all phases of information system security and related technical problems.

8. To ensure that processes exist in the organization for user management – User-ID, conduct review to assess that the access privileges are on the basis of need to know.

9. To maintain hardware and software installation, performance tuning, troubleshooting, contact and work with vendors to obtain product information, and resolve technical problems.

10. To establish and maintain proper risk management policies, standards and guidelines.

11. To carry out daily, weekly and monthly backups on the system for specific work items devolving on the Information Security Officer.

12. To design and maintain applications including web server.

13. To monitor, maintain, manage, safeguard IT related documents, tools, equipment and legal agreements. Document security policies and procedures implemented by the Director of the FIU and implement such policies and procedures.

14. To monitor, on a regular basis, access control to file servers and internet access and submit weekly reports.

15. To initiate, facilitate and promote regular activities to create security awareness within the FIU and document and maintain relevant training manuals. To keep abreast of the latest security, privacy legislations, regulations, guidelines and vulnerability pertaining to the FIU and its legal commitments.

16. To communicate and create security awareness programs among the staff and other stakeholders. To keep abreast of the latest security legislations, regulations, guidelines and vulnerability pertaining to FIU and its missions.

17. To conduct functionality and gap analysis to determine the extent to which key areas and infrastructure at the FIU comply with statutory/regulatory requirement or international standards.

Compliance Division:

Enforcement:

1. To conduct regular compliance inspections as per established FIU's procedures;
2. To collect and maintain all records of documents and other relevant information for regulatory action as may be initiated by the FIU;
3. To write inspection reports;
4. To conduct research on domestic and international AML/CFT developments in respect of DNFBPs;

Compliance:

1. To manage the registration platform of the FIU of all reporting entities;
2. To monitor compliance with AML/CFT requirements of the Financial Intelligence and Anti-Money Laundering Act, 2002 and associated regulations as well as guidelines and directives issued by the FIU;
3. To assist in monitoring payment of penalties imposed by the FIU; and
4. To conduct relevant research and keep abreast of developments in international AML/CFT standards for DNFBPs

NOTE:

Analysts (Operations) posted in any of the above divisions should also:

a. use ICT in the performance of his duties.
b. perform such other duties directly related to the main duties listed above or related to the delivery of the output and results expected from an Analyst in the roles ascribed to him.