Points requiring clarifications in relation to the Request for Proposal No. 59 **"Benazir Income Support Program (BISP) Business Need Assessment & Preparation of IT (Information Technology) and IS (Information Security) Strategy"**

S#	Clarification/ Information Required	Comments
1	Please provide clarity on the required validity of the proposal. Clause 13 requires the proposal to be valid for a period of 180 days, whereas other sections of the RFP state 90 days.	The required validity of the proposal is 90 days.
2	Is there a specific business and/or organizational goal defined that has led to the need for developing an IT strategy for BISP?	BISP started in July 2008 with basic IT infrastructure to service initial set of beneficiaries. With an increase in number of beneficiaries, modernization and integration of IT systems was not done rather standalone applications were built to address the need. The business objective is to transform the BISP IT and IS infrastructure to make the business operations efficient and also to prepare the systems for future expansions in G2P programs.
3	The scope requires pre-certification audit to be carried out (clause 3.1.10). Is a specific certification already identified for BISP to comply with, such as ISO 27000?	The consultant will provide advice on the relevant standard and compliance guidelines.
4	Is the current BISP IT architecture adequately mapped and updated?	No
5	Section 1. Letter of Invitation: It is stated to submit soft copy of the proposal through email. Is "Financial Proposal" also to be submitted through email? We ask because doing so might result in breach of confidential financial information in a competitive bidding process. It would be helpful to understand how said confidentiality would be ensured throughout this process.	Financial proposals remain with procurement department and kept in secure folder to maintain the confidentiality. However proposers may submit password protected electronic copies of financial proposal. Password for financial proposal will be requested by the Purchaser at the time of financial opening.
6	Section 2. Instructions to bidders, A. General, Clause 3. Eligibility: Is the minimum years of relevant experience applicable only to experts, or also to the consulting organization?	It is for both.

7	Section 2. Instructions to bidders, B. Request for Proposal, Clause 6. Contents of the RFP: Annexure A-Proposal Submission Form is not attached in the RFP. Could you share the Annexure A-Proposal Submission Form?	Proposal submission form in word format is uploaded with RFP responses at KRN website.
8	Section 4. Terms of Reference, About the Project: BISP currently runs multiple G2P programs that include both Conditional and Un-Conditional Cash transfers (UCT) and in addition manages a National Socio-Economic Registry (NSER). Whereas, only BISP Business Functionality View for NSER is given in the TOR. To better understand the scope of work, could you also share Business Functionality Views for all other in-scope G2P programs offered by BISP? As much clarification as possible on the following would be helpful in planning the required resources: a) Size and complexity of IT infrastructure that is in-scope for assessment. This may include inventory of critical systems and processes, number of servers and applications in portfolio, and size of IT organization in terms of number of people. b) General size and complexity of all business processes that are in-scope as well as identification of which of those handle, process or store sensitive or confidential or otherwise protected or privileged information, whether electronically or not. It would also help to understand the existing security posture of the organization which includes the following: i. Does the organization have a CISO (Chief Information Security Officer) or similar officer dedicated to an information security function, and if so, where does s/he report into in the organization? ii. Does the organization have an information security team dedicated to or responsible for information	G2P programmes like Unconditional Cash Transfer (UCT), Conditional Cash Transfer (CCT), Graduation, Monitoring & Evaluation (M&E), Case Management System (CMS), and other Wings of BISP including Human Resource (HR), Finance & Accounts (F&A) etc. are connected and use the NSER data for business purposes. a) @NADRA: Oracle Exadata Engineered System Quarter Rack, 13 TB Usable, 96 GB of RAM with an attached Oracle Secure Backup Solution comprise of RTL. @NTC: Primary Site Consists of: 4 x IBM Power 8 Servers (S822LC) with each one having 512GB of RAM and 2 socket processor with 2 x 1TB SSD installed with RHEL7 and linux KVM, 1 x IBM V9000 SAN with 12TB of Flash attached with 4 x IBM Power 8 servers, 1 x HPE DL380 Gen8 with 512GB RAM, dual socket processors installed having 7 x SSDs with VMware EXSi , 1 x IBM SystemX Server with 32GB RAM and 2 x 1TB SATA HDs Whereas at NTC DR site located at Lahore which only contains 1 x HPE DL380 gen8 with 512GB RAM with dual sock processor and 7 x SSDs installed with VMware ESXi. b) NADRA Exadata machine is being accessed by MIS webserver, MIS selective dba, developers only NTC information systems, placed at primary site, are being accessed by MIS-team for administration, monitoring, deployments and troubleshooting whereas selected and specific

	security risk management, and if so, how big is it and are there minimum requirements certification-wise? iii. Does the organization follow a tiered security operations model, with a dedicated Security Operations Center (SOC) and is this managed in-house or is it outsourced? iv. Does the organization have a dedicated team of security analysts responsible for cyber intelligence, incident response and forensics? Are they certified and if so, what certification? v. Does the organization implement best practices such as firewalls, intrusion detection systems, security incident response management (SIEM), behavioral analytics, log review and monitoring (Splunk or similar), antivirus, automated patching and other best practices? If so, which and which not? vi. Does the organization have a well-defined Software Development Life Cycle (SDLC)? vii. Does the organization have well established policies around data classification, lifecycle (including disposal) and handling, business viii. continuity, disaster recovery, employee screening / compliance validation, on-boarding and off-boarding processes, and mandatory time away? If so, it would be helpful to understand which. ix. What is the physical footprint of the organization, how many offices and how many employees in each location?	services/ports of the servers is exposed through multiple layers of firewalls from field VPN tablets. I & II: Organization is hiring 1 x Information Security Specialist and seeking approval to hire another resource for Network Security Specialist. iii & iv: After being hired 2 x IS HR, BISP will be in a position to deploy building blocks of IS footprints in an organization including SOC, Incident Response, computer forensics, SIEM deployments and integration with network/ security appliances. Furthermore, policy documents archival has been established, budgeting requirements to acquire SIEM in FY-2019/20 has been forwarded. Procurement for Database Activity Monitoring (DAM) solution is in pipeline. V: Firewall is deployed at BISP HQ, NTC and NADRA. Site to site VPNs are established, IDS is in place, SIEMS is in plan, central antivirus is deployed. Vi: No VII: as discussed, NTC DR site exist but due to some limitations it is not fully operational. Hence Dry Run/Disaster Recovery Plan could not be performed. VIII: No Ix: Apart from BISP HQ, each province has a regional office, there are also divisional offices in each division, and there are 421 Tehsil offices. Each has different number of employees.

	x. If the organization has internet facing servers, does the organization implement DMZs and monitor firewalls and IDS systems? xi. Does the organization have a penetration testing, vulnerability scanning and war dialing policy? xii. Does the organization have a structured risk acceptance policy? xiii. Does the organization implement periodic employee information security awareness training?	X: Yes XI: No XII: No XIII: No
9	Section 4. Terms of Reference, About the Project, Clause 2. Scope of Work, Sub-Clauses 3.1.2, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 3.1.9: The term "decided standard(s)" is used. To better understand the scope of work and bid accordingly, could you specify what are the decided standards? Is it only ISO 27000 or are there any others as well?	As per TORs, the standard is to be decided after evaluation by the consultant.
10	Section 4. Terms of Reference, About the Project, Clause 2. Scope of Work, Sub-Clause 3.1.8: It is stated to Conduct training and awareness sessions on ISMS and the relevant decided standards for the entire management team of BISP. However, the number of management team members at different offices/branches are not mentioned in the TOR, which is required to plan the training sessions.	Total 30 BISP team members located at BISP HQ Islamabad.
11	Section 4. Terms of Reference, About the Project, Clause 5, bullet point 12: The consultancy firm is required to have minimum annual turnover of USD 5 million. What is the points weightage of this point?	Firm having met this criteria will have an edge, however this condition does not exclude others.

12	Section 4. Terms of Reference, About the Project, Clause 5, point no. 4: It is stated that in case of consortiums, the lead entity will be responsible for ensuring all required pre-requisite documents listed below (for lead and consortium partners) have been provided to Karandaaz Pakistan. Whereas, no documents are listed in the TOR. Could you share the documents list?	Please disregard serial 4 of section "Terms of participation"
13	Annex A is missing. Please provide	Uploaded at KRN website along with response to queries
14	Sec C 11 on page 5 has instructions on the RFP response. Is there anything else we need to know?	No
15	Besides project sponsor, does Karandaaz have any other role in this project such as project manager.	Karandaaz will sit on the steering committee of the project and will play a role in driving key decisions.
16	Is BISP committed to the project? What resources will they provide - people, space to work, etc.	BISP is fully committed and there will be a project team made for this project.
17	Would Karandaaz like to share current 'as-is' status of IT and IS infrastructure available with BISP	BISP website should be referred for any such details. Also please refer to annexure #1 for list of business applications running at BISP.
18	Has BISP NESR program documented the business work-flow for its current operations or would they expect a complete new undertaking?	BISP NSER workflow is documented.
19	What is the overall size of the budget for this project?	Not to be disclosed at this time.
20	Which of the following functions are outsourced? Current Cash Management System, Operations Area, Complaint Management System, NSER	None, except for payment to beneficiaries through banks.
21	Are there any existing frameworks or strategic international practices that BISP already had considered for this assessment or would they want the firm to suggest for example ITIL, COBIT for Technology Governance Roadmap and NIST, ISO 27001 for Information Security Strategy and alignment	Currently no standards have been implemented, we expect the consultant to suggest BISP on which standards need to be implemented based on the nature of BISP work and experts' study findings.

22	Does BISP already have implemented any third party risk assessment methodology?	None
23	Section 3.1.5 Can you please advise what standard has been already decided?	We expect the consultant to suggest BISP on which standards need to be implemented based on the nature of BISP work and experts' study findings.
24	Section 3.1.5.4 Has the organization a SOC (security operation center) in place to detect, analyze, report, respond and recover operations?	Nil
25	Section 3.1.5.4 Are there any real time vulnerability management tools in place for monitoring any information security loop holes?	Nil
26	Section 3.1.5.4 Has the organization established the privacy policy and considering the international regulatory requirements such as GDPR?	Nil
	Section 3.1.10 It seems that the organization is inclined towards ISO 27001 certification, please confirm our understanding?	Not decided
27	Section 3.2.1.5 Will remediation work be also included in the review of internal and external audit reports?	Suggestions/course of action to be suggested.
28	Section 3.2.2.2 Will the review of the software applications include 1) application landscape infrastructure, documentation, implementation etc. 2) security 3) third party outsourcing 4) system stability, please clarify?	Yes
29	Section 3.2.2.5 Does the organization already has a Disaster Recovery in place?	Partially
30	Section 3.2.2.5 Does the organization intend to move towards cloud services for BCP in the future?	Not yet

31	Documentation: Are current processes documented and distributed among stakeholders in company?	Partially
32	On what platform are IT systems programmed?	Net C#, PHP, Android
33	What is the applied standard database format?	This will be revealed to the winning party
34	Please share the list of applications currently running at BISP?	Kindly refer to annexure # 1
35	Please share current top 3 risks at BISP?	1. In absence of state of the art IS/IT standardized policies, there is risk of data security 2. If proper roadmap with future strategy on IT infrastructure is not chalked out and implemented, there is risk of data integration with other government departments. 3. If IT/IS infrastructure is not planned well to meet future needs, professional level IT support from vendors will be an issue.

Annexure # 1: List of Applications used at BISP

S#	Project	Sub-details	Description	Remarks
1	HRMIS	Desktop Applicatoni for Humarn Resource - Management Information System	A desktop developed in Oracle/Developer. Being used in BISP HR for managing data of BISP Employees	In house
2	Payroll System	Desktop Application for Payroll	A desktop developed in Oracle/Developer. Being used in BISP HO for generating/managing payroll of BISP Employees	In house
3	Multiple Reports / Dashboards		Main functional Dashboards: Management Dashboard NSER Waseela-e-Taleem Payments Case Management System	In house
4	Assets Management System	Web Application	Initial version of Assets management system has been developed according to requirements from Admin Wing.	In house
5	Work plan Monitoring Dashboard – M&E	Web Application	Customized application developed on requirements from M&E wing for tracking and monitoring of work plans in BISP.	In house
6	Carrier Planning Data Acquisition Application	Reporting system for ACRs / Synopsis & Quantification System	System developed for regular / congractual employees annual reports submission and assessment	In house
7	Consultants PERs System	Admin, PER Submission, Reporting Officer Module, Reporting Officer Module, HR Module	System developed for consultants tasks assignment and annual reports submission and assessment.	In house
8	Training Wing Application – Software Design		System developed for training wing of BISP to schedule training for BISP employees country wide	In house