



**UCO BANK**

**INVITES**

**EXPRESSION OF INTEREST (EOI)**

**FOR**

**INFORMATION SYSTEMS**

**SECURITY AUDIT (ISSA)**

**Department of Information Technology**

**Head Office**

**Kolkata-700064**



**UCO Bank**

Head Office

Dept. of Information Technology  
3 & 4, DD Block, Sector-1, Salt Lake  
Kolkata – 700.064

**Invitation for Expression of Interest for  
Information Systems Security Audit**

**Date: 02-11-2010**

**1. Background**

UCO Bank, a leading Public Sector Bank headquartered in Kolkata has implemented many key technology solutions like 100% Core Banking (CBS), Internet Banking (e-banking), Mobile Banking, ATMs, Integrated Treasury System, RTGS, SFMS, NEFT etc. The bank is using *Finacle* Software of M/s. Infosys Technologies Ltd. as the Core Banking Solution . The bank's Primary Data Centre (BDC) is located at Bangalore. The Department of Information Technology, H.O. as well as the Disaster Recovery Data Centre (KDC) are located at H.O.-2,Kolkata. The Bank's Treasury & Payment Gateway Primary site is located at its Integrated Treasury Branch, Mumbai and the related DR Site is located at International Wing, Head Office-1, Kolkata. The bank has 18 Network Access Points (NAPs) across the country. The ATM switch Centre of our bank, which is hosted by M/s. FSS is located at Chennai.

The Bank intends to appoint Information Systems Security Auditor to conduct Information Systems Security Audit at above mentioned locations.

**2. Eligibility Criteria**

- 2.1. The Bidder must be a limited company or a registered partnership firm having its registered office in India (Documentary evidence must be submitted).
- 2.2. The Bidder must be engaged in the business of Information System auditing (IS Auditing) in India at least for last three years.
- 2.3. The Bidder must have completed System Audit, in last two Financial years, in at least two (02) Public Sector Banks in India. ( Documentary proofs must be provided as per format given in Annexure-3 along with copies of Work Order/Certificates etc.).
- 2.4. The Bidder must have at least two (2) resources with adequate knowledge and prior experience of each of the applications to be put to audit.
- 2.5. The Bidder must be a profit making firm/company for each of the last three years (Documentary evidence must be submitted).
- 2.6. The Bidder should have reported a turnover of at least Rs.5 crore in each of the last three financial years.

- 2.7. The Bidder must have on their rolls, on permanent employment basis, a minimum of 10 (ten nos.) System audit professionals who are qualified with any one or more certifications in CISA/DISA/CISSP/CISM/CCNA/CCNP/OCP/ ISO 27001 LA/ BS 7799 LA etc.
- 2.8. The bidder should not have been a vendor of IT equipment/peripherals/software/services to UCO Bank in the past 3 years.
- 2.9. The bidder should not have been blacklisted by any Public Sector Bank/ RBI/IBA or any other Government agency/ICAI. A declaration to this effect must be submitted by the bidder along with EOI.
- 2.10. Bidders must certify that no legal action is pending against them for any cause in any legal jurisdiction. If such actions are pending, the Bidder must provide details of such action(s). A declaration to this effect must be submitted by the bidder along with EOI.

### 3. Purpose of Audit:

To conduct IS audit at Bank's Data Center, Disaster Recovery Site, Integrated Treasury branch, Treasury DR Site, NAPs, ATM Switch/Centre providing independent reasonable assurance to the Bank on:

- Robust IT security.
- Mitigation of risks where there are significant control weaknesses.
- Safeguarding the information assets viz. hardware, network etc.
- Maintaining security, confidentiality, integrity and availability of data
- Efficient utilization of resources-IT.
- Ensuring compliance of IT Security Policy and procedures defined by the Bank.
- Providing minimum domain wise baseline security standard / practices in a checklist format to be implemented to achieve a reasonably secure IT environment for technologies deployed at UCO Bank separately for Servers, DBMS, network equipments, security equipments etc.

### 4. Scope of Audit:

4.1. A comprehensive Information Systems Security Audit has to be undertaken covering the various key processes and procedures undertaken at the following locations / sites:-

- i) Dept. of IT, Head Office-2, Kolkata wherein the bank's DR Data Centre(KDC) is located.
- ii) Bank's Primary Data Centre at Bangalore (BDC).
- iii) Integrated Treasury Branch, Mumbai  
(Treasury & Payment Gateway Primary Site)
- iv) Treasury & Payment Gateway DR Site at Head Office-1, Kolkata
- v) ATM Switch Centre (hosted by M/s. FSS) at Chennai.
- vi) Network Access Points at 18 locations across India.

4.2. The IS Audit shall include, but not be limited, to the following : -

#### 4.2.1. Data Centre facilities audit

The **Data Centre facilities Audit** at the above mentioned sites shall cover following aspects:-

- a. Building Management Systems
- b. Power Supply, UPS & DG
- c. Physical Access Controls
- d. Environment Control
- e. Data centre infrastructure - network cabling, raceways, server /Communication racks, Rack Power Distribution Units (PDU), KVM
- f. Fire & Smoke, Water leak Detection and suppression Systems
- g. Air-conditioning :-Temperature & Humidity control systems
- h. Assets safeguarding, Handling of movement of Man /Material/Media/ Backup / Software/ Hardware / Information.
- i. Surveillance systems.
- j. Pest prevention (rodent prevention) systems.

#### **4.2.2. Operating System Audit**

The Operating System audit shall cover following aspects for Servers, Databases, network equipments, Security Systems, Storage Area Networks at above mentioned sites as given in Sl. No. 4.1.

- a. Set up and maintenance of system parameters
- b. Patch Management
- c. Change Management Procedures
- d. Logical Access Controls
- e. User Management & Security
- f. OS Hardening
- g. Performance, Scalability and Availability

#### **4.2.3. Application Audit**

The important Application Softwares which are being used in our Bank are Finacle of M/s. Infosys, Kastle of M/s. 3i Infotech, Panacea AML Package of M/s. Lasersoft, Reuter, ATM switch (Base 24) of M/s. FSS, LAPS, SWIFT, RBI & CCIL Applications, Various Applications presently in use at Treasury branch, Mumbai etc. The Application audit shall cover following aspects:-

- a. Functionality implemented vis-à-vis the Bank's Requirements.
- b. Input, processing and output controls across various schemes across the bank.
- c. Controls for performing parameter setup of functionality across applications.
- d. Segregation of duties .
- e. Accuracy, adequacy and integrity of data in reports and MIS.
- f. Availability of necessary audit logs and its accuracy and effectiveness.
- g. Adherence of reporting to legal and statutory Requirements.
- h. Automated batch processing, scheduled tasks, critical calculations etc.
- i. End of Day, Start of Day, period closure operations including End of Month, End of Quarter and End of Year operations.

- j. Integration with Delivery Channels including data and transaction integrity for the same
- k. Release of software governed by formal procedures - ensuring sign-off through testing, handover, etc.
- l. Formal procedure for change management being adopted.
- m. Impact analysis of changes made.
- n. Associated documents and procedures- being/to be updated accordingly.
- o. Maintenance personnel have specific assignments and that their work is properly monitored. Their system access rights are controlled to avoid risks of unauthorised access to automated systems.
- p. Access log is monitored.
- q. Regular updation of job cards with new version releases.
- r. If outsourced, escrow arrangement with application vendors.
- s. Tracing of all High value transactions
- t. Verification of number of Branch Head (BH) and Asstt. Branch Head (ABH) for branches.
- u. Interfacing between Finacle and various Forex/Treasury Applications.

#### **4.2.4. Database Audit**

The Database audit shall cover following aspects:--

- a. Authorization, authentication and access control review.
- b. Audit of data integrity controls.
- c. Database Backup Management.
- d. Review of database privileges assigned to DBAs/Users.
- e. Security of Oracle systems files.
- f. Synchronization between KDC & BDC Databases for CBS/ Alternate Delivery channels(ADC) and between Treasury Primary Database at Mumbai and Treasury DR Database at HO-1,Kolkata.
- g. Patch Management.
- h. Review of control procedures for changes to parameter files.
- i. Review of Control procedures for sensitive DB passwords.
- j. Review of Control procedures for purging of Data Files.
- k. Review of Procedures for data backup, restoration, recovery and readability of backed up data.

#### **4.2.5. Network Audit**

The Network audit shall cover following aspects:--

- a. Overall Network management.
- b. Network architecture/design review
- c. Network cabling is structured.
- d. Network traffic analysis and base lining
- e. Virtual LANS (VLANs)
- f. Evaluate procedures adopted for:
  - i. Secured transmission of data through dialup/leased line/VPN/VSATs,wireless etc.
  - ii. Bandwidth management
  - iii. Uptime of network -- its monitoring as per SLA.

- iv. Fault management
- v. Capacity planning
- vi. Performance management .
- vii. Monitoring of logs.
- g. Verification of Network Devices for any security threats
- h. Configuration and Access control audit for all Networking Devices viz. Routers, Switches, IDS/ IPS, Firewalls etc.

#### **4.2.6. Security Management Review**

The **Security Management Review** shall cover following aspects:--

- a. Security Equipment Configurations & Policies.
- b. Penetration testing and Vulnerability Assessment (PT / VA) of various security zones/Networks/Delivery channels.
- c. Maintenance of necessary logs.

#### **4.2.7. Delivery Channels Review/Audit**

**I). The ATM Centre/Switch Audit** shall cover following aspects:--

- a. ATM centre management :
  - 1) PIN Management
  - 2) Card Management
  - 3) Time Management in delivering ATM Card/PIN to Customers.
  - 4) Hot listing of cards.
- b. ATM helpdesk and monitoring.
- c. Branch procedures.
- d. Reconciliation:-Visa/NFS Chargeback procedures.
- e. Card Printing/Despatch.
- f. ATM Switch setup, configuration, Security and control.
- g. ATM Switch operational controls, Consortium issues &
- h. Reconciliation/Functional Managerial activities.
- i. Monitoring procedure of ATM's Status (Uptime/down time).
- j. Processing of requests received through Integrated Request Processing system (IRPS).
- k. Review of Prognosis
- l. Interface systems.
- m. Offsite Security Services.

**II). e-Banking Audit** shall cover following aspects:--

- a. Bank's internet banking product line, transaction flow.
- b. Review on internal controls in place to minimize errors & frauds.
- c. Interface with other organizations for utility payments.
- d. Interface with other applications.
- e. Process of creation/Activation/Resetting/delivery of internet banking user ids/ passwords.
- f. Password/PIN management.
- g. Authentication controls.
- h. Vulnerability/ Threat Assessment
- i. External Penetration Testing

#### **4.2.8. Review of IT Processes and IT Management Tools**

The review of IT Processes and Management tools shall cover

following aspects:--

- a. IT Asset Management
- b. Enterprise Management System
- c. Help Desk
- d. Change Management
- e. Incident Management
- f. Network Management
- g. Backup & Media Management
- h. Anti-Virus Management
- i. Vendor & SLA Management

#### **4.2.9. IT Policies review**

An assessment/review of all the important Policies/Procedure Documents of the Bank such as

- a. Information Technology Policy
- b. Information System Security Policy
- c. Disaster Recovery Policy
- d. Data Purging Policy
- e. ATM Policy
- f. E-Banking Policy
- g. Mobile Banking Policy
- h. Outsourcing Policy
- i. Any other policies which are not listed above and are in force

#### **4.2.10. Migration Audit**

Compliance review of Post Migration Audit of 1065 branches migrated on or after 11-09-2009 and review of migration of branches to CBS prior to the above date.

#### **4.2.11. Payment Gateway Audit**

Verification of controls for RTGS, NEFT, SFMS, SWIFT, NFS etc. at Payment Gateway, as per the regulator's policies and guidelines.

#### **4.2.12. Registration Authority (RA) Office Audit**

**Registration Authority (RA) Audit** shall cover following aspects:--

- a. Audit of all RA functions
- b. Compliance to the requirements of IT act 2000, Rules and Regulations.
- c. Compliance of RA functions as per IDRBT checklist.
- d. Reconciliation of digital signatures issued/ revoked by RA with IDRBT.
- e. Digital Certificates details/record maintenance as per IDRBT requirements.

#### **4.2.13. Others**

- a. Privileges available to Systems Integrator and Outsourced Vendors.
- b. Evaluate role, responsibility and accountability of IT Process owners.
- c. Review of DR Drills undertaken for CBS/ADC & other delivery channels at Treasury branch and reports thereof Comments on sufficiency and periodicity etc. of DR Drills undertaken and planned.

- d. Audit of anti virus protection at host and at desktop levels, procedure of antivirus updates at DC, Servers and Desktops, Gateway level AV protection etc.

## 5. Submission of EOI:

- 5.1. Interested Audit/Inspection firms/Companies may submit, in sealed envelope , their Expression of Interest, duly signed by the authorized signatory. The envelope must be superscribed with “**Expression of Interest for Information System Audit of UCO Bank**”, and has to be dropped in the Tender Box located at 5<sup>th</sup>. Floor of our Head Office, DIT at following address:-

General Manager (I.T.)  
UCO Bank,  
Department of Information Technology  
Head Office  
3 & 4, DD Block, Sector-1, Salt Lake  
Kolkata – 700 064

- 5.2. The Expression of Interest must be accompanied by the documents as listed in the annexure-5.
- 5.3. Responses must reach the above referred address on or before **30-11-2010 at 13:00 hours IST**. EOIs received after the prescribed date and time will not be entertained. In case of the designated day being declared a public holiday, the same may be extended to next working day.
- 5.4. The proposal should be submitted strictly in the format provided and should be signed by the authorized signatory with seal of the Company.

## 6. Evaluation and Comparison of EOIs:

- 6.1. The Bank will make a preliminary examination of the EOIs to determine whether the concerns are eligible as per terms of Eligibility Criteria, whether the proposals are complete, , whether the documents are properly signed and whether the EOIs are generally in order. The Bank, at its discretion, may waive any minor informality, nonconformity or irregularity in an EOI.
- 6.2. The Bank, with its own internal people or with the help of its consultant, will evaluate the EOIs.
- 6.3. Based on the documents submitted with the EOI, UCO Bank will, short list the vendors using a set of criteria, as per the annexure-8. The eligible bidder, to qualify, must secure at least 50% marks each in each Category. A detailed 'Request for Proposal' will be issued to the short-listed vendors to elicit detailed information about the proposed IS Audit , in UCO Bank's own structured format, for further evaluation.

## 7. General Terms and conditions:

- 7.1. Any effort by a Bidder to influence the Bank in its decisions for Evaluation and Comparison of EOIs or Contract Award may result in the rejection of the EOI submitted by the Bidder.
- 7.2. The Bank reserves the right to accept/ reject, at any stage of the process, any or all offers submitted in response to this invitation for *Expression of Interest*, and/or to modify the process or any thereof at any time without assigning any reason whatsoever and without any obligation or liability whatsoever.

- 7.3. The Bank reserves the right to short list vendors based on the requirement of the Bank. The Bank may short list vendors separately for each scope/ area as specified in the SCOPE OF WORK as deemed necessary. The decision of the Bank in this regard shall be final.
- 7.4. No further discussion/ interface will be granted to Bidders whose offers have been disqualified for any reason.
- 7.5. Notwithstanding anything contained herein above, in case of any dispute claim and /or legal action arising out of this invitation, the same shall be subject to the jurisdiction of courts at Kolkata only.
- 7.6. The Bank reserves the right to make any changes in the terms and conditions stated above and/or to annul the process.

**\*\*Please Note: This is not a Request for Proposal (RFP) and no commercial bids are required to be submitted with "Expression of Interest".**

---

**Vendor's Profile**

		Attach Separate Sheet, if required
<b>1</b>	<b>Basic Information</b>	
	Company Name	
	Constitution	Registered Partnership Firm / Private Ltd / Public Ltd (Attach Copy of certificate of incorporation/registration).
	Date of Incorporation	
	Corporate Office Address	
	Contact Person	
	Designation	
	Landline No.	
	Mobile No.	
	Fax No.	
	Email Id	
	Address of other centres where the bidder organization is having office	
	Name and Addresses of Directors / Promoters	
	Details of Organizational Structure	
	No. of years in the business of IS Audit / IS Security services	
<b>2</b>	<b>Financial Information</b>	
	<b>Turnover</b> ( Last 3 Years) ( In Rs. Lakhs) 1) 2) 3) (Please attach Audited Balance Sheet for these 3 years)	
	<b>Net Profit</b> ( Last 3 Years) ( In Rs. Lakhs) 1). 2). 3). (Please attach Audited Profit & Loss Statement for these 3 years)	
<b>3</b>	<b>Technical Information</b>	
	a) Levels of Certification Obtained	
	b) No of Technical Staff	
	Hardware	
	Software	
	Network & Telecommunications	
	Database	
	Project Management	
	c) No. of Staff having following Certifications CISA CISSP CISM CCNA / CCNP OCP BS-7799 LA / ISO 27001 LA Others	Please provide - in a separate sheet - names of personnel, their professional certification, years of experience in relevant area.etc in the format as provided in Annexure -2.
	d) Past Experience in conducting IS Audit / IT Security Audits for Bank and/or Financial institutions during the last 3 years	Please attach separate sheet giving detail and support documents.
	e) Name, Address, Telephone Nos. and email of contact persons of the clients where similar assignment was successfully completed in the last 2 years.	Please provide in a separate sheet in the format as provided in Annexure -3.

( Signature of Authorised Signatory with seal )

**CV of Professional Personnel/Staff  
(to be furnished on a separate sheet for each employee)**

Name of Staff			
Date of Birth			
Professional Qualifications/ Certifications			
Services in the firm from			
Previous employment record	Organization	From	To
Details of key assignments handled in the past three years			
Organization	Month and year	Details of assignment done	

**(Signature of Authorised Signatory with seal )**

**References of IS Audits done for Banks.**

(The details of each assignment should be furnished on a separate page. The details should relate to the assignments done during the past two years. We expect four or five references in the minimum)

<b>1</b>	Name of the Bank	
<b>2</b>	Address	
<b>3</b>	Name of the Contact Person	
<b>4</b>	Designation	
<b>5</b>	Direct Phone number	
<b>6</b>	Mobile Phone	
<b>7</b>	E-mail id	
<b>8</b>	Month & Year in which IS Audit was conducted	
<b>9</b>	Names of professional personnel who carried out that assignment	
<b>10</b>	Brief particulars of the Systems for which IS audit was done.	

**(Signature of Authorised Signatory with seal )**

**Proposed Methodology & Work Plan**

(Please mention the details of tasks you propose to do along with the estimates of time lines for each task, the key personnel you intend to engage for each of the tasks in the assignment and the deliverables for each task. In other words, this sheet should provide the entire project plan)

<b>Sl. No.</b>	<b>Details of tasks</b>	<b>Estimated Time lines</b>	<b>Details of Key Personnel to be engaged</b>	<b>Deliverables</b>

**(Signature of Authorised Signatory with seal )**

**CHECKLIST FOR DOCUMENTS TO BE SUBMITTED**

The Firms who are submitting the EOI are requested to fill this checklist and also to ensure that the details/ documents have been furnished as called for in this bidding document.

Please tick ( ) the Yes/No box for this details furnished in the EOI and enclose the documents in the given order.

<b>Sl.No.</b>	<b>Document</b>	<b>Particular</b>	<b>Yes/No</b>
1	Vendor's Profile (in Annexure-1)	Vendor's details	
2	Certificate of incorporation/ Registration	Constitution details	
3	Audited Balance Sheets and Profit & Loss Statements	Copy of balance sheets and P&L statements for last three financial years	
4	Proof of Turnover ,Net Worth & Net Profit (in Annexure-7)		
5	CVs of Professional Personnel/Staffs (in Annexure-2)	Professional's details	
6	Clientele List (in Annexure -3)	References of IS Audits done for Banks/Financial institutions.	
7	Work Order copies	Proof of Experience	
8	Proposed Methodology & Work Plan (in Annexure-4)	Project Plan	
9	Undertaking by the Bidder (Annexure-6)		

**(Signature of Authorised Signatory with seal )**

**Undertaking by the Bidder**

To,  
The General Manager(IT) ,  
UCO Bank,  
Department of Information Technology  
Head Office, 7<sup>th</sup>. Floor,  
3 & 4 DD Block,  
Sector-I, Salt Lake  
Kolkata—700064

Dear Sir,

**Reg: Our Expression of Interest (EOI) for IS audit of UCO Bank**

- a) We hereby confirm that we have read and understood the eligibility criteria and fulfill the same.
- b) We further confirm that all the information as per requirement of the Bank have been included in our EOI.
- c) Further, we hereby undertake and agree to abide by all the terms and conditions and guidelines stipulated by the Bank. We understand that any deviation may result in disqualification of our EOI.
- d) We have not been blacklisted by any Nationalised Bank/ RBI/IBA or any other Government agency/ICAI. No legal action is pending against us for any cause in any legal jurisdiction.
- e) We undertake that adequate number of qualified auditors will be deployed for audit process to complete the audit within stipulated time.
- f) We undertake that we will have legal right to use any third party software if required for audit and under such licenses, in terms set out under any relevant license or sublicense agreement. We will indemnify the Bank for any and all costs that may arise out of the use of software, in which it is alleged that any rights of the owners of such software have been infringed.

(Deviation to the above if any, the Bidder must provide details of such action (s).)

- 1)
- 2)
- 3)
- 4)

**(Signature and the capacity of the person duly authorized to sign Bid for and on behalf of)**

**Financial Position of the Bidder \*\*****Name of Bidding Firm/Company:** \_\_\_\_\_

	<b>Year 1</b>	<b>Year 2</b>	<b>Year 3</b>
<b>Year</b>			
Overall Turnover (Rs. In crores)			
Net Worth (Rs. In crores)			
Net Profit (Rs. In Lakhs)			

**(Signature of Chartered Accountant with seal )**

\*\* This to be certified by CA and certified copy of Balance sheet to be enclosed for each year..

---

**Annexure-8 (Evaluation of EOIs for IS Audit of UCO Bank)**

Basis of scoring													
SI No.	Parameter	Criterion	Marks out of 10	Criterion	Marks out of 10	Criterion	Marks out of 10	Criterion	Marks out of 10	Criterion	Marks out of 10	Criterion	Marks out of 10
1	<b>COMPANY'S PROFILE – 'A'</b>												
1.1	Date of Commencement of business	More than 6 years ago	10	Above 5 years up to 6 years ago	8	Above 4 years up to 5 years ago	6	Above 3 years up to 4 years ago	4	Above 2 Less than 3 years	2		
1.2	Main Activity	Proposed Service is their core activity	10	Proposed Service is one of their activities	5	-	-	-	-	-	-		
1.3	Constitution	Public limited company	10	Private limited company	8	Partnership	6	-	-	-	-		
1.4	<b>FINANCIAL POSITION Over the last Three years:-</b>												
1.4.1	Overall Turnover	Above 10 Crores	10	Above 8 upto 10 crores	8	Above 6 Crores upto 8 crores	6	Above 4 Crores upto 5 crores	4	-	-		
1.4.2	Net Worth	Above 5 Crores	10	Above 4 Crores upto 5 crores	8	Above 3 Crores upto 4 crores	6	Above 2 Crores upto 3 crores	4	Less than 2 crores	2		
1.4.3	Net Profit (PAT)	Above 1.5 Crores	10	Above 1.0 Crores up to 1.5 Crores	8	Above 0.5 Crores up to 1.0 Crores	6	Above 0.1 0 Crores up to 0.5 Crores	4	Less than 0.10 Crore	2		
1.4.4	Growth in profitability	>15%	5	10-15%	4	5-10%	3	3-5%	2	<3%	1		

## 2. PAST EXPERIENCE 'B'

2.1	Conducted IS Audit in PSU Banks in India in last two years	More than 4 PSBs	10	4 PSBs	8	3 PSB	6	2 PSB	4	1 PSB	2	-	-
2.2	Conducted IS Audit in Pvt./Foreign Banks and other Fin Inst in last two years	More than 4 Banks/FIs	5	4 Banks /FIs	4	3 Banks /FIs	3	2 Banks /FIs	2	1 Banks /FIs	1	-	-

## 3. PROJECT PLAN/EXPERTISE AVAILABLE 'C'

3.1	No. of skilled Professionals to be involved in this project	More than 5	10	4	8	3	6	2	4	1	0	-	-
3.2	Expertise / Skills available - CISA /CISSP / CISM /OCP etc.	More than 20	10	16 to 20	8	11 to 15	6	6 to 10	4	5	2	-	-
	<b>GRAND TOTAL</b>		100										