Section III: Schedule of Requirements

eSourcing reference: RFP/2024/55002

TERMS OF REFERENCE

Hosting of CAFI PES tool (Lot 1)

1. Purpose

The primary objective of this Terms of Reference (ToR) is to acquire a cloud hosting environment on Microsoft Azure that fulfills the technical, security, and operational requirements for the Central African Forest Initiative (CAFI) Payments for Environmental Services (PES) tool. The hosting environment will provide the necessary infrastructure to support the secure and scalable operation of the PES tool, which is designed to manage, track, and verify national PES schemes across Central African countries.

This cloud environment will ensure high availability, data security, and seamless scalability to accommodate the expected growth in data volume and user base as the PES program expands. Microsoft Azure, a globally recognized cloud platform, will be utilized due to its robust features in compliance, scalability, security, and global reach, aligning with the operational demands of the CAFI PES tool. The cloud setup will include three dedicated environments—Development, Staging, and Production—for smooth software deployment, testing, and live operation.

Ultimately, this hosting solution will support CAFI's mission to improve the effectiveness and transparency of its PES investments. It will ensure that the digital platform operates efficiently and securely while adhering to the highest standards of cloud infrastructure management. The chosen cloud environment will meet current needs and be flexible enough to adapt as the PES program evolves over time.

2. Background

The Central African Forest Initiative (CAFI) is a multi-donor partnership aimed at preserving the forests of Central Africa and supporting sustainable development across the region. Payments for Environmental Services (PES) is a critical component of this initiative, designed to incentivize local communities and farmers to engage in sustainable land management practices by providing performance-based financial incentives for maintaining forested areas and preserving valuable ecosystem services such as biodiversity conservation, carbon sequestration, and water cycle regulation.

The PES mechanism encourages these communities to adopt environmentally responsible practices, thus

contributing to the fight against deforestation, climate change, and soil degradation. This scheme targets key CAFI partner countries, including Cameroon, the Democratic Republic of Congo, Gabon, and the Republic of Congo. By implementing PES schemes, CAFI aims to reduce agricultural expansion into forest areas while supporting the sustainable livelihoods of local populations.

As part of this strategy, CAFI has developed a digital platform to manage and track the implementation of PES in these regions. This tool supports transparency, accountability, and efficiency in managing PES activities.

The Role of the PES Tool in CAFI Investments

The CAFI PES tool is pivotal in improving the effectiveness, efficiency, and transparency of CAFI's regional investments. The tool streamlines the administration of PES schemes by providing a digital platform to manage the entire PES lifecycle—from participant registration and validation to monitoring and reporting on environmental services delivered. This leads to better resource allocation, more effective results monitoring, and greater accountability among participants.

Furthermore, the tool facilitates real-time access to data and analytics, allowing for timely decision-making and adjustments to PES strategies as needed. This is expected to increase the overall impact of CAFI's investments, ensuring that funds are deployed efficiently and that results are measurable and verifiable.

Key Modules of the CAFI PES Tool

The CAFI PES tool is composed of five core modules that support the end-to-end management of the PES scheme:

1. **Administration Module:** The administration module enables the central management of users, roles, permissions, and workflows within the PES tool. It provides administrators with full control over the platform's configuration, ensuring that only authorized users can access sensitive information and perform key functions. This module also supports platform customization to meet the specific needs of different PES programs.

2. **Admission Module:** The admission module is responsible for registering participants in the PES scheme, including farmers, community groups, and other stakeholders. It handles the validation and verification of eligibility criteria, ensuring that only qualified participants can benefit from the scheme. This module also manages new participants' documentation and approval process, providing transparency and accountability.

3. **Monitoring Module:** The monitoring module tracks the delivery of environmental services, such as agroforestry, reforestation or conservation, by participants in the PES program. This module integrates with remote sensing technologies, geospatial data, and field reports to provide real-time updates on the status of these services. The ability to monitor progress in real time helps ensure that PES participants are meeting their commitments and allows for timely interventions if issues arise.

4. **Reporting Module:** The reporting module generates detailed reports on the performance of the PES program, including financial summaries, environmental outcomes, and compliance with program requirements. These reports can be customized to meet the needs of different stakeholders, including CAFI, partner governments, and donor organizations. This module plays a crucial role in maintaining transparency and demonstrating the impact of CAFI's investments to external stakeholders.

5. **Map Viewer Module**: The map viewer module provides a geospatial visualization of the areas covered by the PES scheme. It allows users to view and analyze land use patterns, forest cover, and other environmental services in a visual format. By overlaying data from multiple sources, the map viewer enables better land management decision-making and helps identify areas where PES interventions are most needed. Together with the reporting module, the map viewer is also a crucial element of transparency and accountability.

Together, these modules form a comprehensive system for managing CAFI's PES programs. This system improves the initiative's overall effectiveness by ensuring that resources are used efficiently, results are clearly documented, and participants are held accountable for their contributions to environmental preservation.

3. Assignment-specific Objectives

The primary objective of this assignment is to establish a cloud hosting environment on Microsoft Azure that will support the successful deployment, operation, and scaling of the Central African Forest Initiative (CAFI) Payments for Environmental Services (PES) digital tool. This environment must meet the technical, security, and operational needs of CAFI's PES tool and ensure the platform can handle the increasing data volume and user base as the program expands.

Key Goals:

1. **Cloud Environment Setup: Development, Staging, and Production**

   o **Development Environment:** This environment will be dedicated to ongoing development work, including implementing new features and functionality, bug fixes, and system enhancements. It will serve as the primary workspace for developers to make changes and conduct preliminary testing.

   o **Staging Environment:** The staging environment will mirror the production environment as closely as possible to allow for thorough testing of new features, integrations, and configurations before they are released. This environment will be used for quality assurance (QA) and validation by the CAFI team and stakeholders.

   o **Production Environment:** The production environment will host the live version of the PES tool used by CAFI, partner governments, and other stakeholders. It must be highly available, secure, and scalable to support the PES program's operational needs.

2. **Scalability and Performance**

   o The hosting environment must be scalable to accommodate the evolving needs of the CAFI PES tool. As more users and data sources are integrated into the platform, the cloud infrastructure should be able to scale seamlessly without compromising performance. This includes handling large datasets, real-time processing, and concurrent user activities.

   o CAFI anticipates increased demand for the PES tool over time, and the selected hosting solution must be flexible enough to allow for adding new features and functionalities while maintaining optimal performance.

3. **Security and Compliance**

   o The cloud hosting solution must meet stringent security standards to protect sensitive data related to PES participants, forest areas, and financial transactions. This includes implementing identity and access management (IAM) controls, data encryption (both at rest and in transit), and multi-factor authentication (MFA) for all users accessing the platform.

   o Compliance with local and international regulations, including data privacy laws and environmental standards, is critical to the hosting environment. The solution must also ensure regular security updates and monitoring to protect against threats and vulnerabilities.

4. **High Availability and Reliability**

   o The production environment must guarantee high availability to ensure uninterrupted access to the PES tool by CAFI and its stakeholders. This includes minimizing downtime and ensuring that the platform can recover quickly from any unexpected disruptions.

   o Microsoft Azure's global network of data centers will be leveraged to provide redundancy, failover options, and disaster recovery capabilities. CAFI's priority is to host the data in Africa with replication in Europe to ensure data security and resilience.

5. **Ongoing Support and Maintenance**

   o The service provider will offer continuous support to manage and maintain the cloud environment, including monitoring system performance, resolving technical issues, and ensuring the system is updated with the latest security patches and software upgrades.

   o The service provider will also assist with cost optimization strategies to ensure that the hosting environment remains financially sustainable while meeting performance and security requirements.

6. **Compliance with CAFI's Technical Requirements**
   - o The cloud hosting environment must be designed to integrate seamlessly with CAFI's PES tool and support its five core modules (Administration, Admission, Monitoring, Reporting, and Map Viewer).
   - o The infrastructure should be flexible enough to support future platform updates or expansions while maintaining compliance with CAFI's technical, security, and operational standards.

By achieving these objectives, the CAFI PES tool will operate efficiently and securely, enabling CAFI and its partners to manage and track PES schemes effectively across Central African countries. The hosting environment will also allow the tool to scale as needed, ensuring it remains a reliable resource for environmental services compensation and conservation efforts.

4. Geographical Coverage

The hosting of the CAFI PES tool requires a global scope to ensure seamless access, data availability, and compliance across multiple regions, particularly in Central Africa. The PES tool will be accessed by stakeholders across CAFI's countries, including Cameroon, the Central African Republic, the Democratic Republic of Congo, Equatorial Guinea, Gabon, and the Republic of Congo, and by international donors, partners, and other involved entities. Therefore, the hosting infrastructure must support secure and reliable global access to meet the needs of all users, regardless of their location.

- Data Hosting in Azure Regions in Africa

To align with CAFI's commitment to supporting development in Central Africa, there is a preference for hosting the PES tool's primary data in **Microsoft Azure regions within Africa**. This ensures the data is stored and processed locally, closer to the countries implementing the PES schemes. Hosting in Africa provides several key advantages:

- **Reduced Latency:** Hosting data closer to end-users in Central African countries reduces latency, improving performance and user experience for local stakeholders accessing the tool.
- **Data Sovereignty:** Hosting within Africa aligns with regional preferences for keeping data within the continent, helping CAFI and partner countries comply with local data sovereignty laws and regulations.

Microsoft Azure offers data centers in Europe. A **secondary data replication site in Europe is essential** in South Africa (Johannesburg and Cape Town), which is well-suited to meet these requirements. A **secondary data replication site in Europe ensures data resilience, redundancy, and disaster recovery**. It also provides a backup option in the event of secure, scalable, and low-latency cloud services.

- Data Replication in Europe for Resilience

To ensure data resilience, redundancy, and disaster recovery, it is essential to have a **secondary data replication site in Europe**. This provides a backup option in the event of any service disruptions or data loss in the primary African data centre. By replicating the data to an Azure region in Europe, CAFI can guarantee that the system remains operational even during unforeseen issues or outages.

Benefits of replication in Europe include:

- **Enhanced Disaster Recovery:** Should the African data center experience any downtime, data replication in Europe ensures that the PES tool can continue to operate with minimal disruption, protecting the integrity of the data and allowing for swift failover if needed.
- **Global Accessibility:** European replication also ensures that international donors, partners, and stakeholders who access the PES tool from other parts of the world experience consistent performance and availability.
- **Compliance with International Standards:** European data centers adhere to strict security and compliance standards, adding an extra layer of protection and resilience to the hosting environment.

- Global Access and Availability

The global nature of the CAFI PES tool requires that the hosting solution provides secure and reliable access to users worldwide. Microsoft Azure's network of global data centers ensures that users in CAFI's partner countries, international organizations, and donor agencies can access the platform efficiently. The system will be designed to manage varying levels of traffic and ensure high performance and uptime for all users, whether in Central Africa, Europe, or other regions.

The combination of hosting data in Africa and replication in Europe balances performance, resilience, and compliance, enabling the CAFI PES tool to function effectively across its wide geographical scope. This approach ensures data integrity, high availability, and rapid disaster recovery while supporting local data regulations and promoting sustainable technological development in Africa.

5. Methodology and Approach

This section outlines the methodology and approach the selected service provider will follow in delivering the cloud hosting solution on Microsoft Azure. The approach encompasses account setup, security and compliance, scalability, support, and maintenance, ensuring that the CAFI PES tool operates effectively and securely, and can grow as required.

5.1 Provisioning Cloud Account

The first step in the assignment is to provision a **Microsoft Azure cloud account** specifically configured to meet the needs of the CAFI PES tool. This includes:

1. **Azure Account Setup**

   o The provider will set up a dedicated Microsoft Azure account for CAFI with access to three distinct environments: Development, Staging, and Production. These environments will be configured according to CAFI's technical and operational requirements to facilitate seamless development, testing, and live operations.

   o Virtual machines, databases, and storage will be allocated based on the predefined estimates for each environment. The provider will also ensure that resource allocation is optimized for cost efficiency and performance.

2. **Configuration of Cloud Resources**

   o **Development Environment:** Configured for ongoing feature development, testing of new functionalities, and bug fixing. This environment will be more flexible to accommodate frequent changes.

   o **Staging Environment:** A stable, near-production replica to conduct quality assurance (QA) and validate system performance before moving updates to production.

   o **Production Environment:** The live environment will be highly secure and scalable to meet the needs of real-time users, ensuring high availability and performance.

   o Network security, virtual networks, and load balancers will be configured to protect resources and enable smooth traffic management across the environments.

3. **Account Access and Permissions**

   o The provider will configure **role-based access control (RBAC)**, ensuring that different users (developers, administrators, and stakeholders) only have access to the required resources.

   o A clear governance structure will be implemented to ensure that the PES tool is managed efficiently with defined roles for administrative functions.

5.2 Security and Compliance

Ensuring the security of CAFI PES data and compliance with regulatory frameworks is critical to this assignment. The provider will implement the following security measures:

1. **Identity and Access Management (IAM)**

   o **Multi-factor authentication (MFA)** will be enforced for all users accessing the cloud environment to reduce the risk of unauthorised access. This includes administrators, developers, and other users involved in the **To reduce the risk of unauthorised access, multi-factor authentication (MFA)** will be enforced for all users accessing the cloud environment, including administrators, developers, and other project users project.

   o **Identity and access management (IAM)** will be configured to control user access to sensitive resources. This ensures that users only have the minimum necessary permissions to perform their tasks.

2. **Data Encryption**

   o **Encryption at Rest:** All data stored in the Azure cloud will be encrypted using advanced encryption standards (AES-256) to protect it from unauthorized, such as **Azure Security Center,** to detect and respond to potential threats in real time access.

   o **Encryption in Transit:** Data transmitted between users and the cloud environment will be encrypted using TLS (Transport Layer Security), ensuring secure communication.

3. **Compliance with Regulatory Requirements**

   o The hosting solution will comply with local data protection laws, including any specific requirements of CAFI's partner countries (such as data sovereignty laws in Central Africa).

   o Microsoft Azure's compliance with international standards such as **ISO 27001, GDPR**, and **SOC 2** will ensure the cloud environment meets stringent security and privacy regulations.

4. **Security Monitoring and Auditing**

   o Continuous security monitoring will be implemented, utilising Azure's built-in tools such as **Azure Security Center** to detect and respond to potential threats in real-time.

   o Regular security audits and vulnerability assessments will be conducted to maintain a high level of security.

5.3 Scalability

The CAFI PES tool is expected to handle increasing volumes of data and a growing user base over time. To ensure that the system remains responsive and performs optimally, the provider will implement the following scalability strategies:

1. **Auto-scaling**

    o **Auto-scaling** will be enabled in the Development, Staging, and Production environments to automatically adjust computing resources based on usage demands. This ensures that the system can handle spikes in traffic without experiencing performance degradation.

    o Additional storage and computational resources will be automatically provisioned as more data is uploaded or as more users access the system, ensuring uninterrupted service.

2. **Elastic Resource Allocation**

    o Azure's elastic infrastructure will allow resources to be scaled dynamically, meaning that computing power, storage capacity, and networking resources can expand or contract as needed without manual intervention.

3. **Load Balancing**

    o Load balancers will be employed to distribute traffic evenly across multiple servers. This will prevent any single server from becoming overwhelmed, ensuring optimal performance even during peak times.

4. **Future-Proofing the Infrastructure**

    o The architecture will be designed with future growth in mind, ensuring that new services or modules can be added without requiring significant reconfiguration of the existing infrastructure.

5.4 Support and Maintenance

To ensure the continued success and reliability of the cloud-hosted PES tool, the provider will offer ongoing support and maintenance services, including:

1. **24/7 Technical Support**

    o The service provider will offer round-the-clock support to address any technical issues or performance concerns that may arise. A dedicated support team will be available to troubleshoot issues and provide prompt resolutions.

    o This includes incident management for use Azure's monitoring tools to continuously track the system's performance. **Azure Monitor** and **Application Insights** will be used to identify downtime, slow performance, or other disruptions to the service.

2. **Monitoring and Performance Optimization**

    o The provider will utilise Azure's monitoring tools to continuously track the performance of the system. **Azure Monitor** and **Application Insights** will be used to identify any potential bottlenecks, optimise performance, and ensure the system is operating efficiently.

    o Regular reports on system performance, security incidents, and usage will be provided to CAFI to keep stakeholders informed.

3. **Billing and Cost Management**
    - o The provider will assist in managing the cloud service costs by optimizing resource allocation and advising on cost-saving strategies. Azure's **Cost Management** tool will track usage and forecast future costs, ensuring that CAFI stays within budget.
    - o Monthly usage reports and billing updates will be shared with the CAFI team to provide full visibility into the ongoing costs of hosting the PES tool.

4. **System Updates and Patches**
    - o The provider will ensure that the hosting environment is updated with the latest software and security patches. Azure's **Update Management** tool will automatically apply critical updates without causing service disruptions.
    - o Periodic system maintenance windows will be communicated in advance to minimize downtime and ensure smooth operations.

Following this comprehensive methodology, the service provider will ensure the CAFI PES tool is hosted in a secure, scalable, and highly available environment. The cloud infrastructure will support both current needs and future growth while adhering to CAFI's technical and compliance requirements. The ongoing support and maintenance will guarantee that the system operates efficiently and that any issues are addressed quickly and effectively.

6. Execution Timeline (Chronogram)

Executing the CAFI PES tool hosting project on Microsoft Azure will follow a structured timeline to ensure that all phases are completed effectively and within the designated time frame. Each phase will focus on specific tasks that are critical to the successful deployment, operation, and scaling of the PES tool. The timeline is divided into key milestones, starting with the initial setup of the cloud infrastructure and culminating in ongoing support and monitoring over 12 months. The total service period must not exceed 57 weeks (2 months and one week for setting up and deploying the hosting solution and 12 months for support and monitoring: 14 months and one week: 56 weeks and one week: 57 weeks in total).

6.1. Week 1: Inception and Mobilization

In the first week, the focus will be on establishing the foundational elements of the hosting environment.

Tasks:

- o Set up the Microsoft Azure account dedicated to CAFI.
- o Provision of initial resources, such as virtual machines and storage, to prepare for the development environment.
- o Define the access control policies using Identity and Access Management (IAM) with role-based permissions.
- o Configure the basic network architecture, ensuring connectivity between virtual machines and storage solutions.

Deliverables:

- o Azure account created and configured.
- o Initial resources and access controls are in place.

6.2. Weeks 2-3: Development Phase

During this phase, the cloud infrastructure will be fully configured to support the development of the CAFI PES tool.

Tasks:

- o Provision and configure virtual networks, databases, storage, and compute resources to support the three distinct environments (Development, Staging, and Production).
- o Set up automated scaling options for resource management.
- o Define security protocols, including multi-factor authentication (MFA), rest data encryption, and transit data encryption.
- o Implement basic monitoring tools, such as Azure Monitor, to track system performance and usage.

Deliverables:

- o The development environment fully set up with all required resources.
- o Security measures and monitoring tools were activated.

6.3. Weeks 4-6: Staging and Testing

The staging environment will be used to deploy the PES tool for testing and validation before final production deployment.

Tasks:

- o Deploy the CAFI PES tool in the staging environment.
- o Conducted system tests, including load testing, performance testing, and functional testing, to ensure that the system performed as expected under different conditions.
- o Implement Quality Assurance (QA) procedures to identify and address potential issues before the tool goes live.
- o Verify security compliance and ensure that data is encrypted and access controls function as required.

Deliverables:

- o The PES tool was successfully deployed and tested in the staging environment.
- o QA reports and performance validation results.

6.4. Weeks 7-8: Production Deployment

Once the PES tool has been successfully tested, it will be deployed to the production environment for end-users.

Tasks:

- o Deploy the thoroughly tested version of the PES tool to the production environment.
- o Ensure all security measures and monitoring tools are fully implemented in the production environment.
- o Conduct final validation to ensure that the production system functions correctly and that end-users can access it without issues.
- o Ensure the system is prepared for scalability and handle any initial feedback or issues during the first days of live operations.

Deliverables:

- o   The PES tool is fully operational in the production environment.
- o   Final validation report confirming system readiness.

6.5. Weeks 9-57: Support and Monitoring

After the production deployment, continuous monitoring and support will be provided over the 12 months to ensure smooth operations.

Tasks:

- o   Implement real-time monitoring tools to track system performance, usage, and potential security issues.
- o   Provide 24/7 technical support to address any issues that may arise.
- o   Regularly review and optimise resource allocation to ensure cost-efficiency and scalability as data volumes and user numbers increase.
- o   Apply software updates, security patches, and performance optimizations as needed.
- o   Provide monthly reports on system performance, costs, and incident resolution.

Deliverables:

- o   Monthly performance and monitoring reports.
- o   System updates and optimizations applied as necessary.

6.6. Execution Timeline Table

This table provides a clear overview of the entire execution timeline, ensuring that all phases are well-structured and aligned with the project's overall goals.

Phase	Tasks	Timeline	Key Deliverables
Inception and Mobilization	- Set up Azure account - Provision initial resources - Configure access control policies	Week 1	- Azure account setup - Basic infrastructure in place
Development Phase	- Configure virtual networks, databases, and compute - Set up automated scaling - Implement security protocols	Weeks 2-3	- Development environment ready - Security and monitoring tools activated
Staging and Testing	- Deploy tool in a staging environment - Conduct QA and performance tests - Verify security compliance	Weeks 4-6	- PES tool tested in staging - QA and performance validation reports
Production Deployment	- Deploy tool in production - Final validation - Ensure scalability and performance	Weeks 7-8	- PES tool live in production - Final system validation
Support and Monitoring	- Provide technical support - Monitor system performance - Apply updates and patches	Weeks 9-57	- Monthly performance reports - Continuous optimization

Each phase is designed to build upon the previous one, leading to the successful deployment and ongoing operation of the CAFI PES tool.

7. Key Personnel

Successfully executing the CAFI PES tool hosting assignment requires a team of highly skilled professionals with specific expertise in cloud infrastructure, security, and technical support. The following key personnel will play critical roles in ensuring the smooth setup, deployment, and ongoing operation of the Microsoft Azure hosting environment for the CAFI PES tool.

Key Personnel

Role	Responsibilities	Expertise and Experience	Qualifications
Cloud Infrastructure Engineer	- Set up Azure account - Configure virtual networks, storage, compute resources - Manage cloud scaling	- Proven experience in managing Azure cloud environments - Strong knowledge of cloud architecture	- Bachelor's/Master's in IT/Computer Science - Azure Solutions Architect certification
Security Specialist	- Implement IAM and encryption - Ensure regulatory compliance - Monitor and respond to security threats	- Experience in Azure security protocols - Strong knowledge of GDPR, ISO 27001, and encryption	- Bachelor's/Master's in Cybersecurity - Azure Security Engineer certification
Support Engineer	- Provide 24/7 technical support - Manage Azure billing and monitoring - Troubleshoot technical issues	- Experience in Azure cloud support - Knowledge of billing and resource optimization	- Bachelor's in IT/Computer Science - Azure Administrator certification

Each team member must have relevant expertise and experience to ensure the project meets its objectives efficiently and securely.

7.1 Cloud Infrastructure Engineer

Role:

The Cloud Infrastructure Engineer will be responsible for the initial setup and configuration of the Microsoft Azure cloud environment, including virtual networks, storage, and computing resources. This individual will also manage the allocation of resources across the Development, Staging, and Production environments and ensure that the system is optimized for performance and scalability.

Responsibilities:

- Set up and configure the Microsoft Azure account according to CAFI's specifications.

- Design and implement the PES tool's virtual networks, databases, and storage solutions.

- Configure and optimize cloud resources for scalability, cost-efficiency, and performance.

- Ensure the proper implementation of load balancers, firewalls, and virtual machines across all environments (Development, Staging, Production).

- Monitor cloud resource usage and optimize infrastructure to ensure smooth operations without exceeding cost budgets.

Expertise and Experience:

- Proven experience in managing Microsoft Azure cloud environments, including setting up and configuring virtual networks, databases, and compute resources.

- Strong knowledge of cloud architecture, resource management, and cost optimization in Azure.

- Familiarity with auto-scaling, performance monitoring, and virtual machine management in large-scale environments.

- Experience with cloud-based DevOps practices, including continuous integration and deployment (CI/CD).

Qualifications:

- Bachelor's or Master's degree in Computer Science, Information Technology, or a related field.

- Certifications in Microsoft Azure (e.g., Azure Solutions Architect, Azure Administrator).

7.2 Security Specialist

Role:

The Security Specialist will ensure that the hosting environment complies with CAFI's stringent security requirements, including data encryption, identity and access management (IAM), and regulatory compliance. This individual will be responsible for implementing and monitoring security protocols to protect sensitive data related to the PES tool and ensure compliance with international data protection laws.

Responsibilities:

- Implement identity and access management (IAM) policies, including role-based access control (RBAC) and multi-factor authentication (MFA).

- Ensure encryption of data at rest and in transit using industry-standard protocols.

- Conduct security audits and vulnerability assessments to identify potential threats and weaknesses.

- Ensure compliance with local and international data privacy and security regulations (e.g., GDPR, ISO 27001).

- Monitor and respond to security incidents in real-time, utilizing Azure Security Center and other security tools.

Expertise and Experience:

- Extensive experience in implementing security protocols and practices in cloud environments, particularly on Microsoft Azure.

- Strong knowledge of IAM, encryption methods, and regulatory compliance standards such as GDPR, ISO 27001, and SOC 2.

- Hands-on experience with security monitoring and incident response tools, including Azure Security Center and Azure Sentinel.

- Ability to conduct security assessments and vulnerability testing in large-scale cloud environments.

Qualifications:

- Bachelor's or Master's degree in Information Security, Cybersecurity, or a related field.

- Certifications in cloud security (e.g., Certified Cloud Security Professional - CCSP, Microsoft Certified: Azure Security Engineer Associate).

7.3 Support Engineer

Role:

The Support Engineer will provide ongoing technical support for the Azure cloud environment, handling day-to-day account management, and troubleshooting issues related to performance, user access, and system configurations. This individual will serve as the primary point of contact for technical issues and will ensure that the PES tool operates smoothly for end-users.

Responsibilities:

- Provide 24/7 technical support to resolve issues related to the cloud environment, such as resource management, network configuration, and system performance.

- Assist CAFI in managing Azure account billing, usage monitoring, and cost optimization.

- Manage user access, permissions, and troubleshooting related to identity and access management (IAM) policies.

- Collaborate with the Cloud Infrastructure Engineer to apply software patches, updates, and system optimizations as needed.

- Conduct routine system health checks and provide monthly reports on system performance and support incidents.

Expertise and Experience:

- Strong Microsoft Azure cloud support background, including resource management, monitoring, and troubleshooting.

- Experience with cloud billing and cost management, ensuring that cloud resources are used efficiently.

- Familiarity with user access controls, permissions management, and technical troubleshooting in cloud environments.

- Excellent communication skills, with the ability to provide technical support and guidance to both technical and non-technical users.

Qualifications:

- Bachelor's degree in Information Technology, Computer Science, or a related field.

- Certifications in Microsoft Azure (e.g., Azure Support Engineer, Azure Administrator).

- Experience in customer support or technical helpdesk environments, particularly for cloud-based solutions.

8. Quality Control

Ensuring the high performance, security, and reliability of the CAFI PES tool hosted on Microsoft Azure is essential for the successful operation and long-term sustainability of the platform. To achieve this, a robust Quality Assurance (QA) plan will be implemented, covering performance metrics, monitoring tools, and thorough testing processes.

Aspect	Description	Tools and Processes
Performance Metrics	- Uptime: 99.9% - Latency: <500ms - Data Integrity: 100% accuracy	- Azure Monitor - Application Insights
Security Standards	- Encryption (AES-256, TLS) - IAM, MFA - Compliance (GDPR, ISO 27001)	- Azure Security Center - Automated security audits
Monitoring	- Continuous monitoring of performance and security - Real-time alerts	- Azure Monitor - Azure Security Center - Automated alerts
Testing	- Functional, Load, Stress, Security, UAT - Comprehensive validation	- Penetration testing - Load and stress testing tools
Reporting	- Monthly reports on performance, security, and compliance	- System performance reports - Security incident reports

This chapter outlines the measures that will be taken to guarantee quality throughout the lifecycle of the hosting assignment, from initial deployment to ongoing operations.

8.1 Quality Assurance Plan

The Quality Assurance (QA) plan ensures that the cloud hosting environment meets the required performance, reliability, and security standards. The following key aspects will be the focus of the QA plan:

1. **Performance Metrics:** The CAFI PES tool must meet the following performance metrics to ensure a high-quality user experience:

    o **Uptime:** The production environment must maintain an uptime of at least 99.9% to ensure that the tool is consistently available to users.

    o **Latency:** The system must maintain low latency, with an average response time of less than 500 milliseconds for end-users, ensuring smooth navigation and interaction.

    o **Data Integrity:** All data handled by the PES tool must be accurate and free of corruption. Automated tools will monitor the consistency and integrity of the data throughout the cloud environment.

2. **Security Standards:** Security is paramount for the CAFI PES tool, given the sensitivity of the data it handles. The following security standards will be enforced:

    o **Encryption:** All data at rest and in transit must be encrypted using industry-standard encryption protocols (AES-256 and TLS).

    o **Identity and Access Management (IAM):** Role-based access control (RBAC) and multi-factor authentication (MFA) will be enforced to limit access to authorized personnel only.

    o **Compliance:** The hosting environment must comply with all relevant legal and regulatory requirements, such as GDPR and ISO 27001.

3. **Reliability and Redundancy:** The cloud infrastructure will be designed for redundancy, with automatic failover mechanisms in place to ensure the system remains operational in the event of any hardware or software failures. Data replication across multiple regions (Africa and Europe) will provide additional resilience and reliability.

4. **Scalability and Resource Optimization:** The QA plan will also include provisions for scalability, ensuring that the system can automatically adjust to increased data volumes and user activity without compromising performance. Automated scaling mechanisms will be regularly tested to ensure that resource allocation meets the system's demands.

8.2 Monitoring

Continuous monitoring is essential for maintaining the performance and security of the CAFI PES tool. Automated tools will track system performance, data security, and compliance in real-time. The following monitoring measures will be implemented:

1. **Performance Monitoring:** Azure's built-in monitoring tools, such as **Azure Monitor** and **Application Insights**, will continuously track system performance. These tools will provide real-time insights into key performance metrics, including:

   o **CPU and Memory Usage:** Monitoring resource utilization to ensure optimal performance.

   o **Network Traffic:** Tracking incoming and outgoing traffic to detect potential bottlenecks or anomalies.

   o **Response Times:** Measuring latency and identifying any slowdowns in the system.

2. **Security Monitoring:** Azure Security Center will monitor potential security threats, unauthorized access attempts, and vulnerabilities in real time. This includes:

   o **Threat Detection:** Continuous analysis of system logs to detect suspicious activity or potential breaches.

   o **Compliance Monitoring:** Regular checks ensure the system complies with all relevant security and regulatory standards (e.g., GDPR, ISO 27001).

3. **Automated Alerts and Notifications:** Automated alerts will be set up to notify the support team in real time if any performance, security, or compliance issues arise. These alerts will allow for immediate intervention to prevent disruptions or security breaches.

4. **Regular Reporting:** The provider will generate and submit reports to CAFI, detailing system performance, security incidents, and compliance status. These reports will be provided every month and will include:

   o Uptime and downtime statistics.

   o Performance metrics (latency, response times, resource usage).

   o Any security incidents and the actions taken to resolve them.

   o System updates and optimizations performed during the reporting period.

8.3 Testing and Validation

Comprehensive testing and validation are critical to ensuring the reliability of the CAFI PES tool before it goes live in the production environment. Testing will occur during the staging phase and focus on functionality and performance. The following testing processes will be conducted:

1. **Functional Testing:** Functional testing will ensure that all aspects of the PES tool work as intended, including its five core modules (Administration, Admission, Monitoring, Reporting, Map Viewer). This will involve:

   o Testing user workflows ensures users can interact with the system as expected.

   o Verifying that all integrations (e.g., data sources, third-party services) function correctly.

   o Confirming that data input, processing, and reporting mechanisms work seamlessly across all modules.

2. **Load and Stress Testing:** Load testing will simulate high traffic and usage conditions to ensure that the system can handle increased user activity without performance degradation. Stress testing will push the system beyond its expected capacity to identify any potential points of failure.

   o **Load Testing:** Simulating high numbers of concurrent users to ensure the system remains stable and responsive.

   o **Stress Testing:** Testing the system's limits by overwhelming it with large data sets and extreme user activity to determine how it responds under pressure.

3. **Security Testing:** Security testing will ensure that the system is protected from potential threats and that sensitive data remains secure. This will include:

   o **Penetration Testing:** Simulating cyberattacks to identify system security protocol vulnerabilities.

   o **Data Privacy Testing:** Verifying that all data encryption mechanisms (both at rest and in transit) are working as required.

4. **User Acceptance Testing (UAT):** CAFI stakeholders will conduct user acceptance testing to ensure that the system meets their expectations and requirements. Feedback from UAT will be used to make any final adjustments before the tool is deployed to the production environment.

5. **Validation:** After completing all testing, a final validation process will be conducted to ensure the system is ready for production deployment. This will include:

   o Verifying that all performance metrics (uptime, latency, data integrity) meet the required standards.

   o Confirming that all identified issues during testing have been resolved.

   o Ensuring that the system is secure, compliant, and fully functional.

This quality control plan ensures that the CAFI PES tool will be deployed with high reliability, performance, and security. The comprehensive QA processes, continuous monitoring, and rigorous testing will ensure that the tool meets CAFI's requirements and maintains its integrity in a live production environment.

9. Deliverables

The successful completion of the CAFI PES cloud hosting project will require the delivery of key outputs that demonstrate the hosting environment's setup, security, and operational readiness. These deliverables will provide CAFI with full transparency regarding the system configuration, performance, and compliance with security standards. Below are the detailed deliverables that the selected service provider will be required to deliver during and after the assignment.

9.1 Fully Operational Azure Account Configured to CAFI Specifications

Description: A fully functional Microsoft Azure cloud account will be set up and configured to meet the specific needs of the CAFI PES tool. This includes establishing three distinct environments (Development, Staging, and Production) and configuring all necessary virtual networks, databases, storage solutions, and security protocols.

Key Features:

- Separate development, staging, and production environments, with resource allocation tailored to each environment's needs.
- Automated scaling configurations to support performance optimization as data volumes and user loads grow.
- Virtual machines, databases, and storage solutions are provisioned according to project requirements.
- Role-based access control (RBAC) and multi-factor authentication (MFA) are implemented for enhanced security.
- Initial load balancers and firewalls set up to ensure traffic management and network security.

Completion Criteria: The cloud infrastructure is fully functional, scalable, and ready to deploy the CAFI PES tool in each of its environments.

9.2 Documentation of Account Setup with Full Configuration Details

Description: The service provider will deliver a comprehensive document detailing the configuration of the Microsoft Azure account. This documentation will serve as a reference for the CAFI technical team, outlining all cloud resources, configurations, and settings to facilitate ongoing management and troubleshooting.

Key Components of the Documentation:

- **Account Structure:** The Microsoft Azure account overview includes the hierarchical structure of resource groups and subscriptions.
- **Environment Setup:** Details of the Development, Staging, and Production environments, including virtual machines, storage allocations, and network configurations.
- **Security Configurations:** Detailed description of the security protocols implemented, such as encryption methods, IAM policies, and MFA configurations.
- **Scaling and Monitoring:** Documentation of scaling mechanisms (e.g., auto-scaling) and the monitoring tools to track performance and security.
- **Backup and Disaster Recovery:** Description of data backup processes and disaster recovery solutions, including replication to European regions for resilience.

Completion Criteria: The documentation provides complete transparency into the account setup, enabling CAFI's team to manage and maintain the environment with minimal external support.

9.3 Support and Monitoring Reports at Predefined Intervals

Description: The service provider will deliver regular reports on the system's performance, security, and operational status. These reports will provide an overview of key metrics and activities, ensuring that CAFI remains informed about the cloud environment's ongoing health and performance.

Key Components of the Reports:

- **Performance Metrics:** Uptime statistics, latency measurements, and resource utilization across all environments.
- **Security Incidents:** Summary of any security threats detected and resolved, including failed login attempts, data breaches, or unauthorized access.
- **System Health:** Insights into the status of virtual machines, databases, and storage resources, including any optimizations or adjustments made to maintain performance.
- **Billing and Usage:** Overview of monthly usage and associated costs, with recommendations for cost-saving measures if necessary.

Reporting Schedule:

- **Monthly Reports:** Delivered at the end of each month, summarising system performance, incidents, and resource usage.
- **Ad-hoc Reports:** Provided upon request if critical incidents or performance issues need immediate attention.

Completion Criteria: Monthly reports are delivered on time and contain detailed insights into system health, security, and cost management.

9.4 Security Compliance Certificate

Description: The service provider will ensure that the Azure hosting environment meets the highest security and compliance standards. Upon completion of the system setup, the provider will deliver a Security Compliance Certificate, demonstrating that all security standards have been implemented and that the environment complies with relevant legal and regulatory requirements.

Security Measures Covered:

- **Data Encryption:** Certification that all data, both at rest and in transit, is encrypted using industry-standard encryption protocols (AES-256 and TLS).
- **Identity and Access Management:** Certification that IAM policies are in place and MFA is enforced for all users accessing the system.
- **Compliance with Regulations:** The hosting environment complies with international standards such as **GDPR**, **ISO 27001**, and **SOC 2**, ensuring that the CAFI PES tool meets global data privacy and security standards.

Completion Criteria: The Security Compliance Certificate is issued after a thorough security audit, verifying that the cloud environment complies with all relevant standards and safeguards.

10. Payment Schedule

The payment schedule for the CAFI PES tool cloud hosting project will be structured around the successful completion of key project milestones. This ensures that payments are directly tied to the delivery of essential deliverables and the achievement of critical project objectives.

Milestone	Deliverables	Payment
Milestone 1: Account Setup and Initial Configuration	- Azure account setup and configuration - Virtual networks, VMs, and storage provisioned - Security setup completed	20%
Milestone 2: Testing and Validation in Staging	- CAFI PES tool deployed in staging - All testing completed - Validation reports delivered	40%
Milestone 3: Production Deployment and First Month of Support	- Production deployment completed - First month of operational support - Monthly report delivered	30%
Milestone 4: 12-Month Performance Review	- 12-month performance review - Monthly support and monitoring reports	10%

The schedule is designed to enable CAFI to ensure that the service provider meets performance expectations before payments are made.

10.1. Milestone 1: Account Setup and Initial Configuration (20%)

Description: The first payment milestone will be tied to the successful setup and initial configuration of the Microsoft Azure account. This includes providing **Once CAFI has reviewed and approved the deliverables, 20%** of the total contract value will be released upon successful completion of the account setup and initial configuration **of Once CAFI has reviewed and approved the deliverables, 20% of the total contract value will be released upon successful completion of the account setup and initial configuration**all necessary cloud resources for the Development, Staging, and Production environments, as well as the implementation of basic security configurations and access controls.

Deliverables:

- A fully operational Microsoft Azure account configured for CAFI's specific needs.
- Initial setup of virtual machines, storage, and networks.
- Role-based access control (RBAC) and multi-factor authentication (MFA) implementation.
- Documentation of the initial setup.

Payment:

- **20%** of the total contract value will be released upon successful completion of the account setup and initial configuration, once CAFI has reviewed and approved the deliverables.

10.2. Milestone 2: Testing and Validation in the Staging Environment (40%)

Description: The second payment milestone will be based on successfully deploying the CAFI PES tool in the staging environment and completing all necessary testing and validation. This stage includes load, security, and functional testing to ensure that the system meets performance, security, and compliance requirements.

Deliverables:

- CAFI PES tool deployed in the staging environment.

- Functional, load, stress, and security tests completed with detailed reports.

- All identified issues resolved, and the system validated for production deployment.

- Full documentation of the staging environment configuration and testing results.

Payment:

- **40%** of the total contract value will be released upon the successful completion of testing and validation in the staging environment, pending CAFI's approval of the test results and validation reports.

10.3. Milestone 3: Production Deployment and First Month of Operational Support (30%)

Description: The third payment milestone will be tied to successfully deploying the CAFI PES tool in the production environment. Additionally, the service provider must complete the first month of operational support, ensuring that the system is stable, secure, and performing as expected for end-users.

Deliverables:

- CAFI PES tool successfully deployed in the production environment.

- Performance monitoring and security measures fully operational.

- End-user access to the production environment validated.

- The first month of support and monitoring completed, with the delivery of a monthly performance and security report.

Payment:

- **30%** of the total contract value will be released after the successful deployment to the production environment and the first month of operational support following CAFI's approval of the deliverables.

10.4. Milestone 4: 12-Month Review of System Performance and Ongoing Support (10%)

Description: The whole final payment milestone will be released after a 12-month review of the system's performance and support services. The payment of this milestone will be made gradually, month by month, until the full amount is reached at the end of 12 months (10% of the contractual amount). This includes an evaluation of the system's uptime, security, scalability, and overall performance and assessing the service provider's ability to deliver ongoing support and monitoring services.

Deliverables:

- 12-month performance and security review, demonstrating compliance with agreed performance metrics (uptime, latency, data integrity, etc.).

- Evidence of successful ongoing support and issue resolution over the 12 months.

- Monthly reports submitted on time throughout the 12 months.

Payment:

- **10%** of the total contract value will be released upon completing the 12-month performance review following CAFI's approval of the system's ongoing operational performance and support services.

11. Technical Information for the PES Tool

The CAFI PES tool requires distinct configurations for the Development, Staging, and Production environments. Each environment has unique technical requirements that ensure optimal performance, security, and scalability while supporting the PES tool's operations.

11.1 Storage Requirements (per environment: Development, Staging, Production)

Each environment has a different storage configuration tailored to its specific needs. Below is a summary of the storage requirements based on the technical estimates.

- **CAFI Dev (Development Environment):**
  - **Storage Accounts:** Block Blob Storage, General Purpose V2 with LRS (Locally Redundant Storage) redundancy. Includes 100 GB of capacity with operations to handle 10,000 write operations and 10,000 read operations.
  - **Additional Storage Services:** Table Storage and Queue Storage have a 100 GB capacity and support table-based operations and message queue operations.

- **CAFI Staging (Staging Environment):**
  - **Storage Accounts:** Similar to the development environment with Block Blob Storage, General Purpose V2, and LRS redundancy, this account has a 100 GB capacity for staging purposes and supports operations such as write, list and read.
  - **Additional Storage Services:** Table Storage and Queue Storage are used for transactional data processing and testing. Staging environments are designed to replicate production usage, enabling thorough performance validation.

- **CAFI Production (Production Environment):**
  - **Storage Accounts:** Block Blob Storage in General Purpose V2, with LRS redundancy for production-scale operations. It includes a 100 GB capacity for data storage and transactional operations and is configured for higher data throughput.
  - **Additional Storage Services:** Table Storage and Queue Storage are also implemented to handle operational data, message queues, and transaction-heavy workloads in the live production environment.

11.2 Compute Resources

The compute requirements for each environment are defined based on the operational needs of the CAFI PES tool, ensuring that the tool performs optimally in development, testing, and production.

- **CAFI Dev (Development Environment):**
  - **App Service:** Basic Tier with two cores, 3.5 GB RAM, and 10 GB storage, designed for low-impact development work.
  - **Functions:** Premium Tier functions with one core, 4 GB RAM, and 250 GB storage, which are used for automated processes and serverless operations in development.
  - **Virtual Machines:** Provisioned for automated testing with two cores, 4 GB RAM, and 270 hours of pay-as-you-go compute time.

- **CAFI Staging (Staging Environment):**

    - **App Service:** Basic Tier with similar configurations to the development environment, used for replicating production workloads in a testing environment.

    - **Functions:** Premium Tier functions with one core, 4 GB RAM, and 250 GB storage for staging workflows and validation.

    - **Virtual Machines:** Provisioned as jump-hosts for testing staging configurations and running pre-production workloads, with 2 cores and 4 GB RAM.

    - **Additional Virtual Machines:** Virtual machines dedicated to Kobo operations, used for performance testing of critical modules.

- **CAFI Production (Production Environment):**

    - **App Service:** Premium Tier with two cores, 8 GB RAM, and 250 GB storage to handle live production operations.

    - **Functions:** Premium-tier functions are provisioned for production with one core, 4 GB RAM, and 250 GB storage to manage automated workflows in real-time.

    - **Virtual Machines:** Jump-host virtual machines are provisioned for production-level operations and optimized for continuous live use with scalable computing resources.

    - **Additional Virtual Machines:** Dedicated machines for Kobo and other core services in the production environment, with 2 cores and 4 GB RAM, configured for uninterrupted, high-availability operations.

11.3 Databases

The CAFI PES tool relies on Azure Database for PostgreSQL to handle structured data across all environments. Each environment's database configuration ensures scalability, data integrity, and reliable transaction processing.

- **CAFI Dev (Development Environment):**

    - **PostgreSQL (App):** Flexible Server Deployment with a single core, 5 GB storage, and burstable computing capacity for development tasks.

    - **PostgreSQL (Keycloak):** This database, which manages user authentication and authorization through Keycloak services, has a similar configuration to the app database.

- **CAFI Staging (Staging Environment):**

    - **PostgreSQL (App):** Flexible Server Deployment with burstable compute resources, a single core, and 5 GB storage designed to handle pre-production validation.

    - **PostgreSQL (Keycloak):** The same configuration for handling authentication processes in staging, ensuring smooth user access and secure identity management during testing.

- **CAFI Production (Production Environment):**

    - **PostgreSQL (App):** High-performance configuration with 2 vCores and 5 GB storage, ensuring reliable and fast data processing for live operations.

    - **PostgreSQL (Keycloak):** Enhanced configuration for user management and authentication services in a live production environment, supporting secure user logins and session management.

11.4 Backup and Disaster Recovery Solutions

Backup and disaster recovery mechanisms are implemented across all environments to maintain system availability and protect data.

- **Backup Services:** Daily automated backups of data and virtual machines in all environments using Azure's Backup services. Backups are stored using LRS redundancy in development and staging, with both LRS and GRS (Geo-Redundant Storage) in production to ensure data resiliency.

- **Disaster Recovery:** Data replication from production in South Africa North to backup regions in North Europe to ensure recovery capabilities in case of data center outages. Azure's Site Recovery service ensures that the PES tool can be restored quickly with minimal data loss.

11.5 Compliance with Azure's Infrastructure and Scalability

All technical configurations for storage, computing, databases, and backup solutions comply with Microsoft Azure's scalable cloud infrastructure and best practices. The CAFI PES tool is designed to scale dynamically based on actual usage, ensuring that each environment can adapt to increasing data volumes and user loads.

Azure's cost management tools will ensure the system's operations remain cost-effective while meeting CAFI's performance and availability requirements. This ensures the system can scale seamlessly while remaining within budgetary constraints significantly as the PES tool expands its user base and integrates with additional data sources.

12. Organization Profile and Requirements

The successful execution of the CAFI PES tool's hosting on Microsoft Azure requires a service provider with extensive experience in delivering cloud-based solutions, mainly using Microsoft Azure's infrastructure. The provider must demonstrate a proven track record of managing, deploying, and supporting large-scale cloud environments focusing on security, scalability, and compliance with at least one certificate of service completion within the last five years. Additionally, the provider must adhere to international standards for cloud infrastructure, security, and data management to ensure the system's integrity, performance, and legal compliance.

12.1 Proven Track Record in Delivering Azure-based Solutions

The service provider must have substantial experience managing Microsoft Azure environments, with a portfolio of successful projects demonstrating expertise in deploying and maintaining Azure-based solutions. The following criteria will reinforce the provider's credibility and qualifications:

1. **Azure Expertise and Certifications**

   o The service provider must possess **Microsoft Certified Partner status**, showcasing their proficiency in Azure-related services.

   o The team must include certified professionals with expertise in Azure solutions, such as **Azure Solutions Architects**, **Azure Security Engineers**, and **Azure Administrators**.

   o The provider must have implemented Azure solutions for organizations of similar scale and complexity, particularly for clients in the public sector, environmental initiatives, or financial systems like the PES tool.

2. **Relevant Project Experience**

   o The provider should present case studies or project references demonstrating their experience in delivering cloud solutions that involve multi-environment deployments (Development, Staging, and Production).

o Preference will be given to service providers who have experience with projects involving **data-heavy applications**, real-time processing, and high-availability systems.

o The ability to manage both **infrastructure as a service (IaaS)** and **platform as a service (PaaS)** solutions will be a key factor in evaluating the provider's suitability for hosting the CAFI PES tool.

3. **Scalability and Performance Optimization**

o It is essential to demonstrate a track record in optimising Azure environments for scalability and performance. The provider must show experience configuring auto-scaling, load balancing, and resource optimization to support growing user bases and increasing data volumes.

o Experience with handling cross-region data replication and failover strategies to ensure service reliability and minimal downtime will be a significant advantage.

12.2 Compliance with International Standards for Cloud Infrastructure, Security, and Data Management

Given the sensitive nature of the data handled by the CAFI PES tool and the project's global reach, the selected service provider must comply with a range of international standards for cloud infrastructure, security, and data management. Compliance ensures that the system operates within legal frameworks and meets the highest data protection and security standards.

1. **Cloud Infrastructure Standards**

o The provider must comply with global standards for **cloud infrastructure** design and management, ensuring the system is robust, reliable, and scalable. Adherence to **ISO/IEC 27001** (Information Security Management) is required to guarantee that the system's cloud infrastructure meets international security and risk management practices.

o Compliance with **ISO/IEC 27017** (Code of Practice for Cloud Security) is also required to ensure the service provider employs best practices for cloud-specific security controls.

2. **Security Compliance and Data Protection:** The CAFI PES tool processes sensitive environmental, financial, and user data, necessitating strict adherence to security and data protection regulations. The service provider must ensure compliance with the following security standards:

o **General Data Protection Regulation (GDPR):** Ensuring that personal data is processed following European data privacy laws, particularly for any data involving EU-based users or stakeholders.

o **ISO/IEC 27018** (Protection of Personally Identifiable Information in Public Cloud): This standard must be followed to ensure the provider protects all personal data in the cloud environment.

o **ISO/IEC 27032** (Cybersecurity): This provides a guideline for protecting data and services from cybersecurity risks and threats. The provider must have a cybersecurity framework to detect and prevent potential attacks.

3. **Data Management Standards**

o **Data Sovereignty and Residency:** The provider must ensure data storage complies with local regulations, particularly regarding **data residency** requirements for CAFI's partner countries. For example, production data must be hosted in **South Africa North** with replication in **North Europe**, ensuring compliance with data sovereignty laws in African and European jurisdictions.

o **Data Integrity and Availability:** Adherence to **ISO/IEC 22301** (Business Continuity Management) to ensure that the CAFI PES tool remains available even during disruptions or failures. This includes implementing disaster recovery and backup strategies that align with international best practices for data availability.

4. **Security and Privacy by Design**

   o The provider must adopt a **Security by Design** approach, ensuring security is embedded throughout the system's lifecycle—from initial design to deployment and ongoing maintenance. This includes identity and access management (IAM), encryption protocols (AES-256, TLS), and regular vulnerability assessments.

   o **Privacy by Design** must also be a priority, ensuring that personal data is handled with the highest degree of privacy protection.

5. **Continuous Monitoring and Auditing**

   o The service provider must implement **continuous monitoring** of the cloud environment using Azure's built-in tools (e.g., Azure Monitor, Azure Security Center) to ensure real-time detection of security threats, system anomalies, and performance bottlenecks.

   o Regular **audits and compliance checks** must be conducted to ensure the system remains aligned with international security and data management standards, particularly as the PES tool scales and integrates with additional services and data sources.

13. Quotation Requirements

The quotation submitted by bidders for the CAFI PES tool hosting project must provide a comprehensive response that clearly outlines the service provider's understanding of the project requirements, their proposed approach, and an itemized budget. The quotation must demonstrate the provider's capability to deliver a secure, scalable, and compliant hosting solution, along with detailed information regarding their experience and expertise.

Bidders are required to include the following key components in their submission:

13.1 Narrative Response to the ToR

The bidder should provide a clear and concise narrative response that demonstrates their understanding of the Terms of Reference (ToR). This response must include the following:

● An explanation of the bidder's approach to meeting the project's objectives, focusing on the setup, security, scalability, and management of the cloud hosting environment for the CAFI PES tool.

● A discussion of how the bidder will ensure compliance with the technical requirements specified in the ToR, including storage, compute resources, data management, and disaster recovery.

The narrative response should also emphasize the bidder's previous experience with similar projects and showcase their ability to deliver on key performance metrics, including uptime, security, and data integrity.

13.2 Detailed Methodological Approach

Bidders must present a detailed methodological approach that outlines the steps they will take to deliver the project. This should include:

- **Cloud Environment Setup:** Description of how the Microsoft Azure environments (Development, Staging, and Production) will be configured and managed. The provider should explain the technical processes in provisioning virtual machines, setting up networks, databases, and storage, and implementing security protocols.

- **Security and Compliance Measures:** A clear explanation of the security measures that will be put in place, including encryption, identity and access management (IAM), multi-factor authentication (MFA), and adherence to international security standards (GDPR, ISO/IEC 27001, etc.).

- **Scalability and Performance Optimization:** An outline of how the system will scale dynamically based on usage, data volumes, and user loads. This section should also include methods for optimizing performance to ensure low latency and high availability.

- **Backup and Disaster Recovery Plan:** A detailed explanation of how data will be backed up and how the disaster recovery solution will function in case of system failure. This should include the bidder's approach to data replication across Azure regions to ensure resilience.

The methodological approach must provide a step-by-step breakdown of how the bidder plans to meet each of the project's technical, security, and operational requirements.

13.3 Assumptions and Risks

Bidders are required to identify and articulate any assumptions that have been made regarding the project's requirements and deliverables. This should include:

- **Assumptions about Data Volumes:** Expected data growth and user load assumptions that influence the hosting configuration.

- **System Integrations:** Assumptions regarding the integrations with external systems and third-party APIs.

- **Performance Expectations:** Assumptions about expected system performance, including uptime, latency, and response times.

Additionally, bidders must provide a comprehensive risk assessment outlining potential risks associated with the project and the strategies they will use to mitigate them. These risks may include:

- **Security Risks:** Possible cybersecurity threats and how they will be addressed.

- **Data Loss and Downtime:** Risks related to system outages, data loss, or backup failures, and the mitigation strategies in place to minimize these risks.

- **Scalability Risks:** Any challenges related to system scalability as the project grows and how the provider plans to handle increasing demand.

13.4 Detailed Work Plan with Timelines

Bidders must submit a detailed work plan that outlines the key tasks and deliverables for each phase of the project. The work plan should include:

- **Inception and Mobilisation:** Setting up the Azure account and provisioning resources in the first week.

- **Development Phase:** Configuring the Development, Staging, and Production environments over weeks 2-3.

- **Staging and Testing:** Deploying the CAFI PES tool in the staging environment and conducting testing (functional, load, security) during weeks 4-6.

- **Production Deployment:** Deploying the PES tool in the production environment and providing operational support from weeks 7-8 onward.

- **Ongoing Support and Monitoring:** Providing continuous monitoring, system optimization, and support throughout the initial 12-month period.

The work plan must include specific timelines for each milestone, clearly outlining when each deliverable is expected to be completed. The timelines should align with the execution timeline outlined in the ToR.

13.5 Two Years of Experience in Cloud Hosting (Preferably with Public Sector Clients)

The bidder must provide evidence of their experience in cloud hosting, mainly using Microsoft Azure, over the past two years. Experience with public sector clients is highly preferred due to the complexity and regulatory requirements typically involved in government projects.

The submission should include:

- **Project References:** Descriptions of at least two relevant projects where the bidder has delivered cloud-based hosting solutions on Azure. These descriptions should highlight the project scope, technical requirements, and outcomes.

- **Client Testimonials:** Testimonials from previous or existing clients demonstrate the bidder's ability to deliver high-quality, secure, and scalable cloud solutions.

- **Public Sector Experience (Preferred):** Any experience working with public sector clients, particularly on projects involving environmental or financial systems, should be highlighted.

13.6 Budget

The bidder must provide a detailed and itemized budget for the entire duration of the project. This budget must include:

- **Setup Costs:** A breakdown of costs for setting up the cloud environment, including the provisioning of virtual machines, databases, storage, and security configurations.

- **Support and Monitoring Costs:** Ongoing support, monitoring, and maintenance costs over the initial 12-month period. This should include performance optimization, security monitoring, and technical support costs.

- **Cost Control Measures:** Any proposed measures to optimize costs, such as leveraging Azure's auto-scaling features to minimize unnecessary resource usage or optimizing storage solutions based on data access patterns.

- **Contingency Costs:** A contingency budget to address unforeseen issues or system requirements that may arise during the project.

Bidders are expected to present a clear cost breakdown that aligns with the scope of work outlined in the ToR. The budget must be transparent and include all expenses required to meet the project's objectives without hidden costs or ambiguities.