REQUEST FOR PROPOSALS

for

Systems Administration Services – Microsoft Technologies

[SUP-WIN-2026]

Information and Communications Technology Services

International Training Centre of the ILO (ITCILO)

May 2026

Contents

Section 1: General information

DATA SHEET

No.	Data	Specific Instructions / Requirements
1	RFP Title	Systems Administration Services – Microsoft Technologies (ref. SUP-WIN-2026)
2	Place of Work	Remote
3	Start of contract	1 November 2026
4	Duration of contract	2+2
5	Language of the Proposal	English
6	Proposal Validity (from submission date)	120 days
7	Currency of Proposal	Euro (EUR)
8	Requests for clarifications - deadline	**15 June 2026**
9	Requests for clarifications - contact	**icts@itcilo.org**
10	Submission deadline	**30 June 2026 23.59 CET**
11	Submission contact	**contracts@itcilo.org**

DEFINITIONS

a) *"Contract"* refers to the agreement that will be signed by and between the International Training Centre of the ILO ("the Centre") and the successful proposer, all the attached documents thereto, and including the Terms and Conditions and the Appendices.

b) *"Instructions to Proposers"* (Section 1 of the RFP) refers to the complete set of documents that provides Proposers with all the needed information and procedures to be followed in the course of preparing their Proposals.

c) *"LOI"* (Section 1 of the RFP) refers to the Letter of Invitation sent by ITCILO to Proposers.

d) *"Material Deviation"* refers to any contents or characteristics of the proposal that is significantly different from an essential aspect or requirement of the RFP, and: (i) substantially alters the scope and quality of the requirements; (ii) limits the rights of the Centre and/or the obligations of the Proposer; and (iii) adversely impacts the fairness and principles of the procurement process, such as those that compromise the competitive position of other Proposers.

e) *"Proposal"* refers to the Proposer's response to the Request for Proposal, including the Technical and Financial Proposal, and all other documentation attached thereto as required by the RFP.

f) *"Proposer"* refers to any legal entity that may submit, or has submitted, a Proposal for the provision of services requested by the Centre through this RFP.

g) *"RFP"* refers to the Request for Proposals consisting of instructions and references prepared by the Centre for purposes of selecting the best service provider to perform the services described in the Statement of Work.

h) *"Services"* refers to the entire scope of tasks and deliverables requested by the Centre under the RFP.

i) "*Supplemental Information to the RFP"* refers to a written communication issued by the Centre to prospective Proposers containing clarifications, responses to queries received from prospective Proposers, or changes to be made in the RFP, at any time after the release of the RFP but before the deadline for the submission of Proposals.

j) *"Statement of Work"* (SOW) refers to the document included in this RFP as Section 2 which describes the objectives, scope of services, activities, tasks to be performed, respective responsibilities of the proposer, expected results and deliverables, and other data pertinent to the performance of the range of duties and services expected of the successful proposer.

GENERAL INFORMATION

1. The Centre invites proposers to submit proposals in response to this Request for Proposal (RFP) to establish a contract for the provision of services as described in the SOW covering an initial period of two (2) years, renewable for an additional two- year period (2+2) subject to availability of funds and satisfactory performance.
2. Proposers must strictly adhere to all the requirements of this RFP. No changes, substitutions or other alterations to the rules and provisions stipulated in this RFP may be made or assumed unless it is instructed or approved in writing by the Centre in the form of Supplemental Information to the RFP.
3. Submission of a Proposal shall be deemed as an acknowledgement by the Proposer that all obligations stipulated by this RFP will be met and, unless specified otherwise, the Proposer has read, understood, and agreed to all the instructions in this RFP.
4. Any Proposal submitted will be regarded as an offer by the Proposer and does not constitute or imply the acceptance of any Proposal by the Centre. The Centre is under no obligation to award a contract to any Proposer as a result of this RFP. Furthermore, the Centre may contract for works or services of the same or similar kind and quality described in the RFP from any other source at any time.
5. In responding to this RFP, the Centre requires all Proposers to conduct themselves in a professional, objective, and impartial manner, and they must at all times hold the Centre's interests paramount. Proposers must strictly avoid conflicts with other assignments or their own interests, and act without consideration for future work. All Proposers found to have a conflict of interest shall be disqualified. Without limitation on the generality of the above, Proposers, and any of their affiliates, shall be considered to have a conflict of interest with one or more parties in this solicitation process, if they:
    - 5.1 Are or have been associated in the past, with a firm or any of its affiliates which have been engaged by the Centre to provide services for the preparation of the design, specifications, Statement of Work, cost analysis/estimation, and other documents to be used for the procurement of the goods and services in this selection process;
    - 5.2 Were involved in the preparation and/or design of the programme / project related to the services requested under this RFP; or
    - 5.3 Are found to be in conflict for any other reason, as may be established by, or at the discretion of, the Centre.

In the event of any uncertainty in the interpretation of what is potentially a conflict of interest, proposers must disclose the condition to the Centre and seek the Centre's

confirmation on whether or not such conflict exists.

6. Similarly, the Proposers must disclose in their proposal their knowledge of the following:
   6.1 That they are owners, part-owners, officers, directors, controlling shareholders, or that they have key resources who are family or relations of the Centre's staff involved in the procurement functions and/or the Government of the country, or any Implementing Partner receiving services under this RFP; and
   6.2 All other circumstances that could potentially lead to actual or perceived conflict of interest, collusion or unfair competition practices. Failure of such disclosure may result in the rejection of the proposal or proposals affected by the non-disclosure.

PREPARATION OF PROPOSAL

1. Sections of Proposal

Proposers are required to complete, sign and submit the following documents:

- Technical Proposal;
- Financial Proposal;
- General Conditions of Contracts (Annex 1);
- Non-Disclosure agreement (Annex 2).

The proposer shall submit copies of the "General Conditions of Contract" and the "Non-Disclosure agreement", signed and stamped by their legal representative. The signature and stamp confirm the Proposer's understanding and acceptance of the "General Conditions of Contract".

2. Clarifications

2.1 Proposers may request clarification of any of the RFP documents no later than the date indicated in the Data Sheet prior to the proposal submission date. Any request for clarification must be sent in writing through electronic means to the Centre address indicated in the Data Sheet. The Centre will respond in writing, transmitted by electronic means, and will transmit copies of the response (including an explanation of the query but without identifying the source of inquiry) to all Proposers who have provided confirmation of their intention to submit a Proposal.

2.2 The Centre shall endeavor to provide such responses to clarifications in an expeditious manner, but any delay in such response shall not cause an obligation on the part of the Centre to extend the submission date of the Proposals, unless the

Centre deems that such an extension is justified and necessary.

3. Amendment of Proposals

3.1 At any time prior to the deadline of Proposal submission, the Centre may for any reason, such as in response to a clarification requested by a Proposer, modify the Data Sheet in the form of Supplemental Information to the RFP. All prospective Proposers will be notified in writing of all changes/amendments and additional instructions through Supplemental Information to the RFP.

3.2 To afford prospective Proposers reasonable time to consider the amendments in preparing their Proposals, the Centre may, at its discretion, extend the deadline for submission of Proposals, if the nature of the amendment to the RFP justifies such an extension.

4. Cost

The Proposer shall bear any and all costs related to the preparation and/or submission of the Proposal, regardless of whether its Proposal is selected or not. The Centre shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the procurement process.

5. Language

The Proposal, as well as any and all related correspondence exchanged by the Proposer and the Centre, shall be written in the languages specified in the RFP. Any printed literature provided by the Proposer written in a language other than the language(s) indicated in the RFP, must be accompanied by a translation in the preferred language(s) indicated in the RFP. For purposes of interpretation of the Proposal, and in the event of discrepancy or inconsistency in meaning, the version translated into the required language(s) shall govern. Upon conclusion of a contract, the language of the contract shall govern the relationship between the contractor and the Centre.

CONTENT OF PROPOSAL

6. Technical Proposal

Unless otherwise stated, the Proposer shall structure the Technical Proposal in accordance with the sections below. Proposals shall be clear, concise, and directly address the requirements of the Statement of Work and its Annexes. Generic or purely descriptive responses without demonstrable evidence may be scored lower.

Criteria 1 (30 points): Technical Expertise

The Proposer shall demonstrate its capability to deliver services of similar scope and complexity and provides the following:

- Description of the company organization's structure, scale, and technical capacity relevant to hybrid Microsoft environments.
- Proven experience in managing comparable environments, including hybrid identity (AD–Entra ID), Microsoft 365, Citrix (or similar technologies), and infrastructure services.
- At least three (3) relevant references, including scope, duration, role (prime/subcontractor), and client contact details.
- Evidence of experience in identity governance, privileged access management, and secure administration models.
- Overview of technical tooling, platforms, and operational capabilities supporting service delivery.
- Confirmation of financial stability and capacity to sustain service delivery.
- Alignment with governance framework: Proposers shall also provide information on relevant certifications like ISO/IEC 27001, ISO 14001 or 14064 or equivalent.
- Alignment with UN principles: The Centre supports the broader goal of achieving respect of human rights, peace, equality and sustainable development. As the principles of equality and non-discrimination are central to the Centre's mission, proposers should provide evidence of policies, staff composition and/ or actions promoting gender quality, non-discrimination, diversity, and inclusion of persons with disabilities and/or underrepresented groups. Membership to the UN Global Compact will be considered an asset.

Criteria 2 (50 points): Methodology and service management

Describe how the required service will be delivered across the hybrid Microsoft environment.

The response shall include:

- Approach to managing hybrid identity (AD, Entra ID, synchronization, authentication, SSO, Conditional Access).
- Methodology for managing Microsoft 365 workloads, Azure services, and integration with on-premises systems.

- Approach to onboarding new services, applications, and workloads within the Microsoft ecosystem.
- Methodology for SaaS integration using Entra ID (e.g., SSO, authentication protocols, access policies).
- Approach to security configuration, monitoring, and compliance within Microsoft platforms.
- Lifecycle management approach, including configuration changes, service evolution, and feature enablement.

The Proposer shall clearly demonstrate how these activities are delivered as part of core operational services.

- Service Delivery Model & Continuous improvement
  The Proposer shall describe how services will be organized, delivered, monitored, and continuously improved.

  The response shall include:
  - Service organization model, including handling of planned activities, incidents, and escalations.
  - Approach to service continuity and resource backup.
  - Collaboration model with ITCILO teams.
  - Service quality management approach, including KPIs, SLAs, and reporting mechanisms.
  - Sample service reporting (e.g., quarterly service review).
  - Approach to documentation, knowledge management, and knowledge sharing.
  - Continuous improvement methodology, including how service performance and efficiency will be enhanced over time.

  Reference to recognized service management practices (e.g., ITIL) is expected where applicable.

- Governance, Security & Transition Approach
  The Proposer shall describe in detail its approach to governance, security, and the initial transition phase, in alignment with the Statement of Work and Annexes.

  The response shall include:

- A structured approach to the Transition and Discovery Phase, including documentation baseline, risk identification, and service takeover.
- Methodology for implementing Role-Based Access Control (RBAC), least privilege principles, and reduction of excessive administrative access.
- Approach to privileged access management, including use of time-bound or controlled elevation mechanisms (e.g., Privileged Identity Management / Just-In-Time (PIM/JIT) where applicable).
- Approach to ensuring that the Centre retains ultimate administrative control of systems and identities.
- Methodology for identifying and remediating security risks and vulnerabilities.
- Approach to documentation, architecture mapping, and maintaining up-to-date technical records.

Responses must clearly demonstrate governance maturity and practical implementation capability, not only conceptual understanding.

- Capacity, Scalability & Flexibility

  The Proposer shall describe its ability to adapt to evolving service requirements.

  The response shall include:
  - Approach to scaling resources during peak demand or special activities.
  - Capability to provide extended or on-call support.
  - Approach to handling new service requirements or expansion of the environment.
  - Flexibility in adapting to changing technologies and operational needs.

  The Proposer shall clearly indicate how additional capacity or services will be integrated without disruption.

  CRITERIA 3 (20 points): Management Structure and Key Resource(s)

  The Proposer shall provide details of the proposed team and governance structure.
  The response shall include:
  - Organizational structure for service delivery, including roles and responsibilities.
  - CVs of key personnel demonstrating relevant qualifications and experience aligned with the SOW.

- Identification of roles responsible for governance, security, and service quality.
- Approach to team continuity, backup, and resource replacement.
- Confirmation of availability of proposed key resources.

The Centre reserves the right to interview proposed key personnel.

7. Financial Proposal

The Financial Proposal shall list all major cost components associated with the services, and the detailed breakdown of such costs. Any output and activities described in the Technical Proposal but not priced in the Financial Proposal shall be assumed to be included in the prices of other activities or items, as well as in the final total price.

The Proposer may include additional options that would reduce the total contract amount as well as a mechanism to review the price should the volume increase / decrease. A tolerance of +10/ -10 should also be envisaged.

The financial proposal should include the quotation as follows:

- Core services during business and weekend hours: a monthly rate to keep the existing systems working optimally as requested in the SOW.
- Daily rate for additional activites such as the implementation of new systems/solutions or significative changes to existing systems .
- Transfer fee in case of on-site activities.
- Hourly rate for work outside of the business hours during the week.
- Hourly / Daily rate for extraordinary activity during the weekend and/or holidays.

Should the monthly rate be based on tickets please specify the number of tickets included.

7.1 Currencies

All prices shall be quoted in Euro.

SUBMISSION AND OPENING OF PROPOSALS

1. Submission

The Financial Proposal and the Technical Proposal **MUST BE SUBMITTED IN SEPARATE E-MAILS** with the subject indicated as either "TECHNICAL PROPOSAL" or "FINANCIAL PROPOSAL", as appropriate.

Each e-mail must clearly indicate the name of the Proposer and the RFP reference. Proposers must be aware that the mere act of submission of a Proposal, in and of itself, implies that the Proposer accepts the Terms and Conditions of the Centre (Annex 1).

Procedures for electronic submission and opening
☒ Address for e-submission: **contracts@itcilo.org** ☒ Document Format: PDF files. ☒ Max email size: 11 Mb ☒ Max nr of emails: unlimited The Proposer shall send separate proposals for: 1) technical proposal, general conditions and non-disclosure agreement signed; 2) Any technical supporting documents 3) financial proposal ☒ Mandatory subject of e-mails: **"Technical proposal" followed by the RFP Reference number** **"Technical supporting docs" followed by RFP Reference number** and a separate email with: **"Financial proposal" followed by the RFP Reference number.** Please **SET-UP A PASSWORD** for the Financial Proposal to secure the offer.

2. Deadline for Submission of Proposals and Late Proposals

Proposals must be received by the Centre at the indicated address no later than the date and time specified in the Data Sheet. The Centre shall not consider any Proposal that arrives after the deadline for submission of Proposals.

8. **Validity Period**

Proposals shall remain valid for the period specified in the RFP, commencing on the submission deadline date also indicated in the Data Sheet.

In exceptional circumstances, prior to the expiration of the proposal validity period, the Centre may request Proposers to extend the period of validity of their Proposals. The request and the responses shall be made in writing and shall be considered integral to the Proposal.

3. **Withdrawal, Substitution, and Modification of Proposals**

No Proposal may be withdrawn, substituted, or modified in the interval between the deadline for submission of Proposals and the expiration of the period of proposal validity specified by the Proposer on the Proposal Submission Form or any extension thereof.

4. **Confidentiality**

Information relating to the examination, evaluation, and comparison of Proposals, and the recommendation of contract award, shall not be disclosed to Proposers or any other persons not officially concerned with such process, even after publication of the contract award.

Any effort by a Proposer to influence the Centre in the examination, evaluation and comparison of the Proposals or contract award decisions may, at the Centre's decision, result in the rejection of its Proposal.

EVALUATION OF PROPOSALS

1. **Preliminary Examination of Proposals**

At this stage, the Centre shall verify that each proposal:

- Is complete with respect to the minimum documentary requirements.
- Covers all required annexes and declarations.
- Conforms to submission instructions and formal requirements.
- Explicitly accepts the Statement of Work and all referenced Technical Annexes as integral and binding components of the Contract.
- Contains no material deviation, exclusion, limitation, or conditional qualification affecting the core scope of services, including but not limited to all the technical annexes.

Any Proposal that:

- Seeks to exclude or materially alter governance, RBAC, documentation ownership, or administrative control provisions;
- Reclassifies the specified core operational services as out-of-scope without justification consistent with the RFP; or
- Introduces conditions that limit the Centre's ownership, oversight, or ultimate administrative control of the infrastructure shall be deemed non-responsive and may be rejected without further technical evaluation. The evaluation committee shall document any identified material deviation prior to proceeding with technical scoring.

2. Evaluation of Proposals

Phase 1: Evaluation of technical proposal

The evaluation team will review and evaluate the Technical Proposals based on the eligibility criteria and responsiveness to the Statement of Work and other documentation provided, applying the evaluation criteria and scoring system indicated below.

ELIGIBILITY CRITERIA (PASS OR FAIL)

To be eligible, The Proposer must:

- Prove execution of at least three relevant projects/contracts in the last three (3) years. At least one of those projects must include the provision of Systems Administration services to 200 users and covering the same technologies indicated in the Statement of Work.
- For each technological stack the proposer shall demonstrate to have redundancy of experts
- Assigned resources must have employment relationships with the Proposer. The Centre reserves the right to verify that status.
- Certification with the ISO/IEC 27001 (possibly 2022, if not 2013) on the services relevant to the scope of this RFP is considered an asset.

A Proposal shall be rendered non-responsive at this stage if it does not meet the eligibility criteria and does not substantially respond to the RFP, particularly the demands of the Statement of Work and if does not reach the minimum technical score of 70%.

Technical evaluation criteria

Criteria	Max Score
Criteria 1: • Experience in similar environment (size, complexity) • Organization capacity (number of staff, required technical expertise and experience). Backup capacity and ability to scale/adapt. • Adoption of recognized governance framework and service management practices. • Alignment with UN principles of sustainable development and gender balance.	**30**
Criteria 2: • Technical methodology • Service delivery model and continuous improvement services • Governance & Security and Transition • Scalability	**50**
Criteria 3: Key resource(s) and Implementation Capacity • Years of experience • Exposure to multiple projects/clients • Relevant Qualification, Expertise & Certifications	**20**
Total TP score	**100**
Min. TP score	**70**

Phase 2 Evaluation of financial proposal

Only the financial proposals of Proposers who meet the minimum technical score (70 points) will be opened for further evaluation.

Phase 3: Overall evaluation and scoring method.

The overall evaluation score will be based either on a combination of the technical score and the financial offer or the lowest evaluated financial proposal of the technically

qualified Proposers.

The rating of the Proposals will be as follows:

Rating the Technical Proposal (TP):

TP Rating = (Total Score Obtained by the Offer / Max. Obtainable Score for TP) x 100

Rating the Financial Proposal (FP):

FP Rating = (Lowest Priced Offer / Price of the Offer Being Reviewed) x 100

Total Combined Score:

(TP Rating) x 60%
+ (FP Rating) x 40%

Total Combined and Final Rating of the Proposal

The Centre reserves the right to undertake a post-qualification exercise aimed at determining, to its satisfaction, the validity of the information provided by the Proposer. Such post-qualification shall be fully documented and may include, but need not be limited to, all or any combination of the following:

a) Verification of accuracy, correctness and authenticity of information provided by the Proposer on the legal, technical and financial documents submitted;
b) Validation of extent of compliance to the RFP requirements and evaluation criteria based on what has so far been found by the evaluation team;
c) Inquiry and reference checking with governmental entities with jurisdiction over the Proposer, or any other entity that may have done business with the Proposer;
d) Inquiry and reference checking with other previous clients on the quality of performance on on-going or previous contracts completed;
e) Physical inspection of the Proposer's offices, branches or other places where business transpires, with or without notice to the Proposer;
f) Quality assessment of on-going and completed outputs, works and activities similar to the requirements of the Centre, where available; and
g) Other means that the Centre may deem appropriate, at any stage within the selection process, prior to awarding the contract.

3. Clarification of Proposals

To assist in the examination, evaluation and comparison of Proposals, the Centre may, at its discretion, ask Proposers for clarifications.

The Centre's request for clarification and the response shall be in writing. Notwithstanding the written communication, no change in the prices or substance of the Proposal shall be sought, offered, or permitted, except to provide clarification, and confirm the correction of any arithmetic errors discovered by the Centre in the evaluation of the Proposals.

Any unsolicited clarification submitted by a Proposer in respect to its Proposal, which is not a response to a request by the Centre, shall not be considered during the review and evaluation of the Proposals.

4. Responsiveness of Proposal

The Centre's determination of a proposal's responsiveness will be based on the contents of the proposal itself.

A substantially responsive proposal is one that conforms to all the terms, conditions, SOW and other requirements of the RFP without material deviation, reservation, or omission.

If a proposal is not substantially responsive, it shall be rejected by the Centre and may not subsequently be made responsive by the Proposer by correction of the material deviation, reservation, or omission.

Section 2: Statement of Work

ORGANIZATIONAL SETUP

The International Training Centre (the Centre) is the capacity development arm of the International Labour Organization (ILO). The Centre is a semi-autonomous entity under ILO oversight (but governed by its own statutes and strongly relying on earned income for financial sustainability). It offers a diversified range of capacity development services directed primarily towards ILO tripartite constituents. Through technology-enhanced, data-driven, and demand-responsive learning, the Centre empowers individuals and organizations from the ILO core constituency and from ILO development partners while fostering diversity, inclusion, and gender equality.

In this context, the Information and Communications Technology Services (ICTS) provides integrated information, communication and learning technology services to the Centre's staff, training participants and institutional clients, working closely with the corporate services and the training department.

ICTS is responsible for the design, implementation, and management of the Centre's ICT infrastructure, systems, and services, supporting both learning activities and core institutional functions. Its main areas of responsibility include:

- **Digital Collaboration tools**: from the traditional file-sharing and e-mail systems to cloud-based tools such as Microsoft Teams and OneDrive.
- **Websites and platforms**: hosting, design, development and maintenance for training activities and projects.
- **End-user support and equipment management**: comprehensive support for computer-related needs, including installation and maintenance of servers, desktop systems and software; This includes technical support for meetings and training events.
- **Core Systems and ERP applications**: develop and maintenance enterprise applications including ERP systems; Business Intelligence Solutions, and Data Management and Analytics.
- **Network infrastructure and connectivity:** secure high performance infrastructure including internet access and Wi-Fi.
- **Cybersecurity and business continuity**: ensuring protection of applications and data. It also manages policies and mechanisms for business continuity and disaster

recovery.

DESCRIPTION OF SERVICES

The team will perform the following operational activities on the systems covered by the service:

- Ensure that all systems are working in an optimal way.
- All systems must be continuously monitored, and alerts must be quickly acted upon.
- Additional monitoring alerts must be configured as needed.
- Systems must be properly backed up and verified that they can be restored.
- Application and System security updates must be installed not more than two weeks from the date of release.
- Patch critical vulnerabilities on Internet exposed systems within one working day of the patch release.
- Perform troubleshooting of issues when they arise
- Provide 2nd level of support to the Service Desk on issues raised by users
- Provide support for applications servers where third-party providers or internal applications provide application support.
- Implement configuration changes as needed.
- Produce operational reports on infrastructure usage
- Create and maintain documentation of all systems.

Contractor Responsibilities

The Contractor shall be fully responsible for the secure, reliable and continuous operation of the Centre's hybrid Microsoft and associated infrastructure environment. The services shall be delivered in accordance with the detailed scope, governance requirements and technical specifications set out in the following technical annexes:

- ANNEX 4: List of Virtual Machines.
- ANNEX 5: List of Major Changes and Tickets.
- ANNEX 6: End-user Technological Context.
- ANNEX 7: Thirty (30) - Day Transition, Discovery, Governance & Security Baseline Phase.
- ANNEX 8: Microsoft Cloud Platform & Hybrid Identity Management - Detailed Scope.

The provisions contained in the above Annexes form an integral and binding part of this Statement of Work. In the event of any ambiguity regarding the scope of services, the Annexes shall prevail in defining the Contractor's obligations.

The Contractor acknowledges that the services include not only operational maintenance but also lifecycle management, integration, security governance, documentation, and controlled administrative access as further described in the referenced Annexes.

1. **Mandatory 30-day Transition & Discovery Phase**

   Upon commencement of contract, the Contractor shall undertake a mandatory thirty (30) calendar day transition, discovery and governance reset phase. This requirement applies equally to a newly appointed contractor or to the incumbent provider if re-awarded the contract. During this phase, the Contractor shall:

   - Conduct a comprehensive technical and security review of the entire hybrid Microsoft environment (on-premises and cloud).
   - Produce a validated documentation baseline, including architecture diagrams, system inventory, configuration overview, and dependency mapping.
   - Perform a full privileged access audit covering Microsoft 365, Azure/Entra ID, Active Directory, and servers.
   - Design and implement a formal Role-Based Access Control (RBAC) model based on the principles of least privilege, segregation of duties, and named individual accountability.
   - Remove excessive or standing privileged roles (including unnecessary Global Administrator assignments) and implement controlled, role-based and where feasible time-bound administrative access for both ITCILO and Contractor staff. Up to the maximum permissible extent, the Global Admin Role shall be limited to ITCILO personnel.
   - Ensure that at least two tenant-level administrative accounts remain under exclusive control of the Centre and that the Contractor does not retain unrestricted administrative control of the infrastructure.
   - Deliver a Security & Governance Risk Register identifying vulnerabilities, privilege exposures, and recommended remediation actions.

   The Transition Phase shall conclude with formal acceptance by the Centre upon validation of documentation, implementation of the RBAC framework, reduction of excessive privileges, and completion of the full list of actions listed in **Annex 7**.

2. **Microsoft Cloud Platform & Hybrid Identity Management (Core Service)**

The Contractor shall provide full operational and lifecycle management of the Centre's Microsoft cloud ecosystem, including Microsoft 365, Azure, Entra ID and integrated IaaS, PaaS, and SaaS platforms. The service shall include configuration, integration, optimization, security hardening, governance and continuous improvement activities as listed in **Annex 8.**

The Microsoft Cloud Platform services described in **Annex 8** are considered core operational activities under the monthly service fee. Activities required to onboard new applications, enable authentication mechanisms, configure policies, extend identity services, or deploy additional workloads within the Microsoft ecosystem shall **NOT** be considered out-of-scope unless they constitute a major platform replacement or enterprise-wide transformation initiative.

Activities constituting a major change in the scope shall be considered out of scope.
Excluded examples include:

- Full tenant-to-tenant migration
- Replacement of identity provider
- Complete M365 tenant rebuild
- Major architecture redesign requiring new infrastructure stack

3. **Full Hybrid Microsoft Platform Coverage (Core Service)**

The Contractor shall provide comprehensive operational and lifecycle management of the Centre's hybrid Microsoft environment, including:

- Hybrid identity services (Active Directory, Entra ID, synchronization, authentication, SSO, Conditional Access, RBAC and MFA).
- Microsoft 365 workloads (OnPrem Exchange, Teams, SharePoint, OneDrive, Power Platform, Power BI, Fabric and associated security services).
- Azure infrastructure and governance (VMs, networking, resource configuration, RBAC and monitoring).
- On-premises Windows Server, virtualization, database and endpoint management.
- Security configuration, vulnerability remediation and privileged access

governance.

- Backup, restore validation and disaster recovery oversight.
- Monitoring, alerting, performance and availability management across on-premises and cloud systems.
- Integration and onboarding of additional Microsoft workloads, IaaS, PaaS, or SaaS applications using Entra ID authentication.
- Reviewing and decommissioning any redundant or legacy services.

The above activities, including configuration changes, policy implementation, identity integration and onboarding of additional workloads within the Microsoft ecosystem, are considered core operational services and shall **NOT** be deemed out-of-scope unless they constitute a full platform replacement or enterprise-wide transformation initiative. Complete details of this core service are defined in **Annex 8**.

4. **Windows Patch Management (Core service)**
    - Manage and operate server patch management processes (including WSUS, SCCM, Intune or equivalent) to ensure timely deployment of operating system and security updates on all Windows servers.
    - Ensure critical vulnerabilities on servers and server-hosted applications are remediated within the timelines defined in the SLA.
    - Configure and maintain endpoint patch management platforms (e.g., Intune, SCCM) to ensure policies, update rings and compliance settings are correctly defined and functioning.
    - Monitor overall patch compliance across servers and report deviations.

    Operational patch deployment and remediation activities for end-user workstations and endpoint devices are out of scope, except where configuration changes to the patch management infrastructure are required.

5. **Citrix Virtual Desktop Infrastructure (VDI) & Application Delivery (Core Service)**

    The Contractor shall provide full operational and lifecycle management and documentation of the Centre's Citrix environment, including Citrix Virtual Desktop Infrastructure (VDI), Citrix ADC, and associated supporting components. The scope

includes:

- Administration, configuration, maintenance and optimization of Citrix Virtual Apps and Desktops infrastructure.
- Management of delivery controllers, storefront services, gateways, profile management, and supporting databases.
- Standard master image management, testing and deployment of updates, patches and version upgrades.
- Performance monitoring, capacity planning and user experience optimization.
- Secure configuration and hardening of Citrix components, including authentication integration with Active Directory and Entra ID.
- Integration with Microsoft services (M365, Azure, hybrid identity and MFA).
- Management of Citrix ADC policies, secure access configuration, certificates and traffic optimization.
- Backup validation, configuration documentation and disaster recovery readiness for Citrix components.
- Onboarding of additional VDI workloads or application publications within the existing Citrix architecture.

These activities, including configuration changes, capacity expansion within the existing Citrix platform, security policy implementation and identity integration, shall be considered core operational services and shall **NOT** be deemed out-of-scope unless they constitute a complete platform replacement or major architectural redesign.

If the Centre replaces or transitions from Citrix to an alternative virtual desktop or application delivery platform during the contract term, the Contractor shall assume operational management and support of the new platform once implemented. The design and implementation of such replacement infrastructure shall **NOT** be considered part of the core operational scope unless separately agreed.

6. **On-Premises Exchange Server (Core Service)**

The Contractor shall provide full operational and lifecycle management of the Centre's on-premises Exchange environment, including:

- Troubleshooting issues related to Microsoft Exchange
- Ensure that the Exchange messaging servers are working optimally through performance optimization and health monitoring of the Exchange environment
- Perform patching and apply updates on the system as required.
- Implement a backup and verification scheme for Exchange
- Certificate management
- Implementation of configuration changes required to maintain service reliability, security and compliance.

In the event that the Centre migrates from on-premises Exchange to an alternative messaging platform, the Contractor shall assume operational management of the new platform once implemented. The design and implementation of such migration shall **NOT** be considered part of the core operational scope unless separately agreed.

7. Authentication and Federation Services (Core service)

- Manage and oversee the phased decommissioning of legacy authentication systems (including AD FS) in alignment with the Centre's identity strategy.
- Administer and optimize Microsoft Entra ID authentication mechanisms, including MFA (based on Entrust), Conditional Access, federation, and secure token services.
- Configure and maintain identity trusts, federation relationships and authentication integrations required for new internal or external services.
- Implement authentication configuration changes necessary to support adoption of new Microsoft IaaS, PaaS or SaaS-based services using Entra ID.

Authentication configuration, federation setup, and identity integration within the existing Microsoft ecosystem shall be considered core operational services.

8. SQL Server administration (core service)

- Monitor and fine tune SQL system performance.
- Perform database backup and recovery.
- Troubleshoot various problems that may arise.

9. Monitoring system operation and maintenance (core service)

- Configure alerts that are deemed necessary for the proper operation of the managed services

- Ensure that monitoring alerts are delivered to the intended recipients in a timely manner
- Act on alerts received from the monitoring system to ensure continuous operation of the managed services

10. Other Infrastructure Services (Core services)

- Management and configuration of Microsoft Defender for Endpoint policies, security monitoring, alert review, and endpoint protection posture across servers and managed devices.
- Administration and support of Remote Desktop Services (RDS), secure remote access configurations and associated authentication mechanisms.
- Lifecycle management of desktop virtual machines and client VMs, including configuration, security baseline enforcement and integration with identity services.
- Operational management of Windows-based application servers, including OS maintenance, patching, security hardening, monitoring and identity integration (excluding functional application support provided by third parties).
- Operational management of any Microsoft Teams-integrated telephony system once implemented; design and deployment of such system shall **NOT** be considered part of the core operational scope unless separately agreed.

NB: The contractor shall manage and support any additional servers, services, or workload added within the same technology stack during the contract term, provided it does not exceed a 20% infrastructure growth threshold.

SERVICE REQUIREMENTS

1. Core services characteristics

The core services characteristics required are the following:

- Customer oriented service delivery
- High quality and promptness in solving support issues
- Continuity of service delivery
- Continuous training of Service Team assigned to the Centre
- Sound coordination and organization of the service
- Monitoring the level of satisfaction at the Centre

2. Languages

The working knowledge for the provision of the services is English. Ticket information

will be recorded on the system in English. The language capacity of the team members may be assessed and will be monitored by the Centre. The Centre might ask the Contractor to organize language training for the members of the team.

3. Skills and competencies

Following are the expected experience, skills and competencies required from the proposed resource(s). Special attention should be given to the role and expertise of the Service Manager that will be the reference person and key contact for all type of requests.

4. Service Manager:

- **Required experience:** at least 5 years of experience in the same role
- **Service-oriented culture:** strong service-oriented culture, attentive towards the prevention of problems and proactive, especially in identifying new emerging needs.
- **Required Certifications:** ITIL Foundation version 4.

5. System Administration team:

- **Required experience:** each resource should have at least 3 years of experience in the same role
- **Service-oriented culture:** the team shall demonstrate a strong service-oriented culture. They shall be extremely attentive towards the prevention of problems and be proactive in anticipating issues and needs
- **Certifications:** Associate-expert on the technologies indicated above such as: Microsoft Certified Solutions Associate/Expert (Windows, Messaging, SQL Server, SharePoint, Citrix, Veeam, etc.

In additional to the technical certifications indicated above the Contractor shall ensure that all team members are familiar with the Information Technology Infrastructure Library (ITIL framework) concepts and terminology and the Prince 2 project management's methodology.

6. General skills and knowledge of Service team members

- identifies new and better approaches to work processes and incorporates these in own work;
- good knowledge of IT Systems analysis, design, implementation and operations;
- keeps abreast of available technology; understands applicability and limitation of

technology to the work of the Centre; actively seeks to apply technology to appropriate tasks; shows willingness to learn new technologies;
- good communication skills (both spoken and written);
- ability to develop IT technical documentation;
- accuracy, rigorous planning, problem solving, sense of initiative;
- capacity to respect deadlines and to prepare timely inputs to reports;
- capacity to organize and manage tasks with limited supervision.

SERVICE VOLUME

The team managed an average of 100 tickets in the last one year.

SERVICE DELIVERY

The service is intended to be performed remotely through a site-to-site VPN.

The service will be provided as follow:

- Business hours: Monday to Friday - from 8:00 to 19:00
- Weekend hours and holiday from 8:00 to 19:00

If appropriate, the contractor may be requested to deliver some activities on premises or outside business hours.

The Centre is open all year round. Vacation leave will be agreed upon in advance, paying particular attention to service continuity. If there is prolonged absence by the assigned resource, this should be communicated at least 30 days in advance, with the contractor providing at his/her own expense a handover period of 3 weeks to another person with equivalent or superior qualifications and skills.

PAYMENT TERMS

The Centre will pay at the end of each quarter upon receipt of the related quarterly service report.

Quarterly reports should at least include:

- Volume / List of planned activities performed.
- Volume of incidents in number of calls and type of incidents, indicating number of

resolved and unresolved incidents, time to first response, time to resolution, number of hours-day needed.

For the additional projects or activity requested by the Centre, the Contractor will invoice once the deliverables have been completed to the satisfaction of the Centre.

The Centre will pay invoices within 30 days from their receipt.

SERVICE LEVEL AGREEMENT, KEY PERFORMANCE INDICATORS AND PENALTIES

1. **Definitions**

   For the definitions of terms used in this section (such as downtime, availability, etc.) please refer to ITIL's definition.

2. **Service Request Response and Resolution Times per Priority**

   An Incident's priority is determined by assessing its impact and urgency. 'Urgency' is a measure of how quickly a resolution of the Incident is required. 'Impact' is measure of the extent of the Incident and of the potential damage caused by the Incident before it can be resolved.

   The following table establishes the categories of urgency:

Category	Description
High (H)	The damage caused by the Incident increases rapidly. Work that cannot be completed by staff is highly time sensitive. A minor Incident can be prevented from becoming a major Incident by acting immediately. Several users at management and senior management level are affected.
Medium (M)	The damage caused by the Incident increases considerably over time. Several users at management and senior management level are affected.
Low (L)	The damage caused by the Incident only marginally increases over time. Work that cannot be completed by staff is not time sensitive.

The following table established the categories of impact:

Category	Description

High (H)	A large number of staff are affected and/or not able to do their job. A large number of clients are affected and/or acutely disadvantaged in some way. The damage to the reputation of the Centre is likely to be high.
Medium (M)	A moderate number of staff are affected and/or not able to do their job properly. A moderate number of clients are affected and/or inconvenienced in some way. The damage to the reputation of the Centre is likely to be moderate.
Low (L)	A minimal number of staff are affected and/or able to deliver an acceptable service, but this requires extra effort. A minimal number of clients are affected and/or inconvenienced but not in a significant way. The damage to the reputation of the Centre is likely to be minimal.

An Urgency-Impact Matrix is used to define the priorities.

		Impact		
		H	**M**	**N**
Urgency	**H**	1	2	3
	M	2	3	4
	L	3	4	4

Based on priorities defined above, you can find below a table indicating the requested response time and resolution time during the business and weekend hours as indicated in the “Service Availability” section indicated in the Statement of Work).

Priority Level	**Business Hours**		**Weekend hours**	
	Response Time	**Resolution Time**	**Response Time**	**Resolution Time**
Critical (1)	30 minutes	4 hours	1 hour	4 hours
High (2)	1 hour	4 hours	4 hours	8 hours

Medium (3)	4 hours	2 business days	1 business day	2 business days
Low (4)	1 business day	10 business days	1 business day	10 business days

3. Service Level Agreements (SLAs)

The advertised availability, expressed as a percentage of uptime in a given year, for the Centre's main IT services is 99,5%.

Any unavailability or non-accessibility of an IT system that is not caused by failures of the services provided by the Contractor will be excluded from the SLA calculations. For example. Power failures, Force majeure (flood, fire, strike, etc.), no access to location and/or user not present (for on-site interventions), etc.

You can find here below the two main SLA to respect:

No.	Performance Metric	Performance Target	Definition	Calculation	Frequency of Review	Service Penalties
SLA-1	Downtime per System outage	99,5% availability	The downtime is any time a system is unavailable	Length of time a system is down for each system outage based on data from the monitoring system	Quarterly	See Table 1 below
SLA-2	Support Ticket Response and Resolution	>90% conformance to the response and resolution targets for each of the ticket priority levels	Measures the length of time to respond to support requests and the length of time to resolve support requests. This SLA will apply separately to	For each priority level, the number of tickets which were within the windows defined in Table 2 / Total number of support requests. The assessment of this SLA will be based on	Monthly	Up to 5% of monthly support and maintenance costs

			each of the ticket priority levels	the data in the Ticketing System		

Table 1 - Incident Duration Service Penalty

Critical and High Incident Duration	**Service Penalty (% of monthly support and maintenance cost)**
< 4 hours	0%
≥ 4 hours and < 6 hours	1%
≥ 6 hours and < 8 hours	2%
≥ 8 hours	5%

4. Key Performance Indicators (KPIs)

Key Performance Indicators (KPIs) will help ensure services provided are performing well. It is important to note that the Contractor systematically endeavours to resolve all problems as soon as possible independently of the SLAs and KPIs set in the spirit of good customer relations and satisfaction.

Below table lists the definitions and measurement of KPIs:

No.	Performance Metric	Performance Target	Definition	Calculation	Frequency of Review
KPI-1	Cumulative *Unplanned Downtime*	Less than 8 hours of *Unplanned Downtime* per month. This does not include *Scheduled Downtime*.	The KPI assesses the stability of the systems managed by the contractor and the ability to quickly recover from a system outage	The assessment of this KPI should be based on the data from the monitoring system	Quarterly (the KPI should be evaluated for each month in the quarter)
KPI-4	Application of security patches	>90%	Percentage of systems with the last released patch	Calculation based on the information	Monthly

			or the previous one, applied by the time indicated in the SOW (1 day when exposed on the internet, 2 weeks for the other systems)	published by the vendors related to security patches for each of the system and the data of their logs	
KPI-5	Successful changes	>90%	Percentage of the approved changed completed successfully compared to the total number of completed changes	The assessment of this KPI should be based on the data in the Change Register	Quarter

All requests are actionable through appropriate channels: email from authorized personnel, ticket creation and/ or phone (when a critical incident occurs).

Section 3: ANNEXES

GENERAL ANNEXES

ANNEX 1: GENERAL CONDITIONS OF CONTRACT

Annex 1 is attached to the e-mail. Please note that it is compulsory to return it duly signed when submitting the technical proposal.

ANNEX 2: NON – DISCLOSURE AGREEMENT

Annex 2 is attached to the e-mail. Please note that it is compulsory to return it duly signed when submitting the technical proposal

ANNEX 3: FAQ

TECHNICAL ANNEXES

ANNEX 4: LIST OF VIRTUAL MACHINES, APPS AND VERSION

ANNEX 5: LIST OF TICKETS, MAJOR CHANGES AND INCIDENTS

ANNEX 6: END-USER TECHNOLOGICAL CONTEXT

ANNEX 7: THIRTY DAY TRANSITION, DISCOVERY, GOVERNANCE & SECURITY BASELINE PHASE

ANNEX 8: MICROSOFT CLOUD PLATFORM & HYBRID IDENTITY MANAGEMENT - DETAILED SCOPE