# Rajshahi Krishi Unnayan Bank

Information and Communication Technology Department

Head Office

272, Banalata C/A, Airport Road, Rajshahi

Website: www.rakub.org.bd

# Terms of Reference (TOR)

# For

ISO 27001 Certification Consultation & Certification for Bank and Cyber Security Capacity Building of Rajshahi Krishi Unnayan Bank.

# Rajshahi Krishi Unnayan Bank

Information and Communication Technology Department
Head Office 272, Banalata C/A, Airport Road, Rajshahi
Website: www.rakub.org.bd

**Table of Contents**

## 1. Project Overview, Objective, Scope & Service Area and Information For Applicant

### 1.1 Project Overview:

Rajshahi Krishi Unnayan Bank Limited intends to have international security standard attestation on its Information Technology Enabled Services (ITES) operation and day to day management. Part of it, bank has decided to obtain Information Security Management Standard (ISO 20071). For this, the Bank wants to appoint a competent ISMA consultation and ISO Certification firm and. Besides, the firm will extend its hand to support for end to end technical documentation for ISO and also arrange cyber security skill development training. The service provider(s) will be responsible for delivering the services as per the scope outlined below.

### 1.2 Objective

The objectives of these staged services will further assure to access organization's high-quality information in support with various services from External Vendor/Service Provider firm for designing and building Information Systems which will assist bank to further withstand against latest sophisticated risks. that are effective at gathering, analyzing and outputting the information we need; and these services also will assist securing our information systems against risks to their confidentiality, integrity, availability (CIA), Authenticity and Reliability of information.

### 1.3 Scope & Service Area

**Scope: ISMS (27001) Scope:**

1. Information and Communication Technology Department.
2. Data Center (DC), Near Data Center (NDC)/Disaster Recovery Site (DRS).
3. No. of ICT Employees : 60 (IT + Others)
4. All application/software (At least 10 systems including 4 critical systems)

**Detailed Scope:**

1. Conducting GAP Analysis onsite with documentation.
2. Conducting pre audit with recommendation and migration.
3. Implementation of ISMS (ISO 27001) including gap assessment, all required documents (policy, procedures, others if required) preparation, remediation consultancy.
4. Review of /(assist to prepare) and implement ICT related policy & procedure, best practice :
    a) ICT Security Policy
    b) Software/Application Development and Management Policy
    c) ICT Risk Management Policy, Frame Work and Risk Assessment Procedure
    d) Asset and Data Management Policy
    e) Incident & Problem Management Policy & Procedure
    f) ICT Hardware and Software Usage and Disposal Policy
    g) Baseline Standard Policy for all Equipment e.g. Desktop/Laptop, Servers, etc.
    h) Log Management Policy
    i) Data Retention and Archival Policy
    j) Data Leakage Prevention (DLP) Policy
    k) Cryptographic Key management Procedure
    l) Patch Management Policy and Procedure

m) Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
n) Backup and Restore Policy and Procedure
o) Domain Control policy
p) E mail Policy
q) Cryptographic Key Management Policy
r) Cyber Security Policy
s) Malicious Code Protection Policy/Check list
t) All other relevant Policy/Procedure as mentioned ISO 27001

5. Risk Management Related :
    a) Preparing Risk Management Framework and Assessment Procedure
    b) Performing Risk Assessment & Gap Analysis as per ISO 27001
    c) A Framework/Template to assess security risk properly with mitigation plan before implementing any new system or updating the existing system
    d) Conducting Risk Assessment onsite with documentation
    e) Performing comprehensive Business Impact Analysis (BIA) to govern overall ICT risk and relevant mitigation measures
    f) A Framework/Template with set of metrics to serve as Key Risk Indicator (KRI) align with risk management framework to assess security risk of any IT system/application
    g) A formal Risk Analysis Process/Framework for all required network connections to the internet or third party and public networks.
6. Compliance to Data Center (DC) Policy Guidelines
7. Assist to prepare Annual Audit Plan including stated audit areas and controls
8. Preparing/Reviewing Internal Audit Methodology (Full documentation)
9. Review of Internal Audit Report and its frequency
10. Creation of a framework and procedure for carrying out the audit. In cases of significant noncompliance, establish a mechanism to resolve audit observations
11. Preparation of various templates required to be filled in by the various stakeholders involved in the audit process
12. Designing/Reviewing of Security strategy and policy documents for the Data Center and Disaster Recovery Center
13. Reviewing of the process and controls followed by existing SI (System Integrator). Auditing of overall Physical and IT infrastructure management processes as per ISO 27001 framework including Monitoring, Maintenance and Management of the entire Data Center, along with providing of Helpdesk services and providing recommendations to Rajshahi Krishi Unnayan Bank
14. Assessing and advising assuring of administrative control of data and its confidentiality, security and privacy with the Rajshahi Krishi Unnayan Bank de-jure and de-facto
15. Preparing of framework to ensure that Data Center Operator's actions are in compliance with laid down policies, standards, procedures, and applicable laws and regulations
16. Supplementary requirement in support of implementing ISMS (ISO 27001) including but not limited to following :
    a) Prepare the ISMS Manual for ISO Accreditation
    b) Security Awareness training for ICT stuff of branches (around 800) including Senior Management onsite (food and logistic support will be provided by bank)
    c) ISO 27001 Lead Auditor (Latest Release) training with certification for 10 (local).
    d) 2-days Information Security Refresher Training to IT team once in year

e) Formulate IS Employee training list template, ISMS training deck
f) Formulate the training MIS/Key Performance Indicator (KPI)
g) Prepare an NCCA Tracer
h) Prepare the objective measurement KPI and performance evaluation
i) 1st party (internal) audit as per ISO 27001 compliance
j) Suggestions on corrective & preventive action plan
k) Assisting on preparation of Corrective Action/Preventive Action (CA/PA)
l) Facilitating Management Review meeting

17. Document preparation to apply for certification
18. Engagement of ISO external Audit firm for accreditation audit
19. Stage-1 & stage-2 audit by certification body
20. Handholding till final certification with certification body
21. Organization of Surveillance Audit (2nd year and 3rd year) by certifying body
22. Provide certificate

## Service Area:

- **Capacity Building:**
  Security Operations and Analysis, Hands on Training by using licensed VA & PT Tools, Awareness & Implementation Training, Certified Secure Computer User (CSCU), CEH with certification, SIEM Design and Implementation, CISA- Certified Information Security Auditor, Open-Source Intelligence (OSINT), Cyber Threat Intelligence, SIEM with Tactical Analytics, Malware Analysis, ISO 27001 Lead Auditor Training with Certification, SOC Training (Cyber Threat Intelligence, Malware Analysis, Digital Forensic & Open-Source Intelligence etc.
- **ISO Consultation & Certification :**
  (a) ISO 27001 Scope optimization, Capacity Building, Pre Audit and Gap Assessment. Gap Remediation & Review of ICT related Policies/procedures, etc. Consulting Firm Must have registered office in Bangladesh. Team lead must have minimum of 5 years banking experience. Must have certification on various standards/framework. Must have adequate acumen in in hand on experience in Technical Documentation. Minimum experience of ISO consulting is 3 out of which at least 2 in bank.
  (b) ISO 27001 Certification including consultancy services, etc. ISO Certification Body Must have registered office in Bangladesh. Minimum three (03) certified Lead Auditor (preferably IRCA/PECB/BSI/SGS Certified) with minimum five (05) years experience. Minimum experience of ISO certificate awards is five (05) out of which at least 1 in bank.
- **Consultancy and Surveillance audit:**
  The total estimated time for the project (consultancy and certification) within six (06) calendar months. Three (03) months for 1st & 2nd Consultancy and Surveillance audit in 2nd & 3rd year.

## 1.4 Information For Applicant

| INFORMATION FOR APPLICANT | | |
|---|---|---|
| 1. | Brief description of Assignment | 1. Submit a work plan on the basis of TORs within 10 working days of joining and provide monthly written progress report, in addition to final report.<br>2. Review of existing network diagram, data flow diagram and perform network segmentation testing as required by ISO.<br>3. Submission of all testing tools generated logs and test results in raw and processed format in electronic media.<br>4. Conduct adequate training and awareness on ISO for internal stakeholders.<br>5. Conduct relevant audit pre-audit to identify ISO readiness and produce the report.<br>6. All software or tools required to deliver the service should be deployed at devices owned by Rajshahi Krishi Unnayan Bank. After completion of the service, the firm may uninstall all installed software or tools.<br>7. Provide end to end support for meeting all functional requirements under all domains (goals) for achieving ISO compliance accreditation for Rajshahi Krishi Unnayan Bank.<br>8. Evaluate compensating controls. On an annual basis, any compensation controls must be documented, reviewed, and validated by the assessor and included with the report on compliance.<br>9. Develop remediation plan for ISO compliance and implementing Strong Control Measures. Also provide support and guidance during the compliance process.<br>10. Monitor the progress of remediation and provide update to management.<br>11. Be onsite for the validation of the assessment or duration as required.<br>12. Monitoring and testing Networks on a regular basis for maintaining a Secure Network.<br>13. Findings and Observations (detailed findings on each requirement and sub requirement, including explanations of all N/A responses and validation of all compensating controls.)<br>14. Provide security needs of internal and external systems for achieving certification.<br>15. Conduct ISO compliance audit/final audit and produce the final report (Report on Compliance)<br>16. Provide attestation of compliance when fully complied.<br>17. Performing all other relevant activities for achieving ISO Certification as necessary. |
| 2. | Experience, Resource & Delivery Capacity Required | **The following minimum Experience, Resources & delivery Capacity are required:**<br>1. Should have minimum five (05) years overall business experience of the consulting firm. In case of participating as joint venture or with local partner, each member of joint venture or local partner should have minimum five (05) years overall business experience and all legal notarized documents related to joint venture or local partnership should be submitted. There shall not be any sub-contracting provision.<br>2. a. Consulting Firm :<br>I. Must have registered office in Bangladesh.<br>II. Minimum 3 Certified Lead Implementer with minimum 5 years experience.<br>III. Minimum experience of ISO consulting is 3 out of which at least 2 in bank.<br>IV. Must have adequate acumen in in hand on experience in Technical Documentation.<br>V. Must have certification on various standards/framework.<br>VI. Official recognition on Data Center, Governance, Cyber Security, IT Operation etc. Will have preference on others.<br>VII. Team lead must have minimum of 5 years banking experience.<br>b. ISO Certification Body :<br>I. Must have registered office in Bangladesh.<br>II. Minimum three (03) certified Lead Auditor (preferably |

| | | |
|---|---|---|
| | | IRCA/PECB/BSI/SGS Certified) with minimum five (05) years experience.<br>III. Minimum experience of ISO certificate awards is five (05) out of which at least 1 in bank.<br>3. Should have satisfactory experience of providing ISO certification services to at least two (02) organizations (Banks/Financial Institutions) in last five (05) years.<br>4. Should have minimum one (01) Certified Information System Security Professional (CISSP), minimum one (01) Certified Information Systems Manager (CISM) and minimum one (01) Certified Information Systems Auditor (CISA) enrolled from last one (01) year and each professional should have minimum five (05) years of relevant experience.<br>5. Should have minimum specific experience of conducting ISO Assessment, Security Consultancy, Gap Analysis, VAPT and documentation for last five (05) years.<br>6. ISO Consultant's should have the following minimum qualification :<br>a) Bachelor's degree in Information Technology or relevant subject with at least ten (10) years work experience in similar or relevant field.<br>b) Experience of providing consultation in achieving ISO certification at least two (02) organizations.<br>7. The project manager should be CISSP/CISM and/or CISA/ISO 27001:2013 Lead Auditor certified professional with minimum five (05) years of experience.<br>8. Average annual Turn Over of the firm(s) should be minimum BDT 3,00,00,000/= during the last five (05) years (Summery sheet of Turn Over statement and year wise audited financial reports of the firm(s) should be enclosed).<br>9. Should have valid insurance coverage as required by ISO.<br>10. Certificate of Incorporation, valid Trade License, VAT/BIN certificate, latest income Tax clearance certificates (if applicable). |
| 3. | Other Details (if Applicable) | No data information will be allowed to be taken outside Bank in any form. |
| 4. | Association with foreign Firm is | Encouraged |

**Time Frame**

| 5. | Ref. No. | Phasing of Servces | Location | Indicative Start Data (Month/Year) | Indicative Completion Date (Month/Year) |
|---|---|---|---|---|---|
| 6. | Onsite Service: ISO 27001Scope optimization, Capacity Building, Pre Audit and Gap Assessment. | Phase-1 | Rajshahi | Duration: 09 weeks | |
| 7. | Onsite service: Gap Remediation & Review of ICT related Policies/procedures, etc. | Phase-2 | Rajshahi | Duration: 28 weeks | |
| 8. | Onsite service: ISO 27001 Certification including consultancy services, etc. | Phase-3 | Rajshahi | Duration: 19 weeks | |
| 9. | Onsite service: Consultancy services, Reporting for next 1 Year (2nd year) and 1st Surveillance audit. | Phase-4 | Rajshahi | Duration: 13 weeks | |
| 10. | Onsite service: Consultancy services, Reporting for next 1 Year (3rd year) and 2nd Surveillance audit. | Phase-5 | Rajshahi | Duration: 13 weeks | |

## 2. Present IT setup:

Rajshahi Krishi Unnayan Bank has been using Information Technology (IT) extensively for its day to day business operations. Information regarding IT has been furnished below:

| Sl. No | Area/ Subject | |
|---|---|---|
| 1 | No. of total Branches: | 383 |
| 2 | No. of computerized Branches: | 383 |
| 3 | No. of Online Branches using Ultimus, CBS- Version 3.0.2.6 | 383 including Head Office |
| 4 | No. of. Branches with internal LAN: | 383 |
| 5 | No. of total Employees: (as on December 2021) | 3727 |
| 6 | No. of total IT Employees | 34 |
| 7 | 3rd Party (with supplier name): | |

**Note:** All relevant information at actual (related to this project) such as DC, DRS/NDC and sophisticated others information will be provided to the awarded bidder after signing of NDA.

## 3. Detail Service Scope:

Details of the services are arranged under various stages and are given below:

### 1. Capacity Building

### SOCTraining:

| Phases | Trainings | Participating teams | Training Location |
|---|---|---|---|
| Phase 1 Foundation Training | Security Operations and Analysis | Events & IR - SA1 and SA2 | Local |
| | Hands on Training by using licensed VA & PT Tools | Vulnerability Assessment | Local |
| | Awareness & Implementation Training | Security and Networking | Local |
| | Certified Secure Computer User (CSCU) | security and networking | Local/Abroad |
| Phase 2 Intermediate | CEH with certification | Cyber Security | Abroad |
| | SIEM Design and Implementation | Events & IR - SA1 and SA2 | Abroad |
| | CISA- Certified Information Security Auditor | 3LOD and SOC Director | Abroad |
| | Open-Source Intelligence (OSINT) | Security and Networking | Abroad |
| | Cyber Threat Intelligence | Threat Intel | Abroad |
| Phase 3 Advanced | SIEM with Tactical Analytics | Events & IR - SA1 and SA2 | Abroad |
| | Malware Analysis | Threat Intel, Threat hunting, | Abroad |

## Training Details

| Phases | Trainings | Details |
|---|---|---|
| Phase 1 Foundation Training | Security Operations and Analysis | • Learn the stages of security operations: how data is collected, where it is collected, and how threats are identified within that data<br>• Dive deep into tactics for triage and investigation of events that are identified as malicious<br>• Discover how to avoid common mistakes and perform continual high-quality analysis<br>• Learn the inner workings of the most popular protocols, and how to identify weapon files as well as attacks within the hosts and data on their network |
| | Hands on Training by using licensed VA & PT Tools | • Cataloging assets and capabilities (resources) in a system.<br>• Assigning quantifiable value (or at least rank order) and importance to those resources<br>• Identifying the vulnerabilities or potential threats to each resource<br>• Mitigating or eliminating the most serious vulnerabilities for the most valuable resources |
| | Awareness & Implementation Training | • Security awareness to prevent and mitigate user risk.<br>• To help users and employees understand the role they play in helping to combat information security breaches.<br>• Formal education, such as structured lessons and mandatory instruction;<br>• Informational learning opportunities, such as weekly emails containing tips, policy updates and cyber security news updates;<br>• Experiential sessions and even gamification, where workers are required to work through simulations and scenarios to test their understanding and reinforce their training so they're better prepared to handle real-world cyber security challenges; and<br>• Security champions, workers who have become particularly skilled at understanding cyber security and are willing to teach and promote cyber security best practices among their colleagues. |
| | Certified Secure Computer User (CSCU) | • Provide necessary knowledge and skills to protect their information assets.<br>• Immerse into an interactive environment where they will acquire a fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, virus and backdoors, emails hoaxes, sex offenders lurking online, loss of confidential information, hacking attacks and social engineering. |

| | | |
|---|---|---|
| Phase 2 Intermediate | Certified Ethical Hacking (CEH) with certification | • Introduction to Ethical Hacking<br>• Foot printing and Reconnaissance<br>• Scanning Networks<br>• Enumeration<br>• Vulnerability Analysis<br>• System Hacking<br>• Malware Threats<br>• Sniffing<br>• Social Engineering<br>• Denial-of-Service<br>• Session Hijacking<br>• Evading IDS, Firewalls, and Honeypots<br>• Hacking Web Servers<br>• Hacking Web Applications<br>• SQL Injection<br>• Hacking Wireless Networks<br>• Hacking Mobile Platforms<br>• IoT Hacking<br>• Cloud Computing<br>• Cryptography |
| | SIEM Design and Implementation | • Build a SIEM from the ground up using Elastic Stack<br>• Dive into third-party integrations and dual-stack SIEMs<br>• Discover new ways to supplement and improve existing SIEM implementations<br>• Understand the basic stages of log collection, parsing, storage, and alerting |
| | CISA-Certified Information Security Auditor | • Provides a valid and reliable means to identify technologists who are competent in incorporating privacy by design into technology platforms, products and processes, communicating with legal professionals, and keeping the organization compliant efficiently and cost effectively.<br>• Identifies IT professionals as experts in IT testing, security and control.<br>• Information System Auditing Process<br>• Governance and Management of IT<br>• Information Systems Acquisition, Development and Implementation<br>• IS Operations and Business Resilience<br>• Information Asset Security and Control |
| | Open-Source Intelligence (OSINT) | • Entry point to learn about OSINT, the concepts and tools taught are far from basic.<br>• To **provide** the foundational knowledge to be successful in the fields, whether they are cyber defenders, threat intelligence analysts, private investigators, insurance fraud investigators, intelligence analysts, law enforcement personnel.<br>• Create an OSINT process<br>• Conduct OSINT investigations in support of a wide range of customers<br>• Understand the data collection life cycle<br>• Create a secure platform for data collection<br>• Analyze customer collection requirements<br>• Capture and record data<br>• Create sock puppet accounts<br>• Harvest web data<br>• Perform searches for people<br>• Access social media data<br>• Assess a remote location using online cameras and maps |

| | | |
|---|---|---|
| | | • Examine geolocated social media<br>• Research businesses<br>• Collect data from the dark web |
| | Cyber Threat Intelligence | • Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios<br>• Identify and create intelligence requirements through practices such as threat modeling<br>• Understand and develop skills in tactical, operational, and strategic-level threat intelligence<br>• Generate threat intelligence to detect, respond to, and defeat focused and targeted threats<br>• Learn the different sources to collect adversary data and how to exploit and pivot off of it<br>• Validate information received externally to minimize the costs of bad intelligence<br>• Create Indicators of Compromise (IOCs) in formats such as YARA, Open IOC, and STIX<br>• Move security maturity past IOCs into understanding and countering the behavioural tradecraft of threats<br>• Establish structured analytical techniques to be successful in any security role |
| Phase 3 Advanced | SIEM with Tactical Analytics | • Prepare for your GCDA GIAC Certification<br>• Create actionable dashboards for log parsing, early breach detection, and in-depth data analysis<br>• Develop methods to handle billions of logs from disparate data sources<br>• Learn to extract actionable intelligence for a tactical SOC |
| | Malware Analysis | • Build an isolated, controlled laboratory environment for analysing the code and behaviour of malicious programs<br>• Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment<br>• Uncover and analyse malicious JavaScript and other components of web pages, which are often used by exploit kits for drive-by attacks<br>• Control relevant aspects of the malicious program's behaviour through network traffic interception and code patching to perform effective malware analysis<br>• Use a disassembler and a debugger to examine the inner workings of malicious Windows executable.<br>• Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst<br>• Recognize and understand common assembly-level patterns in malicious code, such as code L injection, API hooking, and anti-analysis measures<br>• Assess the threat associated with malicious documents, such as PDF and Microsoft Office files<br>• Derive Indicators of Compromise (IOCs) from malicious executable to strengthen incident response and threat intelligence efforts |

**Note**: For SOC Training, the trainer must be professional and "Certified Trainer" in individual domain

**Digital Forensic Training:**

Training Duration: 05 Days each phase.

| Phases | Trainings | Participating teams | Training Location |
|---|---|---|---|
| Phase 1 Foundation Training | Hardware overview | All Digital Forensics team | Abroad |
| | Computer Forensic Foundation | All Digital Forensics team | |
| Phase 2 Intermediate | Access Data FTK Licensed Boot Camp- Digital Forensics | Computer Forensics | |
| | Hands on Digital Forensics Lab sessions | All Digital Forensics team | |
| Phase 3 Advanced | Mobile Forensic Foundation | Mobile Forensics Team | |
| | Oxygen Forensic Licensed Boot Camp- Mobile Forensics | Mobile Forensics Team | |

**Short Note of Digital Forensics Training:**

| Phases | Name | Description |
|---|---|---|
| Phase-1 | Hardware overview | The Digital Forensics with FRED course is designed for Forensic Examiners, eDiscovery Specialists and First Responders. This training highlights all of the features of the FRED forensic workstation and provides a basic foundation needed to utilize the equipment to complete a forensic preview, triage or duplicate copy. The course also covers optimal configuration and installation locations for the most popular digital forensic software along with maintenance and troubleshooting for the FRED.<br><br>Course attendees will gain a complete understanding of the features, functions, and capabilities of their new FRED Forensic Recovery of Evidence Device |
| | Computer Forensic Foundation | This entry-level course provides a solid foundation of knowledge and skills for beginning forensics and eDiscovery practitioners.<br><br>This course is designed to provide foundational skills for a digital forensic examiner, eDiscovery specialist, or first responder. Lessons presented will focus on:<br>• Identifying various digital forensic media<br>• Best practice collection of digital media / evidence<br>• Best practice transportation of digital media / evidence<br>• Forensic triage methods<br>• Duplicating digital media / evidence |
| Phsae-2 | Access Data FTK Licensed Boot Camp Digital Forensics | Digital Intelligence's Access Data FTK Boot Camp (DFFAD) is a comprehensive, this course designed to provide the knowledge and skills necessary to conduct digital acquisitions and investigations using FTK Toolkit.<br><br>Students who attend DFFAD are invited to take the Digital Forensics with FRED (DFF) class at no additional charge. DFFAD is taught Tuesday-through-Thursday so students can combine DFFAD with the one-day DFF class offered on Mondays. This makes the best use of each student's travel time and maximizes hands-on instruction with the combined FRED + FTK solution.<br><br>Upon course completion, attendees should be able to:<br>• Install Access Data software tools<br>• Image, acquire, export, and create forensic images |

| | | |
|---|---|---|
| | | • Access and review registry entries<br>• Create a case, process and analyse documents, metadata, graphics, and e-mails using FTK<br>• Use bookmarks / checkmarks to efficiently manage and process a case<br>• Update / customize the KFF database<br>• Manage evidence using file filters<br>• Perform searches using regular expressions and imported search lists<br>• Carve unallocated disk space<br>• Create and customize reports<br>• Recover passwords using PRTK<br>• Gain practical experience with FTK indexing<br>• Create custom dictionaries using the FTK indexing<br>• Create regular expressions<br>• Use Registry Viewer to locate evidentiary information in Windows 2000 and Windows XP<br>• Integrate Registry Viewer with FTK<br>• Recover forensic information from Recycle Bin INDO2 files<br>• Recovery forensic information from various Windows XP artifacts<br>• Create a PRTK custom dictionary using an FTK word list<br>• Add SAM and Syskey values to PRTK to recover passwords and decrypt files<br>• Recover EFS encrypted files on Windows 2000 and Windows XP systems |
| | Hands on Digital Forensics Lab sessions | The Most Important part of the Training. The hands-on cases would explored during this session. |
| Phase-3 | Mobile Forensic Foundation | This entry-level course provides a solid foundation of knowledge and skills for beginning mobile forensics and eDiscovery practitioners. |
| | Oxygen Forensic Licensed Boot Camp Mobile Forensics | This instructor-led training event is geared toward students that have a working familiarity with mobile device acquisition and extraction. This course does not provide hands-on extraction of mobile devices. That topic matter is available in the Oxygen Forensic® Data Extraction course. This course focuses on the analytic analysis and reporting capabilities of the Oxygen Forensic® 12.0 Detective powered by Jet Engine. |

**Note:** For Forensic Training, the trainer must be professional and "Certified Trainer" in individual domain

**ISO Lead Auditor Training with Certification :**

1) **Information Security Management Standard- (ISMS) ISO 27001:2013 – Lead Auditor Training**

## Vendor Response

### Information Security Management Standard (ISMS) - ISO 27001

| Sl No | Area/Domain | Requirements / Descriptions | Document Reference & Response |
|---|---|---|---|
| 01 | Area to be covered | 1) Information Security and International Standards<br>2) Information System Security Requirements<br>3) Security Policy<br>4) Security Organization<br>5) Asset Classification and Control<br>6) Personnel Security<br>7) Physical and Environmental Security<br>8) Communication<br>9) Operations Management<br>10) Access Control<br>11) System Development and Maintenance<br>12) Business Continuity Management<br>13) Compliance<br>14) Identification of ISO 27001 Controls. | |
| 02 | Duration | 5 Full Days (40 Hours) | |
| 03 | Number of Participants | 10 | |
| 04 | Framework to Follow | Capacity Building must follow the latest international recognized/ attested framework/ syllabus i.e. ISO | |
| 05 | Training Venue | Training will be delivered different location in Bangladesh (outside of Dhaka). | |
| 06 | Facilities | Service provider will provide training infrastructure including training hall, projector, white board, papers a laser printer, trainer, training materials, transport, accommodation (minimum 3 Star hotel), travel expenditure (e.g. plane fair), pickup and dropping services and food & beverage. | |
| 07 | Trainer's Track Record | Trainer must have track record in providing training engagement in national or international training institute/ organization. | |
| 08 | Trainer Qualification | Trainer should be certified on the below domain/subject:<br>1) ISO 27001 Certified Trainer/Certified in Information Security Management Standard (ISMS)/ISO 27001 LA | |
| 09 | Trainer's Profile | For conducting Capacity Building training, 02 profiles of the trainers must be submitted with the consent letter from the trainer. | |
| 10 | Trainer Practical Knowledge | Beside theoretical knowledge, trainer is preferred to have hands on practical ITES operational as well as implementation expertise in financial sector (banking and non-banking). | |
| 11 | Training as Core Activities | For training, the trainer must be a professional trainer. His/her profession must be under similar type of organization (trainer should not be a service holder – giving training as an optional service). | |
| 12 | Track Record for Service Provider (Training) | Details of mentionable IS Training Projects done by Service Provider in previous 3 years. | |
| 13 | Certification Examination | Instructor Led (IRCA) Certification should be included | |

## 4. Preparatory Consultation for ISO Certification of Rajshahi Krishi Unnayan Bank–

Taking ISO Preparatory Consultation Services will assist us to reduce time and man day cost for achieving organizational ISO Accreditation. At this stage, we wish to get consultation services from a service provider who will prepare us in an integrated approach to get ISO 27001for Bank.

| Subject/Area | Requirements / Descriptions | Document Reference & Response |
|---|---|---|
| 1) Information Security Management Standards (ISMS) - ISO27001 Consultation | | |
| Domain | Domain:<br>a. Business Gap Analysis<br>b. Assisting for identifying Management Representative<br>c. Work plan for security management<br>d. Training and documentation for achieving the Information Security Management Standard Certification (ISO 27001).<br>e. Finally assist for the certification | |
| Durations | 90 Man Days (within 03 Calendar Months) | |
| **Scope for ISO** | IT Department (including DC & DRS) | |
| Deliverables | The consultation firm will ensure through individual team (from the bank) to build manuals and also assist the said teams to make necessary processes i.e. SOP (Standing Operation Procedure), various policies and other required documentation for achieving the required standard toward the accreditation. One set of hard copy and softcopy (in MS Word format) of the total work have to be submitted. | |
| Starting Time | i. The selected consultation firm will be required to start the project within 30 days from the date of placing the order for the consultation (ISO preparatory). | |
| | ii. completed within timeframe specified. It is expected that the consultation firm may deploy multiple teams to complete the projects within given time frame. | |
| Experience | Consultation Firm should have expertise and similar type of experience in Bangladesh, specially in Banking Industry (for all the ISO mentioned above). | |

**Deliverables**

The consultation firm will ensure through individual team (from the bank) to build manuals and also assist the said teams to make necessary processes i.e. SOP (Standing Operation Procedure), various policies and other required documentation for achieving the required standard toward the accreditation. One set of hard copy and softcopy (in MS Word format) of the total work have to be submitted.

## Vendor Response

## Preparatory Consultation for ISO Certification of Rajshahi Krishi Unnayan Bank

| Sl No | Requirements | Document Reference & response |
|---|---|---|
| 01 | Existence in Last 05 year (provide necessary proof like -<br>1) Trade License/Certificate of Incorporation | |
| 02 | Consulting firm (Bangladesh Based), must have completed/engaged similar volume/numbers (ISO 9001, ISO 27001 and ISO 20000) of services in the recent past as Integrated Management system (IMS). | |
| 03 | Consulting firm (main bidder) should have 03 (three) IRCA Certified ISO 9001 LA for Quality Management System (QMS), 03 IRCA Certified 27001 LA (Lead Auditor)/Certified ISMS (Information Security Management Standard), 03 IRCA Certified ISO 20000 LA Furthermore, 02 Project management professional and 03 Certified ITIL beside ISO Accreditation Firm. | |
| 04 | Consulting firm should have experience on similar as well as same volume of Preparatory Consultation on ISO services providing and liaison with External ISO Audit firm for achieving organizational ISO Accreditation (completed/engaged) in the recent past in any financial institution of Bangladesh e.g. bank. | |

### Technical Documentation

As part of Business Continuity as well as second line of protection, RAKUB has decided to go for documenting ("Technical Documentation") of its all Information Technology Enabled Services (ITES) for meeting. And for meeting this, bank wish to select service provider(s) having core competence as well as similar expertise in assessing/ evaluating and assisting a technical team from client organization for the preparation of "Technical Documentation" of IT Enable Service (ITES).

Service provider will extend review of the related documentation and make all the "Technical Documentations based on ISO need (end to end).

## Vendor Response

| SL No | Task Name | | Document Reference & Response |
|---|---|---|---|
| 01. | **ROC, AOC and COC:**<br>ROC-Offsite<br>AOC-offsite | I. The bidder shall arrange all the necessary arrangement for the Report on Compliance (ROC), Attestation of Compliance (AOC) and Certification of Compliance (COC). | |
| 02 | **Duration** | 15 Days | |

**1) Certificate maintenance for 02 year after initial certification**

**POST CERTIFICATION COMPLIANCE (To Be Continuous Process)**
**Object Breakdown**
**Post Certification ongoing compliance**

Deliverable to the Bank
Quarterly scan report by ASV (Approved Scanning Vendors)

- VA, PT and other scans reports.
- Report on compliance.
- Attestation of compliance.
- Certificate of the compliance.
- Other required services not covered here for recertification.

Work Breakdown
Maintain:
ISO Maintenance Assistance and Advisory Service

- Unlimited Clarification support and access to ISO Security Expert by email & / or phone
- Provide access to online ISO Awareness & Training programs
- Provide access to Data Security Policies and Procedure Templates
- Provide access to Data Security Literature, information brochure
- Provide access to project methodology and templates

## 5. ISO Certification for RAKUB:

1) ISO Certification for Organization ISO 27001 (Information Security Graded/ ISMS)

## Vendor Response

### ISO (External Audit): Basic

| Subject | Requirements/Descriptions | Document Reference & Response |
|---|---|---|
| | **ISO 27001** | |
| **Deliverables** | The firm should first assess the existing environment, do a gap analysis then do the third-party audit, recommend against the observation, follow up the remedies by the organization and remain in the loop for ISO Accreditation | |
| **Time frame** | 1) The accreditation services will be required to start the project within 30 days from the date of placing the order for the accreditation (ISO).<br>2) The accreditation services will not be time bound. If the bank seems ready for the audit, third party audit must be completed by approximately 7/10 Man Days for each ISO.<br>3) If the organization seems to be ready for third party audit for accreditation, the auditing firm shall complete the said service latest by 1 calendar month (treating the service starting day after the work order as the first day) for each ISO certification. | |

## Vendor Response

### ISO (External Audit): General

| Sl No | Requirements | Document Reference & response |
|---|---|---|
| *External ISO Audit Firm* | | |
| 01 | Existence in Last 05 year (provide necessary proof like -<br>2) certificate of Incorporation (for Bangladeshi/Bangladesh Based firm) or<br>3) Deed of partnership (in case ISO Firm is Foreign Firm)/ Proof of JVCA | |

| | | |
|---|---|---|
| 02 | Participating organization must be a direct part of International ISO Certification Body. | |
| 03 | External ISO Audit firm must provide proof of ISO accreditation services as the core activity of the ISO Audit firm. | |
| 04 | ISO External Audit Firm must have at least 05 certified clients on each ISOs i.e. ISO 9001, ISO 27001 & ISO 20000 | |
| *ISO Coordinating Firm* | | |
| 05 | Coordinating vendor (Bangladesh Based), must have completed/engaged similar volume/numbers (ISO 9001, ISO 27001 and ISO 20000) of services in the recent past as Integrated Management system (IMS). | |
| 06 | Coordinating vendor (main bidder) should have 03 (three) IRCA Certified ISO 9001 LA for Quality Management System (QMS), 03 IRCA Certified 27001 LA (Lead Auditor) / Certified ISMS (Information Security Management Standard), 03 IRCA Certified ISO 20000 LA<br>Furthermore, 02 Project management professional and 03 Certified ITIL beside ISO Accreditation Firm. | |
| 07 | Coordinating Bidder Company should have experience on similar as well as same volume of Preparatory Consultation on ISO services providing and liaison with External ISO Audit firm for achieving organizational ISO Accreditation (completed/engaged) in the recent past in any financial institution of Bangladesh e.g. bank. | |

**Deliverables**

The firm should first assess the existing environment, do a gap analysis then do the third-party audit, recommend against the observation, follow up the remedies by the organization and remain in the loop for ISO Accreditation (here ISO 27001).

## 6. Other Services:

All services within various stages must be compliant with RFP. Service Provider will comply with supporting services beyond the scope of this RFP without any financial involvement (within pre-defined timeframe).

## 7. Support from the Bank

Based on the service(s), representative from bank will be assisting the service provider as and when required.

## 8. Selection process

Purchaser will evaluate proposals of the Respondents on the basis of Financial Status and Technical Capability of the respondent and also the track record of successful delivering /implementation of the products/services required by the Bank. Therefore, respondents should submit necessary details that would help evaluation. Their response submitted should contain the respondent's proposed solution covering all the requirements and scope of "Information Systems Audit, Vulnerability Assessment & Penetration Testing, Complete Technical Documentations, Consultation Services for the assistance of Selecting Composite Information System/Information Technology (IS/IT) Security Solution, Preparatory Consultation for ISO Accreditation and External Audit for ISO Certification, Capacity Building of RAKUB" listed in Requirements Section (3).