UNIVERSITY OF CALICUT

(Purchase Division)

File No.8301/PURCHASE-ASST-A3/2017/Admn

Calicut University P O

Dated.09.08.2017

RE-TENDER NOTICE

Sealed and super scribed competitive tenders **(in three-cover format)** are invited by the Registrar, University of Calicut, for the Audit of the software used for Centralised Admission Process at Directorate of Admissions (DoA) as per the terms and conditions mentioned below in annexure.

Tender Number	No.8301/PURCHASE-ASST-A3/2017/Admn Dated.09.08.2017
Tender form available at	: The tender form can be had from the Purchase Division on payment of cost of tender form of **Rs.525/-** or can be downloaded from the University Website (including general conditions provided thereof) separate DD should be enclosed for cost of tender form (website - universityofcalicut.info)
Date & Time and place for acceptance of Tender	:Sealed tenders with EMD of **Rs.2,500/- (Rupees two thousand and five hundred only)** drawn in favour of Finance Officer should be submitted to the Deputy Registrar (Purchase), University of Calicut, Malappuram - 673635 on or before **24.08.2017 4.00 PM.**
Date & Time of opening of Tender	**:24.08.2017 11.00 AM**
Superscription	:Tender for Audit of the software used for Centralised Admission Process

ANNEXURE

WEBSITE SECURITY AUDIT OF ADMISSION SOFTWARE, DOA UNIVERSITY OF CALICUT

Section 1: Instructions to Bidders

Introduction and Background

Objectives :

The objective of this proposal is to conduct the Audit to discover any vulnerabilities/weaknesses/attacks in the website(s) and web application(s), which are listed in this document. The Audit should be done by using Industry Standards and as per the Open Web Application Security Project (OWASP) methodology.

The main objectives for conducting this website security audit is to:

1. Identify the security vulnerabilities, which may be discovered in the website and website application security audit including cross-site scripting, Broken ACLs/Weak session management, Buffer Overflows, Forceful browsing, CGI-BIN manipulation, Form /hidden field manipulation, Command injection, Insecure use of cryptography, Cookie posing, SQL

injection, Server miss-configuration, Well-known platform vulnerabilities, Errors triggering sensitive information leak etc. on the websites and web applications of the DoA, Calicut University.

2. Requirements and analysis performed to increase overall security posture;
3. Identification and prioritization of various risks to the web applications.
4. Gain a better understanding of potential website/web applications its applications and vulnerabilities.
5. Determine if the current websites/applications are secure and evaluate the security.
6. Identify remedial solutions and recommendations for making the web site applications secure.
7. Rectify / fix identified potential vulnerabilities, and web application vulnerabilities thereby enhancing the overall security.
8. Issuing of appropriate certifications for hosting these applications in the Kerala State Data centre.

Submission of Proposals :

The proposals shall be prepared in a **three-cover format (one each for pre-qualification, technical and financial documents)**

The Bidder shall submit Pre-Qualification Bid, Technical Bid and Financial Bid documents in separate wax sealed envelopes prescribing Pre-qualification, Technical and Financial Bid on the top left hand corner. All these three sealed covers are to be put in a bigger cover which should also be sealed and duly super scribed.

Sealed proposals will be received at the office of the Deputy Registrar Purchase, University of calicut before the prescribed date & time.

Following are terms and conditions for the particular tender bid submission:

1. The tenderer cannot bid in consortium.
2. All proposals should be submitted in English language only.
3. Award of the contract resulting from this tender will be based upon the most responsive Bidder whose offer will be the most advantageous to University in terms of cost, functionality and other factors as specified.
4. University of Calicut reserves the right to reject any or all offers and discontinue this tender process without obligation or liability to any potential Bidder
5. All proposals received after the specified date and time shall not be considered for award of work.
6. The original and copies of the bid, each consists of the documents listed in instructions, shall be typed and shall be signed by the bidder or a person(s) duly authorized to bind the bidder to the contact.

Bid Security :

1. The Bidder shall furnish, as part of its technical proposal, an original bid security of Rs.2,500/- (EMD).
2. The Bid security shall be in the form of Demand Draft/drawn in favour of Finance Officer, University of Calicut. The Bid Security shall be valid for period of 30 days beyond the final bid validity period.

3. The Bid Security must be submitted in the Technical Bid Cover.
4. Any proposal not sealed shall be rejected.
5. Bid security of unsuccessful bidders will be returned within and not later than 30 days of award of contract to the successful bidders.
6. Bid Security is refundable.
7. Forfeitures of Bid Security: The Bid Security may be forfeited if a bidder withdraws its bid during the period of validity of his proposal as specified by the bidder in his proposal; or in the case of the successful bidder, in case the bidder fails to sign the contract or to furnish performance security as mentioned below.

Pre-Qualification/Eligibility Criteria for Bidders:

Eligibility Criteria: Pre -qualification proposal will be used to evaluate if the bidder's technical skill base, financial capacity are consistent with the needs of the project. Following criteria has been defined for eligibility of an audit firm (copy of the documentary evidence must be submitted.) The audit firms that qualify the below mentioned criteria need only apply.

1. This invitation is open to all Indian firms/company (the bidder).
2. The firm/company must be a company registered under the Indian Companies Act, 1956/ The Partnership Act, 1932 or Registration of Societies Act.
3. The bidder must have been empanelled by CERT-IN, having a valid empanelment certificate. Proof of this will have to be submitted.
4. The bidder should have been in operation for a period of at least 3 years.
5. The bidder should have had an average turnover of (Rs) 25,00,000/- (Twenty five Lakhs) only during the last 3 financial years in Information Technology related operations as revealed by audited accounts.
6. The bidder should have adequate number of Certified Information Systems Auditor (CISA / CISSP qualified professionals (say a minimum of 3), so as to associate them with each audit team auditing listed websites in this RFP simultaneously.
7. The bidder should give commitment to deploy a Project Manager in the project, who should be a Graduate in Engineering (B.Tech/B.E) and having at least 10 years experience in the Information Technology field, out of which he/she should have minimum three years experience in the Security Audit related Projects. He/She must be a Certified Information Systems Auditor (CISA). The bidder should have at least 3 security audit certified professionals on rolls who have sufficient experience in Information Technology & Web security audit and they must have Certified Information Systems Auditors (CISA)/CISSP. The details of Project Manager/Auditors for this project has to be submitted with this bid.
8. The bidder should have experience of conducting similar Website Audit as proposed by DoA.
9. The bidder should have SEI CMM Level 5 or higher Certificates.
10. The bidder should own at least one commercial Security Audit Tool. Name, Description of the tool needs to be defined. Proof of this will have to be submitted.
11. The bidder should have at least one implementation/technical support office in South India.
12. The bidder should have to submit the proof for the eligibility criteria including GST Registration, Income Tax PAN Number, Etc., .

Technical Proposal :

The Technical Bid shall include the detailed project plan for website security Audit Corresponding to the deliverables as required by DoA, for the project. The project plan should indicate the

milestones and time frame of completion of the different activities of the project. The bidder is required to give details of the Project Management Methodology, Audit Standards and methodology along with the quantum of resources to be deployed for the project, qualifications, experience of personnel deployed, in the technical bid. Resources and support required from DoA, may also be clearly defined. The technical bid is required to be submitted.

Financial Proposal :

Following are the terms and conditions for the Financial Proposal

1. This tender is for a fixed price bid.
2. The financial proposal shall be priced in Indian Rupees.
3. The Financial proposal shall clearly indicate, as per the Financial Summary Sheet, the total costs of carrying out the services as described in the Terms of Reference (TOR) as well as taxes (to be shown separately).
4. The quotations shall be fixed and shall not allow for any fluctuation in costs of labour, transport, etc. No adjustment shall be made to the contract value for any fluctuation arising following submission of tender.

Disqualifications :

DoA may at its sole discretion and at any time during the evaluation of Proposal, disqualify any bidder, if the bidder has:

1. Submitted the Proposal documents after the scheduled date and time;
2. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements;
3. Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years;
4. Submitted a proposal that is not accompanied by required documentation or is non-responsive;
5. Failed to provide clarifications related thereto, when sought;
6. Submitted more than one Proposal;
7. Declared ineligible by the Government of India/State/UT Government for corrupt and fraudulent practices or blacklisted.
8. Submitted a proposal with price adjustment/variation provision.

Evaluation Process :

A two-stage procedure (i.e Pre-Qualification criteria /Technical Bid and Financial Bid) will be adopted for evaluation of proposals. The process for evaluation of proposals is as given below:

1. Pre-qualification Criteria Evaluation: Preliminary scrutiny of the Proposals for eligibility will be done to determine whether the Proposals are complete, whether the documents have been properly signed, whether any computational errors have been made, and whether the Proposals are generally in order. Proposals not conforming to Prequalification eligibility criteria shall be rejected summarily. Proposal responses conforming to preliminary scrutiny shall be checked for conformance to the prequalification eligibility criteria. Non-conforming Proposals shall be out rightly rejected.
2. Technical Evaluation: An Evaluation Committee will assess all the bids received. Technical

Proposals would be considered only for those bidders, who have been qualified during the Prequalification Evaluation of Proposals. If a Technical Proposal is determined as not substantially responsive, DoA will reject it.

3. Financial Bid Evaluation: Financial Proposals would be considered only for those bidders, who have been qualified during the Prequalification and technical Evaluation of Proposals.
4. The DoA, may, at their discretion and without explanation to the prospective Bidders, at any time choose to discontinue this tender without obligation to such prospective Bidders.

Award and Duration of the work :

On acceptance of Proposal for awarding the contract, DoA will notify the successful bidder in writing that their proposals have been accepted. DoA and successful bidder shall sign the Contract Agreement at the time of signing of Contract. After signing of the Contract Agreement, no variation in or modification of the term of the Contract shall be made except by written amendment signed by the parties. The successful bidder has a period of 15 days to start the work. The successful bidder is expected to complete the work within a period of 45 days once the work has started.

Subcontracting and/or Outsourcing of Work :

Outsourcing / subcontracting of work will not be permissible in any form. Subcontracting/outsourcing will lead to termination of contract and forfeiture of Performance Guarantee. In case of such unavoidable circumstances, the audit firm/company has to take prior written permission from DoA for engaging such agency or individual.

Termination of the Work :

DoA without prejudice to its rights under the Conditions of tender or any other remedy for break of Contract, shall have the right to terminate contract of the Auditor at any time, if, the Auditor breaches any of the terms and conditions.

- Mentioned in this document or in the Award of Contract;
- As defined by CERT-IN, Department of Information technology, Min .of Information Technology, Government of India.
- The contract may also be terminated in case, the Information Technology Department is of the view that the Auditor's performance or competence fails to meet the standards required for the Audit assignment.

Penalties :

For any delay in completion of the task beyond the 45 days period from the date of award of work, the liquidated damages of a sum equivalent to 0.5% of the project value for every day of delay, up to a maximum of 30% of the contract value shall be deducted from the project value. Once the maximum, penalty amount is reached, termination of the contract of shall also be made.

Payment Terms and Conditions :

1. The bidder will offer commercial quote, based on fixed cost, inclusive of GST and other duties, cess, fees etc. if any, (to be shown separately) and DoA will not pay any additional amount other than indicated in the offer.
2. TDS will be deducted at source for any payment made, as per rules of Government of India.
3. DoA will neither provide nor reimburse expenditure towards any type of accommodation, travel ticket, airfares, train fares, halting expenses, transport, lodging, boarding etc.

4. DoA may impose penalty, in case of delay of any deliverables at the rate of 0.5% per week delay, either for completion of audit exercises or submission of draft reports, subject to a maximum of 30 % of the total cost, for all delays attributable directly to the Audit Firm/Company.
5. The audit firm/company will not sub contract part or complete assignment to any other agency or individual. In case of such unavoidable circumstances, the audit firm/company has to take prior written permission from DoA for engaging such agency or individual.
6. The audit firm/company shall keep information related to this project confidential and will not divulge to outside agencies without written consent from DoA
7. If selected, the Audit Firm/Company shall have to sign agreement.

Performance Guarantee :

The successful bidder shall furnish the performance security representing 10% of the total value of the contract within 15 days of the receipt of notification of award. Performance security should remain valid for a period of 60 days beyond the date of completion of all contracts.

Audit Environment :

The Audit may be conducted at the successful bidder's site by accessing remotely or localy from Directorate of Admissions (DoA) /Calicut University Computer Centre (CUCC).

Responsibilities of the auditor :

The Auditor shall ensure that:

1. The auditing is carried out strictly in accordance with the terms and conditions stipulated in the audit assignment contract as well as general expectations of the auditee from an auditor.
2. All applicable codes of conduct and auditing standards are adhered to with due professional care.
3. The audit report is submitted to the DoA and one copy of the report should be submitted to CUCC.

Liability in Respect Of Damage :

The Auditor shall make good or compensate for, all direct damage occurring to website and web applications of DoA in connection with this Contract for carrying out audit.

Provided that this Clause shall not apply if the Auditor is able to show that any such damage is caused or contributed to by the neglect or default of DoA. The security auditor's liability will be limited to the cost of service provided. Default or neglect by the Auditor will include both malicious and non-malicious errors and project mismanagement.

Quality Of Audit :

The selected vendor will ensure that the audit assignments are carried out in accordance with applicable guidelines and standards as mentioned in this document and terms and conditions specified by the CERT-IN, Department of Information Technology, Min. of Information Technology, Government of India.

Confidentiality and copyright :

Information relating to the examination, clarification and comparison of the Proposals shall not be disclosed to any bidder or any other persons. The undue use by any bidder of confidential

information related to the process may result in rejection of its Proposal. During the execution of the project except with the prior written consent of the DoA, the Consultant and its personnel shall not at any time communicate to any person or entity, any confidential information acquired in the course of the auditing. All recipients of tender documents, whether they submit a tender or not, shall treat the details of the documents as private and confidential. Copyright in the documents prepared by the bidder is reserved to the DoA. The Auditor shall ensure that his employees, servants, agents and sub-contractors keep confidential all information in whatever form it is obtained, produced or derived from or related to the carrying out of its obligations under this terms and conditions.

Validity of Proposals :

The bidder proposal shall remain valid for a period of 120 days beyond the closing date of the tender.

Right to Accept/Reject Proposals :

The DoA reserves the right to accept or reject any Proposal(s) at any time prior to award of contract, without thereby incurring any liability to the affected Respondent(s) or any obligation to inform the affected bidder (s) of the grounds for such decision.

RFP Clarifications :

During Pre Qualification and Technical Evaluation of the Proposals, DoA may, at its discretion, ask bidders for clarifications on their proposal. The bidders are required to respond within the prescribed time frame.

Amendments in RFP :

At any time prior to deadline for submission of proposal, DoA may for any reason, modify the RFP. The prospective bidders having received the RFP shall be notified of the amendments through website and/or newspapers and such amendments shall be binding on them.

Force Majeure:

If the performance as specified in this order is prevented, restricted, delayed or interfered by reason of:

- Fire, explosion, cyclone, floods
- War, revolution, acts of public enemies, blockage or embargo
- Any law, order, proclamation, ordinance, demand or requirements of any Government or authority or representative of any such Government including restrict trade practices or regulations.
- Strikes, shutdowns or labour disputes which are not instigated for the purpose of avoiding obligations herein,
- Any other circumstances beyond the control of the party affected then notwithstanding anything here before contained, the party affected shall be excused from its performance to the extent such performance relates to prevention, restriction, delay or interference and provided the party so affected uses its best efforts to remove such cause of non-performance and when removed the party shall continue performance with utmost dispatch.

Follow-Up and Compliance :

The Audit firm/company is required to follow-up with the concerned offices of the DoA and the concerned Department for compliance. The Audit firm/company has to submit a summary

compliance report at end of each task and the final report should certify that the website/web applications (should be mentioned the name of the website and/or web applications) is "Certified for Security ".

Exit Plan :

The Partner will promptly on the commencement of the exit management period supply the following:

- Documentation relating to website audit Intellectual Property Rights ;
- Data and confidential information
- The terms of payment as stated in the Terms of Payment Schedule include the costs of the Partner complying with its obligations under this Schedule.
- In the event of termination or expiry of MSA, Project Implementation, or Operation and Management SLA, each Party shall comply with the Exit Management Plan. During the exit management period, the Partner shall use its best efforts to deliver the services.

Section 2: Terms of Reference

2.1 Scope of the Work

Bidders would be expected to perform the following tasks for Website and the web- application Security to analyze and review the website/application security .The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in website through Internet Vulnerability Assessment and Penetration Testing. 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. The website and Web-application should be audited as per the Industry Standards and also as per the OWASP (Open Web Application Security Project) model. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented. The final report will certify the particular website/web application "Certified for Security ".All the Website security audit reports should contain the details as mentioned at the Audit report of Section 2.2.

The scope of the proposed audit tasks is given below. The audit firm/company will be required to prepare the checklist/reports

2.1.1 Task 1: Web Security Audit/ Assessment :

Check various web attacks and web applications for web attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to the website/Web-application.

Vulnerabilities to SQL Injections CRLF injections

Directory Traversal

Authentication hacking/attacks

Password strength on authentication pages Scan Java Script for security vulnerabilities File inclusion attacks

Exploitable hacking vulnerable Web server information security

Cross site scripting

PHP remote scripts vulnerability HTTP Injection

Phishing a website

Buffer Overflows , Invalid inputs , insecure storage etc .

Other any attacks, which are vulnerability to the website and web-applications

The Top 10 Web application vulnerabilities, which are given below, should also checked from the given websites:

1. Cross Site Scripting (XSS) : XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
2. Injection Flaws : Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker©s hostile data tricks the interpreter into executing unintended commands or changing data.
3. Malicious File : Code vulnerable to remote file inclusion (RFI) allows attackers to Execution 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.
4. Insecure Direct Object Reference : A direct object reference occurs when a developer exposes areference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
5. Cross site Request Forgery (CSRF): A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
6. 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.
7. Broken authentication and session management : Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users identities.
8. Insecure Cryptographic Storage : Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
9. Insecure communications : Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
10. Failure to resrict URL access : Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users.Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

2.1.2 Task 2: Re-Audit based on the Recommendations Report from Task 1 :

The vendor will be responsible to provide a detailed recommendations report for the vulnerabilities observed from Task 1.

2.1.3 Task 3: Re, Re-Audit, if required based on the Recommendations Report from Task 2 :

If vulnerabilities are observed form the re-audit, the vendor has to provide a detailed recommendations report on the vulnerabilities observed or found from Re-auidt/Task2. The DoA is expected that all vulnerabilities will be removed at the Task 3 stage. The Audit firm/company has to submit a summary compliance report at end of each task and the final report should be certify that the website/web applications (should be mentioned the name of the website and/or web applications) is "Certified for Security ".

2.2 Deliverables and Audit Reports

1. The successful bidder will be required to submit the following documents after the audit for each website, as mentioned below and the audit firm must also submit suggestions / recommendations and other detailed steps for enhancing the website security.
    i. A detail report will be submitted with security status and discovered vulnerablities , weknesses and mis-configurations with associated risk levels and recommended actions for risk mitigations.
    ii. Summary and detailed reports on secruity risk, vulnerabilites and audit with the necessary countermeasures and recommended corrective actions as recommended above need to be submitted in duplicate to the DoA. Also the same copy should be submiited to the Calicut University Computer Centre.
    iii. All deliverables shall be in English language and side A4 size format.
    iv. The vendor will be required to submit the deliverables as per agreed implementation Plan.
    - The deliverables (like Summary compliance report, Check list, Audit Report, Executive Summary and Final compliance report after all observations) for each task to be submitted by the Auditors for this assignment as mentioned in the Task1, Task2 and Taks3.
2. Timeframe of the deliverables
    - The selected successful bidder will be required to start the project within 15 days from the date of placing the order for the audit.
    - The entire audit must be completed within 45 days from the placing of order.
    - All the draft reports of the agreed deliverables should be submitted by the firm/company within 15 days of the commencement of the audit.
    - The audit, as mentioned above, has to be completed in time. It is expected that, if required, the successful bidder may deploy multiple teams to complete the audit projects within given time frame.
3. Audit Report : The Website security audit report is a key audit output and must contain the following:
    1. Identification of auditee (Address & contact information)
    2. Dates and Location(s) of audit
    3. Terms of reference (as agreed between the auditee and auditor), including the standard for Audit, if any
    4. Audit plan
    5. Explicit reference to key auditee organisation documents (by date or version) including

policy and procedure documents

6. Additional mandatory or voluntary standards or regulations applicable to the auditee
7. Standards followed
8. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment , password cracking and etc.)
    a. Tools used
    b. List of vulnerabilities identified.
    c. Description of vulnerability
    d. Risk rating or severity of vulnerability
    e. Test cases used for assessing the vulnerabilities
    f. Illustration if the test cases to provide the vulnerability
    g. Applicable screen dumps
9. Analysis of vulnerabilities and issues of concern
10. Recommendations for action
11. Personnel involved in the audit, including identification of any trainees
12. The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.
13. The successful bidder must also follows the guidelines of National Informatics Center (NIC) for website security Audit and submit the Audit report as per the format mentioned in guidelines.

2.3 Expectations Of Auditee Organization From The Auditor :

Following are the expectations of auditee from the auditor:

1. Verification of possible vulnerable services will be done only with explicit written permission from the auditee.
2. The auditee will refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
3. With or without a Non-Disclosure Agreement Contract, the security auditor will be ethically bound to confidentiality, non-disclosure of customer information, and security testing results.
4. Auditor should have clarity in explaining the limits and dangers of the security test.
5. In the case of remote testing, the origin of the testers by telephone numbers and/or IP addresses will be made known.
6. Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering will be taken.
7. The scope should be clearly defined contractually before verifying vulnerable services.
8. The scope should clearly explain the limits of the security test.
9. The test plan should include both calendar time and man-hours.
10. The test plan should include hours of testing.
11. The security auditors are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the customer organization.
12. The exploitation of Denial of Service tests is done only with explicit permission.
13. High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may convey immediate risk, discovered during testing are to be reported

immediately to the DoA with a practical solution as soon as they are found.

14. The Auditor is required to notify the auditee whenever the auditor changes the auditing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the DoA is to be notified with progress updates at reasonable intervals.
15. Reports should state clearly all states of security found and not only failed security measures.
16. Reports will use only qualitative metrics for gauging risks based on industry-accepted methods. These metrics are based on a mathematical formula and not on feelings of the auditor.
17. The Auditor is required to notify the DoA when the report is being sent as to expect its arrival and to confirm receipt of delivery.
18. All communication channels for delivery of report are end to end confidential.

2.4 List of Websites/Web applications for security audit : UG and PG admssion software.

2.5 "Tender will be governed by the specifications, terms and conditions stated in the annexure of the tender notice. For any terms and conditions not stated therein the General Conditions of the tender will be applicable."

DEPUTY REGISTRAR
Purchase Division