Sugar Cane Growers Fund

007/2025

Provision for Cloud Services (IaaS)

Terms of Reference

Contents

1. Introduction - About SCGF

The Sugar Cane Growers Fund **(SCGF)** is committed to supporting sugar cane growers by providing loans tailored to their needs. Currently, the Fund manages approximately 5,351 accounts, encompassing both specialized and priority loans, with a lending portfolio of around $35 million, including individual farmers and institutional loans. The portfolio continues to expand, with ongoing product and service revisions expected to drive significant growth in the coming years.

SCGF’s head office is located on the 2nd floor of the Sugar Cane Growers Council Building, at **75** Drasa Avenue, Lautoka. Additionally, the Fund operates in six district offices across Rakiraki, Tavua, Ba, Nadi, Labasa, and Seaqaqa. SCGF also owns a subsidiary, South Pacific Fertilizers Limited, specializing in the sale and distribution of fertilizers and weedicides.

SCGF invites proposals from qualified cloud service providers for deploying a cloud infrastructure to support the Digital Transformation. This system will be implemented in three key phases: deployment of a vanilla instance, staging and user acceptance testing (UAT) environment setup, and production environment deployment.

2. Primary Objective

The primary objective is to setup staging and production environments on cloud that will enable SCGF to provide a sustained level of performance to its end stakeholders by provisioning the optimal compute / memory / storage capacities to begin with and having the ability to quickly scale up / down the capacities as per the workload requirements listed below in the next sections.

SCGF also expects to gain cost efficiencies through the “Opex” / “pay-per-use” payment model so that SCGF pays only for the resources it consumes.

3. Purpose of the Terms of Reference

This Terms of Reference (TOR) aims to procure cloud services from various Cloud Service Providers for SCGF. It seeks a cloud partner to provide the necessary infrastructure, technical expertise, and support for deploying the current virtual environment.

The TOR invites proposals from eligible and interested bidders but does not commit the IT Department to a binding agreement. Throughout this document, potential bidders are referred to as "Bidders."

4. Scope

SCGF seeks proposals for Infrastructure as a Service (IaaS) solutions, covering the following:

The project will be carried out in three phases as outlined below:
Phase 1: Deployment of Vanilla Instance of the Cloud.

- Initial Setup of the Cloud Environment
- Installation and Configuration
- Testing and Verification

Phase 2: Staging and User Acceptance Testing (UAT) Environment Setup

- Setup of Staging/ UAT Environment
- Migration of Test Data
- Risk Mitigation and Change Management

Phase 3: Deployment of the Production Environment

- Provisioning and Optimization of Production Resources
- Security and Compliance
- Data Migration to Production
- Testing, Performance Tuning, and Validation
- Go-Live and Post-Deployment Support

SCGF wishes to engage / select CSP for providing Cloud Services for a period as required for hosting of IaaS. The scope of work is as:

1. The Bidder will be responsible for provisioning of required IT infrastructure as IaaS for hosting SCGF Applications.
    1. The proposed landscape for the deployment of SCGF applications are
        a. Development
        b. Staging
        c. Production
2. The above environments are to be deployed on the Virtual Private Cloud.
3. The environment of Virtual Private Cloud shall comply with the respective data sovereignty policy of Government of Fiji.
4. Each of the environments mentioned above should be logically isolated, i.e., separate from the production environment in a different VLAN than the production environment and setup such that users of the environments are in separate networks.
5. The Bidder shall be responsible for provisioning required compute infrastructure (server/virtual machines), storage for hosting SCGF applications. The bidder has to manage and maintain the VM’s including underlying Hardware, Operating systems, etc. for the contract period for 3 years.

6. The bidder will be responsible for provisioning of requisite network infrastructure (including switches, router, firewalls, and load balancers) to ensure accessibility of the servers as per defined SLA's. All the equipment's/Devices in the path have to be in HA mode.

7. The database server storage has to be provided on high-speed disks (SSD's) for better performance.

8. Manage the instances of storage, compute instances, and network environments. This includes IT Department-owned & installed operating systems and other system software that are outside of the authorization boundary of the CSP. Service Provider is also responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations.

9. Provide support to technical team of SCGF / IT Department or nominated agency for Optimization of resources in cloud environment for better performance and also provide physical and virtual access to the technical persons for the resolution of any issue pertaining to the operation, maintenance or rectification to keep the application running without any problem, as authenticated by SCGF / IT Department.

10. The bidder should provide 24*7 Helpdesk & Technical support services. This will include system maintenance windows. Bidder should provide a 24*7 operated contact number which will be used by SCGF / IT Department or its authorized agency to raise any issues related to the services provided by the bidder.

11. CSP should provide training to SCGF nominated minimum 3 officials/personnel on usage of the Console and any other technical aspect for monitoring of SCGF project.

4.1 Calendar of Events Timelines

On a high level the timelines that we are looking at for this project would be as follows:

Milestones	Tentative Timeline
Advertisement of Tender	04th Jul 2025
Tender Closing	18th Jul 2025
Presentation and Evaluation of Tender	31st Jul 2025
Finalization of Award of Tender	5th Aug 2025
Contract Negotiation and Finalization	15th Aug 2025
Service Delivery and full Implementation	30th Sep 2025

4.2 Role of existing System Integrator (SI)

IT Department's existing SI would deploy the IT Applications in the cloud infrastructure. The SI would manage the application, data and the database. The selected CSP shall provide required VMs and other cloud resources and System Software for deploying such applications.

4.3 Security & Statutory Requirements

Certification/Compliance:

1. The CSP/Bidder facilities/services need to be certified / compliant to the following standards based on the project requirements.
2. ISO 27001 - Data Center and the cloud services should be certified for the latest version of the standards.
3. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information Technology.
4. The bidder shall submit the respective certificates issued by the authorized agency/persons.

Privacy and Security Safeguards

1. CSP/Bidder to notify the agency promptly in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively.
2. The CSP/Bidder shall ensure that all the storage blocks or multiple copies of data if any are unallocated or zeroed out by the CSPs so that data cannot be recovered. If due to some regulatory reasons if it is required to securely decommission data, IT Department can implement data encryption at rest using IT Departments managed keys, which are not stored in the cloud. Then IT Department may delete the key used to protect the decommissioned data, making it irrecoverable.
3. The CSP/Bidder shall report forthwith in writing of information security breaches to the IT Department by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.
4. The CSP undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the IT Department.

Confidentiality

1. The Bidder shall execute non-disclosure agreements with the IT Department with respect to this Project. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:
2. Information already available in the public domain;
3. Information which has been developed independently by the Service Provider;
4. Information which has been received from a third party who had the right to disclose the aforesaid information;
5. Information which has been disclosed to the public pursuant to a court order.

4.4 Location of Data

The location of the data (text, audio, video, image files, drawing files, GIS files, pdf, and any compressed data and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the IT Department account and any computational results that IT Department or any end user derives from the foregoing through their use of the CSP’s services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider.

4.5 Law Enforcement Request

The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the Cloud Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency.

4.6 Audit

IT Department shall ensure that the Cloud Service Provider’s services offerings are audited and certified.

4.7 Architecture, Auto Scaling & Performance

1. The proposed architecture for the cloud service should be capable of auto scaling without any manual intervention for all the resources including but not limited to vCPU, vRAM, Bandwidth, storage etc.
2. The proposed architecture should Auto scale the cloud workload to meet high / unpredictable demands. In this context, provisioning of Load Balancing, amongst others must be an integral part of the proposed architecture / solution.
3. Auto-scaling to be done based on defined rules and parameters e.g., CPU utilization and memory usage.
4. Scaling should be done both vertically – by increasing the amount of memory available to each instance – or horizontally – by creating additional instances.
5. The Cloud platform should provide a way to track the billing based on utilization and service levels in a Dashboard.
6. The architecture should have the inherent feature capability to auto scale the deployed application in the scaled-up resources.

4.8 Audit & Governance Requirements

The CSP shall implement the audit & compliance features to enable SCGF or its nominated agency to monitor the provisioned resources, performance, resource utilization, and security compliance:

1. View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
2. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
3. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.
4. Review of auto-scaling rules and limits.
5. Logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.
6. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and IT Department or its nominated Agencies should be given the ability to dig into the configuration history to perform incident analysis.
7. Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using Identity and Access Management (IAM), and weak password policies.
8. Automated security assessment service that helps improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices. After performing an assessment, the tools should produce

a detailed list of security findings prioritized by level of severity.

5. Bidding Terms & Conditions

5.1 Instructions to Bidders

- Availability of TOR Documents

The TOR can be downloaded from the website. The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the TOR documents. Failure to furnish all information required as mentioned in the TOR documents or submission of a proposal not substantially responsive to the TOR documents in every respect will be at the bidder's risk and may result in rejection of the proposal and forfeiture of the bid security.

- Bidders Queries and SCGF's Response

1. All enquiries from the prospective bidders relating to this RFP must be submitted in writing exclusively to the contact person. A copy of the bidder enquiries should also be emailed to the bid issuer's email address.
2. After the TOR is issued to the bidder, SCGF shall accept questions/inquiries through email from the bidders. SCGF will endeavor to provide a complete, accurate, and timely response to all questions to all the bidders within 3 days.
3. In order to allow bidders a reasonable time to take the amendment(s) into account in preparing their bids, SCGF at its discretion, may extend the deadline for the submission of bids.

- Proposal Preparation Costs

The bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal in providing any additional information required by SCGF to facilitate the evaluation process, and in negotiating a definitive Service Agreement and all such activities related to the bid process.

- Commercial Bid Formats

Please provide a separate detailed fee structure and implementation schedule for each scope as part of your submission clearly indicating VAT/GST and other Taxes. Breakdown of costing should be in the following format. The lines in the table are a guideline and further details may be added as required to fully show all costs involve in this engagement:

Activities	Unit Cost FJD$ (VIP)	Remarks
Primary Cloud		
Backup		
Replication		

Security and Firewall		
Cloud Dedicated Internet		
WAN Connectivity		
Any other Cost		
Cost		
VAT component		
Total Cost (VIP)		

- Language of Proposal

The proposal and all correspondence and documents shall be written in English.

- Bid Submission Instructions

Bid must be direct, concise, and complete. All information not directly relevant to this TOR should be omitted. SCGF will evaluate bidder's bid based on its clarity and the directness of its response to the requirements of the project as outlined in this TOR.
Bidders shall furnish the required information on their technical and price binds in the formats provided in the TOR. Any deviations in format the tender will be liable for rejection.

6. Expectations

On a high level the expectation that SCGF would have from the selected firm would be, but not limited to the following:

1. Adhere to the communication guidelines as set out in this Terms of Reference;
2. Act in the interest of SCGF at all times;
3. Maintain Transparency and provide honest, clear and sound advice;
4. Adhere and uphold SCGF policies and procedures;
5. Refrain from entering into agreements or obligations on behalf of SCGF;
6. Sign an NDA and uphold strict confidentiality;
7. Ensure that all **information, data, innovations, and solutions** remain SCGF's intellectual property;
8. Meet all timelines and provide required documentation throughout the engagement.

7. Business Requirements of IaaS

	Category	Type	Configuration	Requirements
1	Compute (VM)	Virtual Machines Storage VCPU RAM	As per SCGF server specification-Refer to Appendix A	
2	Security and Firewall	Required		
3	Backup	Full VM backup required		
4	Replication	Full VM backup required		
5	Cloud Dedicated Internet	Required		
6	WAN Connectivity	Required		
7	Disaster Recovery Site	Define the type of Recovery Site Offered		
8	Disaster Recovery Test	Define the number of tests included per year		
9	Recovery Time Objective	Define Recovery Time Objective(4 hours)		
10	Recovery Point Objective	Define Recovery Point Objective (1 hour)		
9	Downtime	Define downtime of services		

8. EOI Requirements

Payment will be made periodically, based on deliverables, milestones, or mutual agreement.

Applicants must:

1. Submit proposals covering the entire project scope.
2. Provide a list of required human resources (HR) and their roles in implementation.
3. Disclose third-party involvement, including HR details.
4. Quote all prices in Fijian Dollars, specifying the exchange rate if using foreign currency.

9. Composition and Authority to Act

The appointed firm reports to the Chief Executive Office of SCGF but functionally to the

Manager Information Technology. All reports and communication are to be addressed to the Chief Executive Officer with copies to the Manager Information Technology.

10.Selection Procedures

The selection of the successful tenderer will be done in accordance with SCGF's Internal Policy guidelines. Bidders are advised to study the tender document carefully. Some important criteria are:

- Experience implementing IaaS environment
- Security & Compliance
- Reliability & Performance
- Scalability & Flexibility
- Integration & Compatibility
- Cost & Pricing Models
- Timeline of delivery
- Support & Service Level Agreement (SLAs)

Late, proposals will not be accepted. SCGF reserves the right to accept, decline or negotiate with one or all bidders. The lowest bid may not necessarily be accepted.

11.Contractual Arrangements

SCGF will establish a Contractual Arrangement with the appointed service provider based on a final negotiation of the cost arrangements as based on the outlined fee structure and implementation schedule. There will be one contract between SCGF and the appointed service provider.

No binding legal relationship will exist between any of the Respondents and SCGF until execution of a contractual agreement. The terms of reference documents contains statements derived from the information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with SCGF.

12.Cost Structure

Please provide a separate detailed fee structure and implementation schedule for each scope as part of your submission clearly indicating VAT/GST and other Taxes. Breakdown of costing should be in the following format. The lines in the table are a guideline and further details may be added as required to fully show all costs involve in this engagement:

Activities	Unit Cost FJD$ (VIP)	Remarks
Primary Cloud		
Backup		
Replication		
Security and Firewall		
Cloud Dedicated Internet		
WAN Connectivity		
Any other Cost		
Cost		
VAT component		
Total Cost (VIP)		

13.Submission of Proposal guidelines

The Proposal must be submitted by no later than 4.00 pm, Friday 18th July 2025. Proposals may be submitted via two (2) methods:

The bids must reach the office of SCGF on or before **18th July 2025 at 4:00 pm** via email – **tender@scgf.com.fj** and/or placed in the tender box provided at Level 2 at the Sugar Cane Growers Fund Head Office at Sugar Cane Growers Council Building, 75 Drasa Avenue, Lautoka. Late submissions will not be accepted.

"EOI – 007/ 2025 –IaaS Solution Provider"
The Chairman
Tender Committee
Sugar Cane Growers Fund
P O Box 13, Lautoka

14.Enquiries

Please note that for any clarification on the Purchase or Terms of Reference, the following Sugar Cane Growers Fund Personnel should be contacted:

1. Sheetal Shalini
Manager Information Technology
PH: (679) 665 0777 / 9987793
Email: sheetal@scgf.com.fj
2. Shikant Chand
System Analyst
PH: (679) 665 0777
Email: shikant.chand@scgf.com.fj

15.Appendix A

No:	Server Name	Vcpu	Memory (GB)	Total Storage (GB)	Growth Rate per Year	Operating System	Daily Backup Retention	Weekly Backup Retention	Monthly Backup Retention
1	Domain Controller	4	6	300	10%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
2	App Server	6	8	400	10%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
3	DB Server	6	12	1000	15%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
4	FS Server	4	8	1500	20%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
5	Sage Server	4	8	400	10%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
6	Payroll Server	4	8	400	10%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
7	Mobile App Server	4	8	400	10%	Windows Server 2019 Standard or higher	1 Week	1 Month	2 Months
		32	**58**	**4400**					