



REQUEST FOR PROPOSAL

Ref No. STF-26-SVP-1344

The CENTRAL MINDANAO UNIVERSITY, through its Bids and Awards Committee (BAC), is inviting all interested Consultant or Consulting Firm to submit a Proposal for the project with details as follows:

Project Title : CONSULTING SERVICES ON: Development, Validation, Finalization, and Submission of the Central Mindanao University Information Systems Strategic Plan (ISSP) 2028–2030

Approved Budget for the Contract : Php 500,000.00

Source of Funds : Special Trust Fund

Location : Office of the Bids and Awards Committee, Admin Extension Building Musuan Maramag Bukidnon

Delivery Period : 13 working days – 5 days online, 5 days face-to-face and 3 days online from receipt of the Notice to Proceed (NTP)

End-User : Central Mindanao University – Digital Transformation Office

Terms of Reference : Please see attached TOR

ACTIVITIES	SCHEDULE
Posting of the Request for Proposal (RFP)	09 October 2026
Deadline for Submission of Proposal	15 October 2026, 9:00 am
Opening of the Proposal	15 October 2026, 9:00 am

This RFP is subject to the Terms and Conditions herein provided. Please submit your best offer for the items described using the attached Price Quotation Form.

Submit your duly signed Proposal not later than 15 October 2026, 9:00 am. Manual submissions shall be at the address indicated.

HERMIE P. PAVA
BAC Chairperson, Consulting Services
Office of the Bids and Awards Committee
Central Mindanao University
Musuan Maramag Bukidnon

The CMU-BAC Office reserves the right to accept or reject any offer or to cancel the entire procurement process at any time prior to award of the contract without thereby incurring any liability to the affected Consultant or Consulting Firm.

Late Submission of Proposal shall not be accepted or considered.



TERMS AND CONDITIONS

I. VALIDITY OF PRICE QUOTATION AND OTHER IMPORTANT REMINDERS

- The award of the Contract shall be made only to the Highest Rated and Responsive Quotation (HRRQ) which complies with the minimum technical specifications and other terms and conditions stated herein.
- The prospective Consultant or Consulting Firm shall provide correct and accurate information required in the Price Proposal Form (PPF).
- The use of the PPF is highly encouraged to minimize errors or omissions of the required mandatory provisions.
- A partial Proposal is not allowed.
- Proposals must be valid for a period of One hundred twenty calendar days (120 cd) from the date of submission which is the date indicated in the PPF.
- Price Quotations must be denominated in Philippine peso.
- Price Quotations must include all taxes, delivery charge and other incidental expense.
- Price Quotations exceeding the Approved Budget for the Contract shall be rejected.
- In case two or more prospective Consultants or Consulting Firms are determined to have submitted the same HRRQ, the BAC-CMU shall adopt and employ "draw lots" as the tie-breaking method to finally determine the winning Consultant or Consulting Firm.

II. PERFORMANCE SECURITY

- The Consultant or Consulting Firm shall be required to post a Performance Security in the form and in the amount not less than the required percentage of the Total Contract Price (TCP) under Section 68.4 of the IRR of RA 12009. The Performance Security may be in any of the following forms:
 - a. Cash or Cashier's or Manager's check issued by a bank – 5% of the TCP;
 - b. Bank draft or guarantee or irrevocable Letter of Credit issued by a bank – 10% of the TCP
 - c. Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security – 30% of the TCP

III. DOCUMENTARY REQUIREMENTS TO BE SUBMITTED TOGETHER WITH THE QUOTATION

- Submit the following eligibility requirements together with your Proposal:

Legal Documents

- a. 2026 Mayor's/ Business Permit;
- b. Registration certificate from the Securities and Exchange Commission (SEC) for corporations and partnerships, the Department of Trade and Industry (DTI) for sole proprietorships; -for corporations, an updated General Information Sheet reflecting the beneficial ownership information duly submitted to the SEC in accordance with its annual reportorial requirements.
- c. PhilGEPS Certificate of Registration.



Office of the Bids and Award Committee

- d. Tax clearance, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).
- e. Income/ Business Tax Return; and -Annual Income Tax Returns of the preceding tax year; VAT or Percentage Tax Returns covering the previous six months.
- f. Notarized Omnibus Sworn Statement

Certification of Platinum Membership may be submitted in lieu of documents a, b and c.

a. Additional documentary requirements:

- g. Authorization / Board Resolution / Special Power of Attorney or Secretary's Certificate duly authorizing the Consultant's or Consulting Firm's representative to sign the PPF, Notice of Award (NOA), Purchase Order, and Notice to Proceed (NTP).

Technical Documents:

- h. Eligibility Documents Submission Form
- i. Organizational Chart
- j. Statement and Summary of completed and ongoing projects
- k. Plan of Approach and Methodology
- l. List of key personnel to be assigned to the project with their complete qualification and experience data with Curriculum Vitae (CV) for Proposed Professional Staff
- m. Certificate of Availability of Key Personnel

Financial Document:

- n. Financial Proposal Submission Form
 - The financial form shall be submitted in a separate sealed envelope.

IV. PERFORMANCE SCHEDULE AND ACCEPTANCE

- The services must conform to and comply with the Terms of Reference herein attached.

V. PAYMENT TERMS AND LIQUIDATED DAMAGES

- Payment shall be made upon to the satisfactory completion and acceptance of each corresponding milestone or deliverable as required in the TOR. No payment shall be made for incomplete, non-compliant, or rejected deliverables. Please refer to the attached TOR for the milestone set.
- Liquidated damages equivalent to one tenth of one percent or 0.1% of the value of the services not performed within the prescribed period shall be imposed per day of delay. Central Mindanao University may rescind the Contract once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the Contract, without prejudice to other courses of action and remedies available to it.



VI. DEADLINE OF SUBMISSION AND OPENING OF QUOTATION

- The Proposal, together with the mandatory requirements, may be submitted in a sealed envelope manually or by registered mail to the following address not later than 15 October 2026, 9:00 am.

HERMIE P. PAVA
BAC Chairperson, Consulting Services
Office of the Bids and Awards Committee
Central Mindanao University
Musuan, Maramag Bukidnon

VII. RESERVATION CLAUSE

- The CMU-BAC reserves the right to accept or reject any offer or to cancel the entire procurement process at any time prior to award of the Contract without thereby incurring any liability to the affected Consultant or Consulting Firm.



PRICE PROPOSAL FORM

Date: _____

OFFICE OF THE BIDS AND AWARDS COMMITTEE

Central Mindanao University
Musuan Maramag Bukidnon

Sir/Madam:

Having examined the Request for Price Proposal No. **STF-26-SVP-1344** which includes the technical specifications, the receipt of which is hereby acknowledged, the undersigned, offer to, in conformity with the said Request for Price Proposal for the sums stated hereunder:

ITEM NO.	ITEM DESCRIPTION	QTY.	UNIT	UNIT PRICE (VAT Inclusive)	TOTAL PRICE
1	CONSULTING SERVICES ON: Development, Validation, Finalization, and Submission of the Central Mindanao University Information Systems Strategic Plan (ISSP) 2028–2030	1	Lot		
Total Price Proposal					
Total Price in Words:					
Terms of Delivery: 13 working days – 5 days online, 5 days face-to-face and 3 days online upon receipt of Approved Contract/Notice to Proceed					
Terms of Payment: Upon satisfactory completion and acceptance of the required consultancy services and deliverables					

We undertake, if our Proposal is accepted, to deliver the services as identified in the Technical Specifications/Terms of Reference and in accordance with the delivery schedule.

Our quotation excludes all taxes, duties and/or levies payable and is valid for a period of ONE HUNDRED TWENTY (120) calendar days upon issuance of this document.

We understand that the CMU Bids and Awards Committee (BAC) may require from us the submission of documents that will prove our legal, financial and technical capability to undertake this project.

Until a formal Contract is prepared and executed, this Proposal, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

Very truly yours,
Signature: _____
Printed Name: _____
Date: _____
Company Name: _____



CONSULTING SERVICES ON:

Development, Validation, Finalization, and Submission of the Central Mindanao University Information Systems Strategic Plan (ISSP) 2028–2030

TERMS OF REFERENCE

DESCRIPTION

The project covers the consulting services for the development, validation, finalization, and submission of the Central Mindanao University Information Systems Strategic Plan (ISSP) 2028–2030.

The consultancy aims to provide specialized technical assistance to Central Mindanao University (CMU) in assessing its existing ICT environment and capabilities and in developing a comprehensive, risk-informed, and sustainable Information Systems Strategic Plan aligned with the University's institutional priorities, ICT governance requirements, cybersecurity considerations, regulatory compliance requirements, and applicable Department of Information and Communications Technology (DICT) requirements and prescribed templates.

The consultancy shall cover ICT assessment, gap analysis, cybersecurity and information security review, software and systems assessment, network infrastructure review, ICT policy and governance assessment, capacity building, risk-based ICT planning, regulatory compliance review, ISSP development, stakeholder consultation, validation, finalization, presentation, and follow-up technical support.

DELIVERABLES	STATE "COMPLY" OR "NOT COMPLY"
I. SCOPE OF SERVICES 1. Pre-Assessment and Project Initiation - Conduct project kick-off and initial consultations with ODT, the CMU ICT team, and concerned stakeholders; - Define the project scope, objectives, activities, expected outputs, and schedule; - Identify key stakeholders and establish appropriate communication and coordination channels; - Provide and review pre-assessment forms, questionnaires, and data requirements; - Gather and review relevant ICT documents, policies, plans, systems documentation, infrastructure information, and other necessary records; and - Establish the assessment and ISSP development approach based on CMU's institutional context and requirements.	



2. ICT Assessment and Gap Analysis • Assess the current state of CMU's ICT environment, capabilities, systems, and resources; • Conduct assessment of cybersecurity, information security, software development, network infrastructure, ICT governance, and existing ICT policies; • Conduct interviews, surveys, consultations, documentation review, and onsite inspection as necessary; • Identify ICT strengths, weaknesses, vulnerabilities, risks, and operational gaps; • Compare existing ICT practices and capabilities against applicable ISMS best practices and relevant standards; • Identify immediate, medium-term, and long-term ICT improvement requirements; and • Develop prioritized recommendations to address identified ICT gaps and risks.	
3. Cybersecurity and Information Security Assessment • Review existing cybersecurity and information security measures and controls; • Assess existing security protocols, incident response mechanisms, data protection measures, and access control practices; • Conduct appropriate cybersecurity assessment activities, including vulnerability assessment and penetration testing (VAPT), where applicable and within the agreed scope; • Identify risks affecting the confidentiality, integrity, and availability of University information and systems; and • Recommend appropriate measures to strengthen CMU's cybersecurity and information security posture.	



Office of the Bids and Award Committee

4. Software and Information Systems Assessment • Review the lifecycle of internally developed and procured software applications; • Assess existing software systems in relation to institutional requirements and operational needs; • Review software development practices and applicable secure coding considerations; • Identify opportunities for improving software functionality, efficiency, interoperability, and security; and • Recommend appropriate frameworks, tools, and strategies for sustainable software and information systems development.	
5. Network Infrastructure Assessment • Conduct an assessment of the University's existing network topology, infrastructure, and equipment; • Assess bandwidth utilization, connectivity, redundancy, fault tolerance, and network reliability; • Identify network bottlenecks, vulnerabilities, and areas requiring improvement; • Evaluate the adequacy of existing network infrastructure in supporting University operations; and • Recommend appropriate network improvements and long-term infrastructure requirements.	
6. ICT Governance, Policy, and Regulatory Compliance Review • Review existing ICT policies, procedures, and governance mechanisms; • Assess policies related to data privacy, access control, cybersecurity, disaster recovery, and other relevant ICT areas; • Benchmark existing ICT policies and practices against applicable ISMS best practices and relevant standards; • Assess alignment with applicable regulatory requirements, including data privacy, cybersecurity, and other relevant government and educational regulations; • Identify policy, governance, and compliance gaps; and • Recommend appropriate new, revised, and/or updated ICT policies and governance measures.	



Office of the Bids and Award Committee

7. Capacity Building and Training • Conduct training sessions on Information Systems Strategic Planning; • Provide training on risk-based ICT planning and management; • Conduct sessions on cybersecurity, information security, and ISMS best practices; • Provide orientation on applicable regulatory and compliance requirements; • Facilitate practical workshops on ISSP preparation and strategic planning; and • Equip identified CMU stakeholders with knowledge, skills, tools, and techniques necessary to participate in the development, implementation, monitoring, and maintenance of the ISSP.	
8. Risk-Based ICT Planning • Introduce appropriate frameworks and tools for ICT risk identification and assessment; • Facilitate the identification and analysis of ICT-related risks; • Develop and/or assist in the preparation of ICT risk registers; • Identify appropriate risk mitigation strategies and controls; • Develop contingency and continuity considerations for critical ICT resources and services; and • Integrate identified risks, mitigation strategies, and risk considerations into the ISSP.	
9. ISSP Development and Strategic Planning • Facilitate stakeholder consultations and strategic planning workshops; • Consolidate and analyze outputs from the ICT assessment, gap analysis, workshops, and stakeholder consultations; • Identify and prioritize the University's ICT strategic directions and priorities; • Identify appropriate ICT programs, projects, systems, infrastructure, and investments; • Ensure alignment of ICT initiatives with CMU's academic, administrative, research, and institutional priorities; • Integrate cybersecurity, risk management, ICT governance, and regulatory compliance considerations into the strategic plan; • Assist CMU in drafting the Information Systems Strategic Plan (ISSP) 2028–2030; and • Ensure that the ISSP is prepared in accordance with applicable DICT requirements and prescribed templates.	



10. ISSP Validation and Finalization • Present the draft ISSP to concerned CMU officials and stakeholders; • Facilitate validation and review sessions; • Consolidate and address comments, recommendations, and required revisions; • Review the ISSP for completeness, consistency, strategic alignment, and compliance with applicable requirements; • Finalize the ISSP and related supporting documents; and • Prepare the completed ISSP for submission to DICT.	
11. Final Presentation and Knowledge Transfer • Present the ICT Assessment Report and finalized ISSP to CMU leadership and concerned stakeholders; • Discuss major findings, identified risks and gaps, strategic priorities, recommendations, and proposed ICT programs and projects; • Provide relevant planning tools, templates, frameworks, training materials, and documentation; • Facilitate knowledge transfer to the CMU ICT team and other concerned stakeholders; and • Provide recommendations for the continuing implementation, monitoring, and evaluation of the ISSP.	
12. Follow-Up Technical Support • Provide technical guidance on initial ISSP implementation concerns; • Provide support for modifications and revisions resulting from DICT evaluation; • Assist in addressing comments and recommendations related to the ISSP; • Provide guidance on continuing ICT strategic planning, monitoring, and evaluation; and • Recommend continuing training and capacity-building activities as necessary.	
II. OBJECTIVES	
1. Develop the CMU Information Systems Strategic Plan (ISSP) 2028–2030 Develop a comprehensive and strategic ICT plan that provides clear direction for the University's information systems, ICT infrastructure, programs, projects, investments, and digital transformation initiatives in support of CMU's institutional priorities.	



Office of the Bids and Award Committee

2. Assess Existing ICT Capabilities and Identify Gaps Conduct a comprehensive assessment of CMU's existing ICT systems, infrastructure, cybersecurity, software applications, network environment, governance, policies, and capabilities and identify gaps, risks, and priority areas for improvement.	
3. Strengthen ICT Governance and Information Security Enhance CMU's ICT governance and information security posture by identifying appropriate policies, controls, risk mitigation measures, and cybersecurity strategies aligned with applicable ISMS best practices and relevant standards.	
4. Integrate Risk-Based ICT Planning Establish a risk-informed approach to ICT strategic planning by identifying ICT risks, assessing their potential impact, and incorporating appropriate mitigation strategies and priorities into the ISSP.	
5. Ensure Regulatory and Policy Compliance Strengthen alignment of CMU's ICT strategies, policies, systems, and practices with applicable regulatory requirements, data privacy requirements, cybersecurity standards, and other relevant government and educational regulations.	
6. Establish Strategic ICT Priorities and Investment Directions Identify and prioritize ICT programs, projects, infrastructure requirements, information systems, and investments based on institutional needs, identified risks, available resources, and long-term digital transformation objectives.	
7. Facilitate Validation and Preparation for DICT Submission Ensure that the CMU ISSP 2028–2030 is properly reviewed, validated, finalized, and prepared for submission in accordance with applicable DICT requirements and prescribed templates within the prescribed period.	
III. Tasks/Key Responsibilities of the Consulting group:	
1. Project Initiation and Coordination i. Collaborate with CMU to define the project scope, objectives, activities, expected outputs, and schedule. ii. Identify key stakeholders and establish appropriate communication and coordination channels. iii. Conduct initial meetings and consultations with ODT, the ICT team, and concerned offices.	
2. Pre-Assessment and Data Gathering i. Provide pre-assessment forms, questionnaires, and data requirements. ii. Review relevant CMU documents, ICT plans, policies, systems, infrastructure information, and other supporting records.	



Office of the Bids and Award Committee

iii. Conduct interviews, surveys, consultations, and onsite assessment activities. iv. Gather and analyze information necessary for ICT assessment and ISSP development.	
3. ICT Assessment and Gap Analysis i. Assess cybersecurity, software systems and development, network infrastructure, ICT governance, policies, and existing ICT capabilities. ii. Identify strengths, weaknesses, vulnerabilities, risks, and gaps. iii. Compare existing practices against applicable ISMS best practices and relevant standards. iv. Recommend short-term and long-term ICT improvement measures	
4. Cybersecurity, Software, and Network Assessment i. Conduct appropriate cybersecurity assessment activities, including vulnerability assessment and penetration testing where applicable. ii. Review software applications, development practices, and information systems. iii. Assess network topology, equipment, bandwidth, redundancy, reliability, and security. iv. Identify areas requiring technical improvement and provide recommendations.	
5. ICT Policy and Compliance Review i. Review existing ICT policies and governance mechanisms. ii. Assess data privacy, access control, disaster recovery, cybersecurity, and related policies. iii. Identify policy and regulatory compliance gaps. iv. Recommend development, revision, and/or updating of ICT policies.	
6. Capacity Building and Training i. Conduct training and workshops on ISSP development, risk-based ICT planning, cybersecurity, ISMS best practices, ICT governance, and regulatory compliance. ii. Facilitate practical workshops and exercises tailored to CMU's ICT environment. iii. Provide training materials, tools, and planning frameworks.	
7. Risk Assessment and Management i. Facilitate ICT risk identification and assessment. ii. Develop and/or assist in preparing risk registers. iii. Identify appropriate risk mitigation strategies and priorities.	



Office of the Bids and Award Committee

iv. Integrate risk management considerations into the ISSP.	
8. ISSP Development i. Facilitate stakeholder consultations and planning workshops. ii. Consolidate assessment findings and stakeholder inputs. iii. Assist in identifying strategic ICT priorities, programs, projects, systems, infrastructure, and investments. iv. Collaboratively prepare the CMU ISSP 2028–2030. v. Ensure integration of risk management, cybersecurity, governance, and regulatory compliance considerations.	
9. ISSP Validation and Finalization i. Present the draft ISSP to CMU officials and stakeholders. ii. Facilitate validation and review sessions. iii. Incorporate comments and recommendations. iv. Finalize the ISSP and supporting documentation. v. Prepare the ISSP in accordance with applicable DICT requirements and prescribed templates.	
10. Final Presentation and Knowledge Transfer i. Present the ICT Assessment Report and finalized ISSP to CMU leadership and key stakeholders. ii. Explain major findings, risks, recommendations, strategic priorities, and proposed ICT initiatives. iii. Provide relevant tools, templates, frameworks, and documentation. iv. Facilitate knowledge transfer to CMU personnel.	
11. Documentation and Reporting i. Prepare the ICT Assessment Report. ii. Prepare workshop and consultation reports. iii. Document assessment findings, risks, gaps, recommendations, and strategic priorities. iv. Provide the draft and finalized ISSP and other required supporting documents.	
12. Follow-Up Technical Support i. Provide technical guidance on initial implementation concerns. ii. Assist in modifications and revisions arising from DICT evaluation. iii. Provide follow-up consultation and technical assistance related to the ISSP. iv. Recommend continuing training, monitoring, and evaluation activities.	