# NATIONAL INSTITUTE OF FASHION TECHNOLOGY

A Statutory Institute governed by the NIFT Act 2006, Ministry of Textiles,
Government of India, An ISO 9001:2008 Certified Institute.

HauzKhas, Near Gulmohar Park,
New Delhi - 110 016,

# TENDER FOR IT SECURITY AUDIT

## TABLE OF CONTENTS

## I. INTRODUCTION

National Institute of Fashion Technology (NIFT) was set up by the Ministry of Textiles, Government of India in 1986 which has been accorded statutory status under the Act of Parliament in 2006 (NIFT Act 2006) for the promotion and development of education and research in field of Fashion Technology.

NIFT provides fashion business education across the country through its network of 16 campuses. It provides four years under graduate (UG) program in design and technology, two years post graduate (PG) program in design, fashion management & fashion technology and sort duration education program to address the specialized needs of professional and students in the field of fashion.

NIFT has its head office at New Delhi with its campuses located at Bengaluru, Bhopal, Bhubaneswar, Chennai, Gandhinagar, Hyderabad, Jodhpur, Kangra, Kannur, Kolkata , Mumbai, New Delhi, Patna, Raebareli, Shillong and Srinagar.

## II. TENDER INVITATION – QUALIFYING CRITERIA

Campus Management Solution a automation solution developed by a In- house Software Development team of NIFT based at NIFT Chennai Campus. NIFT invites the interested & eligible Indian Auditing firms having following minimum qualifying criteria:

1. The bidder should be CERT-In or SQTC empanelled agency as on the date of bid submission. Copy of the valid empanelment certificate shall be enclosed in the Technical bid. Bids without empanelment certificate shall not be considered. Without spotting SI.No.1 to SI.No.8, tender will not be evaluation.
2. The Bidding company should have executed at least 10 IS Security Audit/Assessment and Penetration Testing Projects for any Government / Banks / Financial Institution / PSU in the country in last 5 years (i.e., 2012-13,2013-14,2014-15,2015-16 & 2016-17). Out of which, the Bidder should have conducted IS Security Audit/assessment and penetration testing for at least one or two enterprises totalling to 3000+ Computing Devices (IPs) from these enterprises. The individual order value from such projects should be above Rs.5 Lakhs. Bidder should be able to produce documentary evidence such as agreements, Brief detail of the projects handled should be added chronologically.
3. The bidder should have Quality Certifications ISO 9001 (valid copy of the certificate with certificate issue date and expiry date).

4. The Bidder must have on its rolls, on permanent employment basis, a minimum of Ten (10 nos.) Certified professionals. They must deploy at least two professionals who hold valid professional certifications like CISA/CHFI/CEH/ CISM/ CISSP/ ISO 27001 LA/ BS 7799LA/ ISO27001 LA. (Proof of Certification along with candidate's resumes should be attached).
5. Auditing company must deploy their full time employees only, whereas outsourcing to external/outside consultants or subcontracting to other companies is not acceptable. Personnel deployed for this engagement must have a valid police verification certificate. An undertaking to this effect shall be submitted by the vendor in the bid.
6. The bidder shall not have been black listed or shall not have any poor performance & litigation with any State /Central Govt./PSU/Corporation or any other Autonomous Organization of Central/State Government as on bid calling date. Self-declaration certificate on the company letter head signed by the CEO/Authorized Signature.
7. Bidder should submit the Mandatory Self declaration certificate on the company letter head signed by the CEO on the following:
    a. not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons;
    b. not have, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a Service contract within a period of three years preceding the commencement of the services, or not have been otherwise disqualified pursuant to debarment proceedings;
    c. not have a conflict of interest in the providing services in question as specified in the bidding document.
    d. Comply with the code of integrity as specified in the bidding document.

8. Bidder should use minimum of two commercial license scanners to perform the audit. (valid copy of the scanners license with certificate with expiry date should be provided).

## III. **SCOPE OF WORK**

### 3.1 Introduction

Further, as per the security policy , it is mandatory that the web applications undergo security audit to obtain a “Safe to Host” certification. The web based application need a Web application scanning solution that can scan for security loopholes in Web based applications to prevent would be hackers from gaining unauthorized access to corporate information and data. Web applications are proving to be the weakest link and are easy to hack. Therefore, intrusion detection and defense mechanisms are required to mitigate breach of security perimeters and gain unauthorized access to an organization’s network.

For Security Assessment/Audit, an iterative testing procedure shall be followed, with a gap for fixing issues identified during each iteration. At the end of each iteration, a report detailing the vulnerabilities identified, if any, should be submitted. It will be the responsibility of the concerned Client Department to plug these vulnerabilities, do a first level checking that the vulnerabilities identified have been corrected, before providing the web application for the second iteration. The vendor should cover at least three iterations.

a. Level 1 Security Audit / Assessment
Selected IT Security Audit Agency shall be responsible for the assessment of the security, vulnerabilities, threat and risks that exist in Web applications/ERP Systems by running Internet Vulnerability Assessment and Penetration Testing Scripts with appropriate usage of testing tools.

b. Level 2: Re-Audit based on the recommendation report from Level 1

The selected ISA shall undertake vulnerability assessment exercise on the rectified and corrected Web applications/ERP Systems submitted by the application development team of the concerned Client Department post Level 1. ISA shall also submit the detailed recommendation report for the vulnerabilities identified at Level 1 along with the summary/ checklist of vulnerabilities identified with subsequent correction status.

c. Issuance of “Safe to Host Certificate”

Web applications/ERP Systems security audit are to be conducted in iterative cycles (called as level) of testing and code correction till identified as “Safe for hosting”. APTS expects that all the vulnerabilities and potential threats would get rectified by the end of Level 2 or Level 3, once done selected ISA shall be responsible for the issuance of “Safe to Host” certificate for the considered Web applications/ERP Systems and submit the Final Audit Report.

The engaged Audit Agency shall be responsible to undertake the Security Audit as per Industry Standards and methods like and provide assurance as per the following Acts:

- Information Technology Act, 2000 as amended in 2008 and thereof (http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amen dme nt_act2008.pdf, etc.)
- Guidelines for Indian Government websites (GIGW) – NIC & DARPG
- CERT-In guidelines for web security & security audit (http://www.cert-in.org.in)
- Applicable best practices and Industry Standards like Open Web Application Security Project (OWASP), SANS top 20, ISO27001/ ISO 27001(2), OSSTMetc. during the auditing process
- NIFT may choose to avail follow up audit service depending on the necessity and guide lines of Department of Electronics and Information Technology, GoI on this issue.

## 3.2 DETAILED SCOPE OF WORK

### I.Security Audit of Web Applications

The selected IT Security Audit Agency shall be responsible for the assessment of the vulnerabilities, threats and risks that exist in web application through Internet Vulnerability Assessment, Penetration

Testing and Industry standard methodologies. This will include identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security of the website. The bidder will also be expected to propose a risk mitigation strategy as well as give specific recommendations to tackle the residual risks emerging out of identified vulnerabilities assessment.

Details of web application to be audited are provided below.

| S.No | Query items | Response |
|---|---|---|
| 1 | Name of the application proposed for audit | |
| 2 | Application details along with the work flow | |
| 3 | Name & Contact Details of Developer (Ph No. & Email) | |
| 4 | Url of the target application on test server for Audit | |
| 5 | Operating System Details (Deployed Server) (i.e., Windows-2003, Linux, AIX, Solaris, etc.) | |
| 6 | Web/Application Server with version (i.e., IIS 5.0, Apache, Tomcat, etc.) | |
| 7 | Front-end Tool [Server side Scripts](i.e., ASP, Asp.NET, JSP, PHP, etc.) | |
| 8 | Back-end Database<br>(MS-SQL Server, PostgreSQL, Oracle, etc.) | |
| 9 | Site users (closed user group and/or open to public) | |
| 10 | Any target date for the audit to be started ? | |
| 11 | Any target date for the audit to be completed by? | |
| 12 | Levels of Authorization (number of roles) | |
| 13 | Number of Static pages | |
| 14 | Number of Dynamic pages | |
| 15 | Total Number of Input fields | |
| 16 | Provision for e-commerce and/or payment gateway (Yes or NO) | |
| 17 | Whether the site contains any content management | |

| | | |
|---|---|---|
| | module (Y/N) | |
| **18** | Will the testing be conducted on-site or remotely via internet or VPN? | |
| **19** | No. of phases to test (number of itereations) | |
| **20** | Is the web application is protected by a firewall/IDS/IPS/Load Balances or any other security mechanism? Please provide details. | |
| **21** | Are web services integrated with the application? If yes, how many? | |
| **22** | Is this assessment 1 time a year (yearly) or 4 times a year (quarterly)? | |
| **23** | How many commercial licensed scanners / tools would you like us to use ? (1, 2, or 3) | |

## 3.3 SERVICES TO BE PERFORMED

IT Security Audit Agency should check for the below indicative list of potential threats and attacks which are vulnerable to the Websites/ Web application and shall submit a detailed recommendation report for the identified vulnerability.

| S. No | Potential Threats | Definition |
|---|---|---|
| 1. | Injection Flaws | Injection flaws, such as SQL, OS, and LDAP injection, occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. |
| 2. | Cross-SiteScripting (XSS) | XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. |

| | | |
|---|---|---|
| 3. | Broken Authentication and Session Management | Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities. |
| 4. | Insecure Direct Object References | A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. |
| 5. | Malicious File Execution | Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework, which accepts filenames or files from users. |
| 6. | Cross-Site Request Forgery (CSRF) | CSRF attack forces a logged on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests for the vulnerable application, which in turn thinks are legitimate requests from the victim. |
| 7. | Security Misconfiguration (NEW) | Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application. |
| 8. | Insecure Cryptographic Storage and Weak Ciphers and Session Keys | Many web applications/ websites do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. |
| 9. | Information Leakage and Improper Error Handling | Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks. |

|  |  |  |
|---|---|---|
| 10. | Failure to Restrict URL Access | Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway |
| 11. | Information tampering by forensic evidence | Whether there is an evidence to confirm that sufficient logs are maintained for all transactions and systems are in place to capture and maintain forensic evidence in a manner that maintains |
|  |  | control over the evidence and prevents tampering with and collection of false evidence |
| 12. | Insufficient Transport Layer Protection | Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly. |
| 13. | Un-validated Redirects and Forwards | Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages. |

Additional Testing for the following exploitable vulnerabilities:

- Canonicalization (standardization or normalization))
- Insecure Communications (clear text protocols like telnet, ftp for sensitive data)
- URL Access, Regular Expression Checks, Tainted Parameters, Header Integrity
- Path Manipulation, Thread Safety, Hidden Form Field Manipulation
- Fail Open Authentication, Weak Session Cookies, Miss configurations and Weak Passwords

The above list is only indicative; hence selected IT Security Audit Agency shall also be responsible to carry out the assessment for any other attack which is vulnerable to the website/web application.

## 3.4 DELIVERABLES

Web Application Security Report with a summary of High, Medium and Low vulnerabilities (Ref Annexure III)

i. Application Security Posture Assessment Approach.

ii. Snapshot of Current Application Information Security Posture

- Map Organizations reports to OWASP Top 10 errors
- Map Organizations web application errors to Top 25 programming errors per OWASP
- Summary of High Risk, Medium Risk and Low Risk Vulnerabilities specific to the enterprise.

iv. Penetration Testing Summary

- Analysis of Top 10 Configuration Errors and Top 25 Programming Errors per OWASP.
- Attack Types and Attack Methods Used
- Common Hacker Techniques

v. Recommendation for optimization and enhancement to the existing application wherever applicable

## 3.5OTHERS

i. The vendor shall maintain the validity of CERT-In or SQTC empanelled certificate till the end of the contract, failing which the contract is null & void and GoAP will be make alternate arrangements.

ii. Bidder should be ready to conclude comprehensive Service Level Agreement (SLA) and Non-Disclosure agreement. The bidder and/or their representatives shall be responsible for ensuring security and secrecy of the information coming to their knowledge during the discharge of their obligations. iv.Web application security audit should be conducted on a Staging Server in an “as is where is” basis will be almost replica of the live deployment.

v. Auditing on the live site if any conducted should be non-destructive and should not affect the system.

vi. For Web Application Security Assessment/Audit, an iterative testing procedure shall be followed, with a gap for fixing issues identified during each iteration. The vendor should cover at least three iterations.

vii. At the end of each iteration, a report detailing the vulnerabilities identified, if any, should be submitted. It will be the responsibility of the concerned Client Department to plug these vulnerabilities, do a first level checking that the vulnerabilities identified have been corrected, before providing the web application for the second iteration.

## IV BID SUBMISSION

### 4.1 Bid Submission

a) Agencies are advised to study the Bid Document carefully. Submission of the Bid will be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms and requirement specifications in the tender document with full understanding of its implications. Bids not complying with all the given clauses in this tender document are liable to be rejected. Failure to furnish all information required in the tender Document or submission of a bid not substantially responsive to the tender document in all respects will be at the agency's risk and may result in the rejection of the bid.

b) All the bids must be valid for a period of 90 days from the date of tender opening for placing the initial order. However, the rates should be valid until the work order completion.

c) The bids will be submitted in three envelopes as follows: EN-01: This envelope should contain a draft of Rs.7,500.00 (Rs. Seven Thousand Five Hundredonly) towards EMD drawn on a scheduled commercial bank and payable to NIFT, New Delhi. The envelope should be sealed and superscripted "EMD for NIFTfor IT Security Audit, due on 06/06/2017 at 03:00 PM". EN-02: This envelope should contain Technical Bid as per Annexure-I, should be sealed and superscripted as "Technical Bid for NIFT for IT Security Audit, due on 06/06/2017at 03:00 PM". EN-03: This envelope should contain the Financial Bid as per Annexure-II, should be sealed and superscripted as “Financial Bid for NIFTfor IT Security Audit, due on 06/06/2017 at 03:00 PM”. The above three envelopes may be sealed in an outer cover superscripted “NIFTfor IT Security Audit, due on 06/06/2017 at 03:00 PM”.

The envelope should be addressed to The Director – IT NIFT and submitted at NIFT, New Delhi office before the due date and time specified above.

4.2 Earnest Money Deposit (EMD)

The participating Agencies will furnish, Earnest Money Deposit (EMD) of Rs. 7,500/- in the form of Demand Draft from a scheduled commercial bank, drawn in favor of NIFT payable at New Delhi. The EMD of unsuccessful agencies shall be returned without interest after finalization of the tender. EMD of the selected agency shall be retained as the Security Deposit until the last work order completion. The amount retained as Security Deposit shall be returned after the satisfactory completion of the last work order without any interest.

4.3 Last date for bid submission

a) Bids, complete in all respects, must be submitted to NIFT office by the due date and time. In the event of the specified date for the submission of Bids being declared a holiday, the Bids can be submitted up to the appointed time on the next working day for which NIFT will make necessary provisions.

b) NIFT may, at its own discretion, extend the date for bid submission. In such a case all rights and obligations of NIFT and the Agencies shall be applicable to the extended time frame.

c) The bids will be accepted in NIFT office up to the specified date and time only. NIFT will not be responsible for any delay in obtaining the terms and conditions of the tender or submission of the bid before the due date and time of submission.

d) The offers submitted as documents, by telex/telegram/fax/Email or any manner other than specified above will not be considered. No correspondence will be entertained on this matter.

e) At any time prior to the last date for receipt of bids, NIFT, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective agency, modify the Tender Document by an amendment. The amendment will be notified on NIFT's website http://nift.ac.in and should be taken into consideration by the prospective agencies while preparing their bids.

f) In order to give prospective agencies reasonable time to take the amendment into account in preparing their bids, NIFT may, at its discretion, extend the last date for the receipt of bids. No bid may be modified subsequent to the last date for receipt of bids. No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified by the agency in the bid. Withdrawal of a bid during this interval may result in forfeiture of Agency's EMD.

g) The agencies will bear all costs associated with the preparation and submission of their bids. NIFT will, in no case, be responsible or liable for those costs, regardless of the outcome of the tendering process.

h) Printed terms and conditions of the agencies will not be considered as forming part of their bid. In case terms and conditions of the contract applicable to the Invitation of bid are not acceptable to any agency, they should clearly specify the deviations in their bids.

## V OPENING OF BIDS AND EVALUATION

### 5.1 Technical Bid

a) NIFT shall convene a bid opening session on 06/06/2017 at 03:30 PM where one representative from the participating agencies can participate.

b) Subsequent to this, NIFT will open the main cover and EN-01. The technical bids of only those agencies, whose EMD draft has been found to be in order and haven't withdrawn their bids, shall be opened constituted Technical Evaluation Committee (TEC).

### 5.2 Financial Bid

a) Financial bids, of only the technically qualified agencies, shall be opened on a notified date and time, in the presence of agency's representatives, who choose to remain present.

b) The financial bids will then be passed on to a duly constituted Financial Evaluation Committee (FEC) for evaluation.

### 5.3 Evaluation of Bids

NIFT reserves the right to accept any bid, and to cancel/abort the Tender process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected agencies or agencies and of any obligation to inform the affected agencies of the grounds for NIFT's action and without assigning any reasons.

## 5.4 Technical Evaluation

The technical bids will be evaluated by a duly constituted Technical Evaluation Committee (TEC). The first process for the TEC is to examine the eligibility of the agencies as per the tender eligibility. Bids, not satisfying the eligibility criteria will be rejected.

## 5.5 Financial Evaluation

a) After approval of the TEC report by the competent authority, the processing of the second stage will commence with the opening of the Financial Bids of only the technically qualified Agencies. A Financial Evaluation Committee (FEC) would scrutinize the commercial bids. The bids, found lacking in strict compliance to the commercial bid format will be rejected straightaway.

b) L1 is the agency quoting least Total cost in column (3) of the financial bid table in Annexure-II. In case two or more agencies quote the same Total Cost, then the agency having the highest total turnover as per Si.No.10 of Annexure-I shall be L1.

c) Document for minimum financial turnover of Rs.50 Lakhs per annum during the last 3 years (2013-2014, 2014-2015 and 2015-2016).

d) The rates quoted by L1 agency shall be accepted as the tender rates.

## VI DELIVERY, PERFORMANCE & PENALTY

a) Any unexcused delay by the agency in meeting the prescribed time schedule will attract a Penalty at the rate of 0.5% (point five) per day of the value of work assigned for up to ten days. Beyond ten days NIFT will have the option of getting the balance work done from alternate sources at the cost and risk of the defaulting agency.

Further NIFT may forfeit the EMD/Security Deposit of the defaulting agency and terminate the empanelment for default.

b) If at any time during performance of the Contract, the selected agency should encounter conditions impeding timely performance of Services, the agency shall promptly notify NIFT in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the selected agency's notice, NIFT shall evaluate the situation and may at its discretion extend the time for performance in writing.

c) The selected agency shall not outsource the work assigned to any other agency or franchisee, under any circumstances. This violation will attract forfeiture of EMD/Security deposit and cancellation of work order. The cost incurred on executing the work order through alternate source will also be recovered from the outstanding bills or by raising claims.

VII PAYMENTS

a) Payment will be made in Indian Rupees, after successful & satisfactory completion of the assigned work. The empanelled agency shall submit pre receipted bills in triplicate in the name of User, Accounts NIFT (or as instructed) along with

i. The completion certificate from The Director, IT

ii. The Security Audit Clearance Certificate

b) All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the income- Tax Act,1961 as amended from time to time.

c) Payments will be released within 30 days of the submission of bills complete in all respects.

## VIII GENERAL TERMS & CONDITIONS

a) The selected agency will not, without NIFT's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, sample of information furnished by or on behalf of NIFT in connection therewith, to any person other than a person employed by the agency in the Performance of the Contract. Disclosure to any such employed person will be made in confidence and will extend only so far as may be necessary for purposes of such performance.

b).In the event of the agency's company or the concerned division of the company is taken over / bought over by another company, all the obligations under the agreement with NIFT, should be passed on for compliance by the new company / new division in the negotiation for their transfer.

c) The selected agency automatically agrees with NIFT for honoring all aspects of fair trade practices in executing the work orders placed by NIFT.

## IX FORCE MAJEURE

a) Force majeure clause will mean and be limited to the following in the execution of the contract / work orders placed by NIFT :-• War / hostilities. • Riot or Civil commotion. • Earthquake, flood, tempest, lightning or other natural physical disaster. • Restriction imposed by the Government or other statutory bodies, which is beyond the control of the agencies, which prevent or delay the execution of the order by the agency.

b) The agency will advise NIFT in writing, duly certified by the local Chamber of Commerce, the beginning and the end of the above causes of delay, within seven days of the occurrence and cessation of the force majeure conditions. In the event of a delay lasting for more than one month, if arising out of clauses of force majeure, NIFT reserve the right to cancel the order without any obligation to compensate the agency in any manner for what so ever reason.

## X ARBITRATION

NIFT and the vendor will make every effort to resolve amicably, by direct negotiation, any disagreement or dispute arising between them under or in connection with the work order. If any dispute will arise between parties on aspects not covered by this agreement, or the construction or operation thereof, or the rights, duties or liabilities under these except as to any matters the decision of which is specially provided for by the general or the special conditions, such dispute will be referred to two arbitrators, one to be appointed by each party and the third to be appointed by the Director IT, National Institute of Fashion Technology, New Delhi and the award of the arbitration , as the case may be, will be final and binding on both the parties. The arbitrators or the umpire as the case may be, with the consent of parties, may modify the time frame for making and publishing the award. Such arbitration will be governed in all respects by the provision of the Indian Arbitration Act, 1996 or later and the rules there under and any statutory modification or re-enactment, thereof. The arbitration proceedings will be held in New Delhi, India.

## XI APPLICABLE LAW

The work order will be governed by the laws and procedures established by Govt. of India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing.

Annexure – I

## TECHNICAL BID

1. Name of the Agency
2. Address of the Agency
3. Telephone No
4. Email
5. Cert-in or SQTC empanelment No. Date, Validity
6. Amendment, Extension (if any) No., Date and Validity
7. Total Experience in IT Security Audit
8. Service Tax Registration No
9. PAN No.
10. Financial Turnover of the agency for the last 3 years (2013-2014, 2014-2015 and 2015-2016).

| Financial Year | Amount (Rs in Lakhs) | Remarks if any |
|---|---|---|
| | | |
| | | |
| | | |

Authorized Signatory

Parameters for Technical Evaluation would include the following criteria. Kindly enclosed the proff as per Tender invitation – qualifying criteria without spotting proff undertaking will not be evaluated

| SNo | Description | Criteria Points | (Max Marks) |
|---|---|---|---|
| 1 | Number of years of experience of the Firm in IS Audit area (Will be considered only on submission of satisfactory certificate from at least two clients)<br>• 3+ to 7 Years<br>• More Than 7 years | <br>5<br>10 | 10 |

| | | | |
|---|---|---|---|
| 2 | At least one prior engagement stating the firm's capability of undertaking IS Security Audit/Assessment and penetration test of computing devices in an enterprise (Bidder has to submit satisfactory certificates from the clients in respective area) | | |
| | • 3000 + to 5000 computing devices (IPs)<br>• More than 5000 computing devices (IPs) | 10<br>20 | 20 |
| 3 | List of Clients (IS Audit and penetration test exercise conducted by the bidder in Centralized data center will only be considered) (In the last 2 financial years considered for points award).<br>• For 5 or more in Govt. Sector/PSU/Banks/FIs in India<br>• For 3 or More Govt. Sector / PSU/Banks/FIs in India<br>• For 1 or more Govt. Sector / PSU/Banks/FIs in India | 15<br>10<br>5 | 15 |
| 4 | At least one prior engagement stating the firm's capability of undertaking IS Security Audit/Assessment and<br>Penetration test of servers in an enterprise<br>• More than 200 servers<br>• 200 servers or less | 10<br>0 | 10 |
| 5 | Details of qualified professionals on the role of the firm handling IS Audit. [Following professional qualifications will be considered:<br>(CISA/CHFI/CEH/CISM/CISSP/SANS)]<br>• More than 15 professionals<br>• 10 to 15 professionals<br>• Less than 10 professionals | 10<br>5<br>0 | 10 |
| 6 | ISO9001/ISO27001 Certification for Maintenance for IS<br>Audit/Software Audit area<br>• If Yes<br>• If No | 10<br>0 | 10 |
| 7 | Research experience & paper publications in security journals in the field of Information Security, Intrusions, etc. (proff submit)<br>• If Yes<br>• If No | 5<br>0 | 5 |
| 8 | Incident Handling Engagements in Govt. Sector<br>• If Yes<br>• If No | 10<br>0 | 10 |

Annexure – II

FINANCIAL BID

Name of the Agency:

Address:-

| SI.No<br>(1) | Service Offering<br>(2) | Amount<br>(3) |
|---|---|---|
| 1 | First level security audit, Report generation including recommendations | |
| 2 | Interim level security audit, report generation including recommendations | |
| 3 | Second & subsequent level security audit, report generation including recommendation | |
| | Total cost | |
| (Rupees in words ___________________________________________ | | |

| SI.No | Module | Forms | Reports |
|---|---|---|---|
| 1 | Admission | 35 | 72 |
| 2 | Student Life Cycle Management | 111 | 175 |
| 3 | Academic Administration | 88 | 73 |

a) Service tax will be paid extra as applicable from time to time.

b) Rates should be quoted in INR and indicated in both figures and words. Price in words prevail in the event of any mismatch.

c) Agencies have to quote rates for all categories/constituent items mentioned in SI. No. 1 to 3 and Total cost of the Financial Bid quoted by the agency then the lowest total cost shall be L1. In case rates for any of the constituent items are not quoted by the L1 agency their bid will be rejected, EMD forfeited.

Authorized Signatory:

Name:

Mobile:

E-mail:

Company Seal

Annexure III

Sample format for Effort Estimation

Name of the user / customer:

Address:

User Contact Person details:

Name of the website / web application:

URL if any

| SI.No | Service Offerings | Number of Man Days |
|---|---|---|
| 1 | First level security audit, Report generation including recommendations | |
| 2 | Interim level security audit, report generation including recommendations | |
| 3 | Second & subsequent level security audit, report generation including recommendation | |
| | Total | |

Service Tax as applicable

Lead Time required for beginning the security audit on receipt of work order

Mode of security audit:- On-site / off site

The rates are needed to be quoted in the work in Annexure II

Authorized Signatory:

Name:

Mobile:

E-mail:

Company Seal